No. 81 / 1st quarter 2011

COMMUNICATIONS & STRATEGIES

DigiWorld Economic Journal

The economics of cybersecurity

Edited by Loretta ANANIA, Johannes M. BAUER & Michel VAN EETEN

- Between Awareness and Ability: Consumers and Financial Identity Theft
- The Impact of Public Information on Phishing Attack and Defense
- Is Security Lost in the Clouds?
- Might Governments Clean-up Malware?
- Cyber-Security at European level: The Role of Information Availability
- Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing

Interviews with
Keith BESGROVE, OECD
Evert Jan HUMMELEN, OPTA

20 years!

www.idate.org IDATE

Foreword

Rest assured, COMMUNICATIONS & STRATEGIES will not be joining those who discover with poorly feigned astonishment that the Web is also home to criminal activity and manipulative strategies!

On several occasions, our journal has chosen to highlight the tremendous contributions that the Internet has made to the various forms of innovation. This now allows us to take an unambiguous look at the darker side of the Web, namely cybercrime, through articles that examine the different dimensions that underpin Internet users' trust and security.

Thinking about the future of the Internet also means finding effective ways of combating criminal activities online, even if they do not appear to be in any way hampering the growing use of the Web and its many applications. This battle has to include informing users of the dangers, while also stepping up coordinated discussions on digital identity, paying full attention to privacy issues, and planning for the next steps in Internet governance while also distinguishing it clearly from the much less legitimate demands for increased control over the network of networks.

I'll also take this opportunity to announce the upcoming publication of our popular DigiWorld Yearbook (*). In it, readers will find key data and an exploration of the overriding trends in telecom, Internet and media markets, prepared by IDATE analysts, along with a look at the outstanding events in our sectors that played out in 2010.

As for upcoming issues of our journal, they will be devoted to:
- A single market for eCommunications? (June)
- ICT and Health (September)
- Net Neutrality: what next? (November)

And, finally, we are especially proud to announce that this 81st issue marks the 20th anniversary of COMMUNICATIONS & STRATEGIES! This gives me a chance to reiterate the editorial policy we endeavour to uphold: to provide a journal devoted to exploring the central issues shaping the telecom, Internet and media industries, offering up analyses from the finest economists and academics from around the globe.

Enjoy the issue!

Yves GASSOT
Executive Director of Publication

(*) For more information, visit us online at: www.digiworld.org

Call for papers

Dossier to be published in no. 82 – 2nd quarter 2011

A Single Market for eCommunications?

Edited by Denis LESCOP, Lorenzo Maria PUPILLO & Ulrich STUMPF

The single market is a key objective of the European Union. A single market for digital services is among the priorities of the Commission's Digital Agenda. Among the main initiatives of the Commission to support a digital single market, one can identify:

- Promotion of European-wide content rights, towards which European rights owners have to balance the static risks of lower possibility to discriminate and optimise value and the dynamic opportunities of a European-wide market. This balance may differ between video, music, books or game types of contents.
- Regulating inter-state roaming prices to converge to domestic prices by 2015 as announced by Commissioner Kroes. This has to be balanced with the potential impact of such evolution on domestic mobile prices and on the economic transfers between Member States and customers which may result of the regulation.
- Impulse consistent and timely spectrum policies in Europe, in particular concerning the availability of Digital Dividend. In that respect, the implementation of service or technological neutrality principles should be pragmatic in order to preserve the benefits of standardisation and of the technical efficiency of spectrum utilisation.
- Harmonise the implementation of European regulation leveraging the outcome of the review of the European framework adopted in December 2009: the role of Berec and enhanced European powers to monitor regulatory remedies in national markets. However, harmonisation to date has often been experienced by market players as alignment on the more severe level of regulation which may explain some reservations on the harmonisation process.

Policies such as specific provisions for new member states or the promotion of geographical segmentation in regulatory market analysis may also be part of the single market program:

- Specific provisions for new Member States are meant to bridge the gap, in particular in terms of infrastructures, between all Member States, provided European rules of State Aids or of Services of General Economic Interest are respected.

- Geographical segmentation of market analysis may help to differentiate remedies, where the competitive conditions in parts of the territory justify a lighter touch on, or the withdrawal of, existing regulatory measures, or regulatory forbearance, where new measures are considered. However, the detailed implementation of such analysis needs to be discussed.

Despite the strong impulsion given by the European Commission in favour of efficient and competitive fixed and mobile market in European Member States, its digital agenda recognizes the failure of Europe at achieving digital successes similar to those the USA have generated over the last decade. To which extent European policies have influenced this outcome needs to be discussed. First, there are general issues such as the European tax regimes, which non-European firms are better placed than European ones to take the maximum benefit of. Concerning specifically Information Society regulation, recent research has, for instance, shown that the enforcement of the e-privacy directive in Europe had an important negative impact on the relative efficiency of European on-line advertising business compared with its international competitors. Also, European policy has concentrated the constraints of regulatory pressure on electronic communications services providers which is the part of the digital value chain where European players had the strongest position world-wide. In that respect, Single Market may also mean consolidation of the market structure and reduction of the number of players: should European policy favour or limit such trends? These examples show that in the future, the strength and competitiveness of European digital industry in the world-wide competition for digital services may also need to become a critical element of European digital policy.

Contributions to this special issue on Single Market may refer either to the global questions or to any of the relevant specific topics mentioned above.

Please send proposals (full papers) before April 4th 2011 to:
s.nigon@idate.org

Call for papers

Dossier to be published in no. 83 – 3rd quarter 2011

ICTs and health

Edited by Steven ANDLAUER, Elettra RONCHI & Graham VICKERY

A healthy active population is widely recognized as one of the main drivers of economic growth and prosperity as well as being a fundamental building block for modern societies. Improved access to health services and better health care delivery are important steps in maintaining and improving the level of health in the general population, underpinned by advances in medical technology. However, health budgets have ballooned in all countries and health care expenditures take a larger and continually increasing share of household and government expenditures. This is due to many factors, including more widespread care delivery, aging populations in many countries, increased costs associated with technological and medical advances, and increasing demand from patients and the general population for more advanced treatment for illness and diseases, many of which are increasingly costly to treat.

Against this background Information and communications technologies (ICTs) are seen as providing important tools and solutions to improve the level of health and contain costs. ICTs can be used in a wide range of applications ranging from distance health care and monitoring aging populations to new areas of medical research. However one of the most widely heralded and most difficult to implement technologies has been in the area of electronic health records. These in principle should allow patients and health-care professionals to access the medical history of patients and the general population, enable immediate updating and modification to reflect changing health profiles, improve health delivery and health system efficiency, while saving costs. With improvements in communications and widespread Internet access health records and patient-centred health care strategies should be increasingly enabled

The papers of this C&S dossier will address both theoretical and empirical aspects of developing and using electronic health records to improve health performance including:

- Technology trends and developments
- New Web-based developments in access
- Case studies at regional and national levels

- New combinations of health information and access
- Applications in particular areas of health-care
- Patient-centred health care records

Please send proposals (full papers) before April 30th 2011 to: s.nigon@idate.org

Submission of papers

All papers submitted for publication will be reviewed using the "double blind" system by at least two referees, selected based on the subject matter of the paper, from the journal's panel of referees. Shorter articles appearing in the "Features" section are refereed at the discretion of the Editor.

Proposals must be submitted in Word format (.doc) and should not exceed 6,500 words, including the footnotes and references.

Please ensure that all illustrations (graphics, figures, etc.) are in black and white - excluding any color - and are of printing quality.

Bibliographical references should be included at the end of the article. Should these references appear in the text, please indicate the author's name and the year of publication in brackets.

Coordination and information
Sophie NIGON
s.nigon@idate.org
+33 (0)4 67 14 44 16
www.comstrat.org

COMMUNICATIONS & STRATEGIES

No. 81, 1st quarter 2011

Dossier

The economics of cybersecurity

Edited by Loretta ANANIA, Johannes M. BAUER & Michel VAN EETEN

Other paper

Features

Use Logics

Book Review

Events

Dossier:
The economics of cybersecurity

Introduction to the Economics of Cybersecurity

Johannes M. BAUER
Michigan State University

Michel VAN EETEN
Delft University of Technology

The challenges of cybersecurity

Cybercrime, cyberterrorism, and cyberwar are apocalyptic horsemen of the information age. Business leaders regularly name information security as the biggest challenge facing them in the future. Information security breaches entail direct and indirect costs to businesses and individuals that are affected and to society at large. But the negative effects of such violations go much further. Information security is critical to sustain trust in electronic transactions. Without such trust, only part of the productivity gains that could be achieved with the help of advanced information and communication technologies will materialize. Moreover, trust in the security and confidentiality of electronic means of communication is also an important precondition for realizing many of their potential benefits for invigorated civic life. It is difficult to estimate the extent of opportunities foregone by insufficient information security and it is the unknown magnitude of the associated opportunity costs that renders the formulation of good policies difficult.

Information and communications technologies have permeated all aspects of society. Embedded in all other critical infrastructures, including energy, transportation, as well as health and emergency services, they themselves form a critical nervous system of the economy, government and private life (SOMMER & BROWN, 2011; GALLAHER, LINK & ROWE, 2008). They have also become an indispensible component of research, development and innovation, the key drivers of change in knowledge-based economies. As general purpose technologies, they are used in an increasing range of business transactions, such a financial services, e-commerce, and global supply chains. Their wide diffusion has greatly enhanced the range of technological opportunities in sectors not least by enabling new forms of networked interaction. Many efforts to expand the frontiers of knowledge rely on collaboration and flexible sharing of information and data across time and space: e-research is increasingly based on massive, openly accessible

datasets; health services can be greatly improved by electronic information sharing; open innovation is built around fluid organizational boundaries, often mediated by information and communication technology; and social media derive a large part of their appeal from the sharing of information.

Reaching an appropriate level of information security is difficult. A first factor complicating matters is the increasing number of players required to provide advanced communication systems. In addition to hardware manufacturers and network operators, software vendors, a plethora of application and service providers, and different types of users populate this space (OECD 2009). As these players complement each other, the problem is compounded by the high interdependence among them. Increasing national and international broadband connectivity enhances the opportunities of cybercriminals to launch attacks with high trans-border agility, as the risk of being caught and prosecuted is lessened by the complications of orchestrating effective international law enforcement. At the same time, the sophistication of attacks increases continuously in a technology race between defenders, such as information security service providers, and increasingly specialized attackers. Heterogeneous communities of application developers – some open source, some proprietary, some hybrid – and user groups with greatly varying information security savvy open many potential inroads for attacks. The proliferation of new uses such as social networks, new mobile devices and applications, and the emergence of new services related to cloud computing all open new vulnerabilities.

The threat landscape is continuously shifting and attacks are becoming increasingly sophisticated. Early generations of "white hat" hackers were motivated by notoriety and fame but typically sought to reveal security problems to help fix them. During the past decade, a differentiated and skilled underworld of cybercrime has emerged whose primary motive is financial gain. Whereas computer viruses continue to be a problem, criminal attack strategies now more typically rely on malware, propagated in multiple ways via viruses, worms, trojans, and drive-by attacks from compromised websites (e.g., Symantec, 2011). Large numbers of infected computers are integrated in versatile botnets, which serve as platforms for sending spam, fraud, and other types of cybercrime (OECD, 2009; HOGBEN *et al*., 2011). For the past few years, attacks have become more targeted. Nearly half the respondents in the latest CSI Computer Crime and Security Survey that had experienced security incidents reported targeted attacks, double the number from two years prior (CSI, 2010).

Information security has both private and public good characteristics. Given the complexity of the information and communications system, the question of whether a desirable level of security for individual players and society overall will be achieved by decentralized decisions of the players demands close scrutiny. Each of the players responds to incentives relevant to their own objectives. For example, application providers, such as Facebook, encounter trade-offs between providing high levels of security and privacy and their ability to earn revenues from advertisers and complementary business partners. Many incentives nudge players toward higher security but there are also many potential flaws that may cause a deviation between the private and the social costs and benefits of decisions. If this is the case, a sub-optimal level of security overall will result (VAN EETEN *et al*. 2008; BAUER & VAN EETEN, 2010). Moreover, in highly interconnected systems, the overall level of security may be strongly influenced by the weakest link (VARIAN, 2004).

The Internet and the vibrant information services enabled by it have evolved largely in an environment free of government regulation. Many of the governance issues were addressed using bottom-up methods of self-regulation or, in some cases, co-regulation between government agencies and stakeholders. From these developments hybrid forms of governance emerged, in which alternative and traditional forms of regulation complement (and sometimes rival) each other. The collective-action problems of cybersecurity have led to several new initiatives at the national, regional, and international levels by government and non-government actors. They range from government-led international thrusts such as the Cybercrime Convention, promulgated by the Council of Europe, and the London Action Plan (LAP) to national legal and regulatory initiatives, such as the Australian Internet Security Initiative (AISI), often in public-private partnerships. Moreover, several private sector-led projects address cybersecurity, including the Messaging Anti-Abuse Working Group (MAAWG) and the Cloud Security Alliance (CSA). Currently, these measures amount to a patchwork rather than an integrated approach but they are steps in the right direction and will help designing more effective solutions. Recent work on the economics of cybersecurity, to which we turn in the next subsection, is an important source of knowledge for these initiatives.

Economics of cybersecurity

At the heart of the rapidly growing field of the economics of cybersecurity, we find this key insight captured by ANDERSON & MOORE (2006, p. 610):

> "[P]eople have realized that security failure is caused at least as often by bad incentives as by bad design."

Market players make their own tradeoffs regarding what kind of security measures they deem appropriate and rational, given their business model. Clearly, these business models are very different for actors in the different niches of the complex ecosystem surrounding information systems and networks. In other words, many instances of what could be conceived as security failures are in fact the outcome of rational economic decisions, given the costs and benefits facing the actors involved within the timeframe of those decisions.

As security comes at a cost, tolerating some level of insecurity is economically justifiable. From an economic perspective, the key question is whether the costs and benefits perceived by market players are aligned with social costs and benefits of an activity. In certain situations, the security decisions of a market player may be rational for that player, given the costs and benefits it perceives, but its course of action may impose costs on other market players or on society at large. These costs are typically not taken into account by the market player making the initial decision, causing an "externality." Externalities are forms of market failure that lead to sub-optimal outcomes if left unaddressed. In the presence of externalities, Internet-based services may be less secure than is socially desirable.

Security externality is a key concept, but economics offers a broader framework to make sense of security issues. As ANDERSON (2001, p. 1) wrote in an early, ground-breaking piece:

> "Many of the problems of information security can be explained more clearly and convincingly using the language of microeconomics: network effects, externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons."

Within this research, the incentives that stimulate efficient behavior are central.

The approach has been used, for example, to explain security issues in software markets (ANDERSON & MOORE, 2006). These markets tend to be dominated by a few firms. Dominance can be due to network externalities –

the more people use certain software, the more valuable it becomes, and the more users it attracts. These incentives have effects on security. First-mover advantages reward a short time to market, rather than longer development cycles that result in better security. Vendors of platform software, such as operating systems, have to attract vendors of complementary products for the platform. The more complementary products are available, the more valuable the platform. To become dominant, platform vendors may be reluctant in implementing security restrictions for those complementary products.

In the markets for Internet access, incentives drive how providers deal with security issues in their networks (VAN EETEN & BAUER, 2008). A dominant incentive is the often high cost of customer support, which works against contacting large numbers of customers with infected machines. On the other hand, providers that do not act against abuses can suffer a backlash from other providers who blacklist and block their traffic. In the interactions among providers, it was suggested that large providers are more or less immune to such forms of peer pressure and, therefore, have weaker incentives to act against security problems (MOORE *et al.*, 2009). Recent empirical research, however, revealed that the networks of large Internet service provider harbor, on average, fewer infected machines per subscriber than those of small providers (VAN EETEN *et al*., 2010). Other incentives seem to be more powerful, such as whether telecommunication regulators are active in the area of security of providers.

The incentives of financial service providers, such as banks, lead them to often compensate customers for the damage they suffered from online fraud. In that sense, they internalize the externalities of sub-optimal security investments of their customers as well as the software vendors whose software is exploited to execute the attacks. The financial institutions bear these externalities, but they are also in a position to mitigate the size of these externalities, i.e., they can manage the risk through the security measures around online financial services. For these providers, but also for society as a whole, it may currently be more efficient to keep losses at acceptable levels, rather than to aggressively seek to reduce them. A dominant incentive is the benefits of a growing online transaction volume. Any security measure that might reduce the ease of use of online financial services may impede this growth, which implies costs that are likely to be much higher than the current direct damage from malware-related fraud.

The behavior of many different market players has been examined from an economic perspective. Looking at security issues in terms of costs and

benefits also helps to put broader security questions in perspective. For example, in a technical sense, the number of phishing attacks may be rising, but this may in fact reflect a diminishing economic success of these attacks (HERLEY & FLORENCIO, 2008). The evidence indicating the actual losses of security incidents is ambiguous. The earlier cited CSI Computer Crime and Security Survey found that while reported losses of firms rose in recent years, they are still much lower compared to the losses reported in 2001 and 2002.

Where we have better evidence that economic damage is indeed rising, such as with financial fraud, fraud levels may actually be diminishing in relative terms, compared to the total volume of transactions. In 2009, the UK Payments Administration reported that card-not-present fraud – which includes Internet-based fraud – had risen by 350 percent in the period from 2000 to 2008 (APACS, 2009). In the same period, the total value of online shopping alone increased by 1,077 percent. As an aside, the figures for 2009 and 2010 actually show a decrease compared to 2008, even in absolute terms (UK Cards Association, 2011).

Main themes of this special issue

Research in the area of the economics of cybersecurity is still expanding. This special issue aims to contribute to a blossoming field that has changed our understanding of security issues. The papers in this special issue reflect state-of-the art thinking on the economics of cybersecurity and responses by public policy and non-governmental action.

The unabated use of public awareness campaigns to stress the ability and responsibility of consumers to protect themselves against cyberrisks receives both support and resistance. Supporters see consumers as clueless facilitators of crime, by publishing personal data online or otherwise disclosing it. Opponents stress that consumers are victims and that private and public organizations are diverting attention away from their own facilitating behavior. (van der) MEULEN addresses this tension, focusing on the issue of identity theft. She argues that neither side adequately appreciates how recent developments are eroding the consumer's ability to actively control the facilitation process and explores several alternatives to public awareness campaigns.

A classic and still critical question in cybersecurity is this: who benefits more from publicly available information on security incidents, the attackers

or the defenders? MOORE & CLAYTON bring an innovative empirical approach to bear on this issue. They study the impact of publicly available information on phishing web sites. If attackers benefit more from this information than defenders, then phising websites placed on a public blacklist should be re-compromised more often than phishing websites that are only known within closed communities. Their analysis forcefully demonstrates the opposite. Their conclusion is that strategic disclosure of incident information can actually help defenders, if properly designed.

BLUMENTHAL critically examines the security implications of cloud computing. Cautioning against the current hype surrounding the provision of platforms as a service (PaaS), infrastructure as a service (IaaS) and software as a service (SaaS), she reveals several potential security risks. Clouds could be used as new platforms for malice, offering both new ways to configure attacks and to evade criminal prosecution. Users of cloud services cannot easily assess the security policies and precautions of service providers, which often decline liability for data breaches in their service agreements. Given these potential risks, the paper discusses implications for organizations and individuals and suggests next steps for researchers and public policy that could help address the concerns raised.

The enduring problem of infected end user machines, most notably in the form of botnets, has demonstrated that this problem cannot be solved by end users alone. Increasing attention is paid to the role of critical intermediaries, such as ISPs. ISPs, however, have incentives that discourage them from dealing with large numbers of infected customers. CLAYTON explores a specific solution to overcome this incentive problem, namely government subsidies for cleaning up computers. In other words, we would treat infections as a public health issue. Based on certain assumptions, he estimates that the costs of such an initiative may be lower than is often assumed, and could be as low as one dollar per person per year.

BISOGNI, CAVALLINI & TROCCHIO discuss the role of information availability in enhancing cybersecurity. Their narrowly construed analysis is based in an economic model of information security investment, in which the effects of a lack of information are examined. After a brief overview of the prevailing European institutional and regulatory framework for cybersecurity, the authors discuss three actions at the European level that could contribute to better information security: (1) information sharing about threats, (2) information sharing about information security breaches, and (3) measures that increase information security competence.

Challenges of securing the vast, decentralized Internet infrastructure are addressed by KUERBIS & MUELLER. Early routing protocols were designed without particular attention to security. The paper focuses on Resource Public Key Infrastructure (RPKI), an effort to reduce the resulting vulnerabilities. RPKI changes the relations among stakeholders, increasing the influence of centralized players at the expense of Internet Service Providers (ISPs). Describing in detail the mixed incentives of the various players (ICANN, regional registries, and ISPs), the paper examines conflicts of interest. The authors show how, for the time being, consensus could be achieved by permitting voluntary actions by ISPs but anticipate continued tensions over the establishment of more centralized governance structures.

The special issue is rounded-off with two interviews about the challenges of information security and ongoing initiatives to meet them. Keith Besgrove is the First Assistant Secretary, Consumer Policy and Post division of the Australian Department of Broadband, Communications and the Digital Economy. He also serves as the Chairman of the OECD Working Party on Internet Security and Privacy (WPISP). Evert van Hummelen is the head of the team Internet Security at the Dutch regulatory agency OPTA. Both provide important perspectives by experts on the forefront of policy efforts to enhance information security.

Putting together this special issue involved the collaboration of many individuals. We would like thank the contributors for their submissions and their prompt responses to editorial requests. We also would like to thank reviewers for their critical reading and helpful comments on the original manuscripts. Special thanks also to Keith Besgrove and Evert Jan Hummelen who found time in their busy schedules to respond to our questions. Sophie Nigon at IDATE was a good cheerleader who kept us motivated and on track and Yves Gassot lent his support to pursue the topic of cybersecurity. We received a larger number of good papers than could be accommodated; several will be published in future issues of *COMMUNICATIONS & STRATEGIES*.

References

ANDERSON, R. (2001). *Why Information Security is Hard – An Economic Perspective*. Proceedings of the 17th Annual Computer Security Applications Conference, New Orleans, Louisiana IEEE Computer Society. http://www.acsac.org/2001/papers/110.pdf.

APACS (2009): Fraud – *The facts 2009. The definitive overview of payment industry fraud and measures to prevent it*.
http://www.theukcardsassociation.org.uk/files/fraud_the_facts_2009.pdf.

BAUER, J.M. & VAN EETEN, M., J.G. (2009): "Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options", *Telecommunications Policy*, 33(10/11), 706-719.

CSI (2010): *2010/2011 CSI Computer Crime & Security Survey*, New York: Computer Security Institute.

HERLEY, C. & D. FLORENCIO (2008): "A Profitless Endeavor: Phishing as Tragedy of the Commons". http://research.microsoft.com/apps/pubs/?id=74159.

GALLAHER, M.P., LINK, A.N. & ROWE, B.R. (2008): *Cyber Security: Economic Strategies and Public Policy Alternatives*, Cheltenham, UK; Northampton, MA: Edward Elgar.

HOGBEN, G., PLOHMANN, D., GERHARDS-PADILLA, E. & LEDER, F. (2011): "Botnets: Detection, Measurement, Disinfection & Defence", Heraklion, Crete, Greece: European Network and Information Security Agency (ENISA).

OECD (2009): *Computer Viruses and Other Malicious Software*, Paris: Organisation for Economic Co-operation and Development.

SOMMER, P. & BROWN, I. (2011): "Reducing Systemic Cybersecurity Risk", OECD/IFP Project on Future Global Shocks, IFP/WKP/FGS(2011)3. Paris: Organisation for Economic Co-operation and Development.

Symantec (2011): "MessageLabs Intelligence", February.
http://www.messagelabs.com/globalthreats.

UK Cards Association (2011): "Fraud losses drop on UK cards, cheques and online banking".
http://www.theukcardsassociation.org.uk/media_centre/press_releases_new/-/page/1323/

VAN EETEN, M. & BAUER, J.M. (2008): "The Economics of Malware: Security Decisions, Incentives and Externalities: Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy", DSTI/ICCP/REG(2007)27, Paris: OECD.

VAN EETEN, M., J. BAUER, H. ASGHARI & S. TABATABAIE (2010): "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data", STI Working Paper 2010/5, OECD.
http://www.oecd.org/officialdocuments/displaydocument/?doclanguage=en&cote=dsti/doc(2010)5

VARIAN, H. (2004): "System Reliability and Free-Riding", in L.J. CAMP & S. LEWIS (Eds), *Economics of Information Security* (pp. 1-15), Berlin, New York: Springer.

Between Awareness and Ability: Consumers and Financial Identity Theft

Nicole S. van der MEULEN
The Centre of Expertise (HEC), the Hague

Abstract: The role consumers play in the facilitation of financial identity theft is an important topic of discussion. Academics often side with consumers and recognize them as victims rather than facilitators. Others, both in the public and the private sector, believe consumers play a more prominent role in the facilitation of financial identity theft. This is particularly apparent through the popularity of public awareness campaigns. Neither of these accounts manages to reflect the complexity of the overall picture. The following article demonstrates how the role consumers play is continuously changing as a result of the evolution of methods used by perpetrators of identity theft. This evolution requires a different response from both the public and the private sector as consumers lose more control over their potential indirect facilitation of financial identity theft.

Key words: Financial identity theft, consumers, information security, public awareness campaigns.

On July 27, 2009, the Ministry of Justice of the Netherlands launched a large public awareness campaign to prevent citizens from falling victim to cybercrime. [1] During five weeks, the campaign which features a fictional character 'Sandra', was seen on television and heard on the radio. In the commercial used for the campaign, Sandra reveals all. Her bank account number, pin code, log-in name, and video tapes of her holiday at the beach are made public. Sandra herself watches and listens as people gather on the street to witness the publication of all her information. She appears flabbergasted. She is the perfect depiction of the unaware and naïve citizen. Security on the Internet, the campaign claims, is in your hands. [2]

The continued proliferation of public awareness campaigns which emphasize the potential for and the ability of consumers to protect

1 See http://www.nederlandveilig.nl/veiliginternetten/.

2 In Dutch the slogan is: "*veilig internetten heb je zelf in de hand*."

themselves, against cybercrime in general and financial identity theft [3] in particular, receives both support (CATE, 2001; MILNE, 2003) and resistance (SOLOVE, 2003; HOOFNAGLE, 2005). As a result, there is an ongoing discussion which focuses on the degree to which consumers maintain both the ability and responsibility to 'prevent', or at least reduce the risk of financial identity theft. In particular, SOLOVE (2003) states how even if individuals did take all steps advised to them, significant risk reduction still fails to occur. This lack of significant risk reduction is due to the actions of both the public and the private sector, which play a more prominent role in the facilitation of financial identity theft, according to SOLOVE. In the overall problem, consumers are victims rather than facilitators. Their share in the enablement of the problem is minimal, if existent at all.

Certain sources even consider the emphasis on individual responsibility a mere political strategy to divert the attention away from the 'actual' facilitators (WHITSON & HAGGERTY, 2008). A similar sentiment is echoed by MARRON (2008: 29) when she states: "[t]he problem becomes pitched not as one of systemic institutional culpability, but as lack of awareness on the part of individuals." According to STONE (1989) stories of 'inadvertent cause' are common in social policy. Individuals 'cause' many problems such as poverty, malnutrition, and disease, because they fail to understand the harmful effects of their willful actions. "Inadvertence here is ignorance;" STONE (1989: 286) writes, and "the consequences are predictable by experts but unappreciated by those taking the actions. These stories are soft (liberal) versions of blaming the victim: if the person with the problem only changed his or her behavior, the problem would not exist." Awareness campaigns, such as the one described above, appear to depict such a story of inadvertent cause. While various authors reject this claim, they do so based on the argument that the role of both the public and the private sector overshadows the impact of consumer actions.

This article aims to shed a different light on the ongoing discussion and accepts an alternative position in an effort to add another dimension to the debate. Rather than rejecting the focus on user education based on the actions of the public and the private sector, this article aims to demonstrate

[3] Financial identity theft for the purposes of this article refers to both account takeover and true name fraud. Account takeover occurs when perpetrators obtain the credentials of an existing account of another individual and use such credentials to drain the account's balance. True name fraud, on the other hand, occurs when perpetrators manage to obtain sufficient personal information about another individual to open a new account or request a new credit card in the name of the other person.

how user education and awareness campaigns fail to address the range of threats faced by consumers, in their role as facilitators of financial identity theft. This failure is important to take into consideration with respect to future policy initiatives set forth in an effort to reduce the risk of financial identity theft. The three categories presented below aim to depict how the evolution of the methods used by perpetrators has theoretically led to a crucial expansion of ways to take advantage of consumers, and how the consumer's ability to actively control the facilitation process is slowly, but surely, diminishing.

■ The others

Before delving into the manners through which consumers can potentially facilitate the first stage of financial identity theft, the comprehensive character of the argument developed within this contribution requires a brief reflection on the potential facilitation of other actors. [4] As indicated in the introduction, the role played by other actors, such as government agencies, financial service providers, data brokers, etc., is often used to illustrate how restricted the influence of consumers is on the prevention of financial identity theft (See SOLOVE, 2003; HOOFNAGLE, 2005; HOOFNAGLE, 2009). This is the case for two reasons. First of all, the only influence consumers may exert with respect to the facilitation of financial identity theft is in relation to the first stage, where perpetrators acquire the personal information needed to either commit true name fraud or account take over. The second stage, where perpetrators abuse the previously obtained personal information, is at the discretion of the public and the private sector, through the means of authentication implemented for e-government and e-commerce or e-banking transactions, respectively. Consumers may mitigate the damage through being more alert and keeping a close watch on account activity and credit reports; but this can only mitigate, not prevent or reduce risks.

The second reason for the restricted influence of consumers is the extensive information collection and storage exercised by the public and the private sector. Over the years, this massive collection and storage of personal information has drawn significant attention as a result of the

[4] This article is an excerpt of the author's doctoral dissertation *Fertile Grounds: The Facilitation of Financial Identity Theft in the United States and the Netherlands*, where 'the others' receive a far more extensive analysis with respect to their potential facilitation of financial identity theft.

publicity afforded to several major data security breaches. To what extent data security breaches actually contribute to financial identity theft is a challenging question to answer (See GOVERNMENT ACCOUNTABILITY OFFICE, 2007). Whilst it is difficult to determine where the information misused for financial identity theft purposes originates, certain breaches have been directly connected to incidents of financial identity theft. A prime example is Choicepoint, a large data broker in the United States, which suffered a highly publicized data security breach several years ago (see SULLIVAN, 2005). According to the official complaint issued by the Federal Trade Commission (FTC), the Choicepoint data breach led to at least 800 cases of identity theft.[5] Due to the pioneering data breach notification legislation in California, Choicepoint was obligated to notify consumers of the breach. In total, Choicepoint notified 163,000 consumers, according to the FTC. The sheer size of such data security breaches certainly appears to trump the potential for facilitation of individual consumers with respect to financial identity theft. And since these data security breaches are widespread[6] in both the public and the private sector, the impact of consumer actions appears limited. This limitation, however, can also be illustrated and extended through a different venue, which is the primary contribution this article aims to make.

■ 'Voluntary' facilitation

The term 'voluntary' is problematic because its usage within the current context can lead to misguided interpretations. Voluntary facilitation here mainly refers to information dispersion which is unprompted by the perpetrator. The term is mainly used to indicate the distinction between the current and the subsequent categories of facilitation, and does not carry any normative implications. The voluntary exposure of consumers' personal information can facilitate the first stage of financial identity theft. Perpetrators have developed several methods to potentially take advantage of such exposure. Among the most infamous methods is dumpster diving. Basically, unsuspecting consumers toss out various documents containing sensitive personal information. Perpetrators become aware of this and start

5 *United States of America* v. *ChoicePoint* (2006). Supplemental stipulated judgment and order for permanent injunction and monetary relief: 4.

6 The Privacy Rights Clearinghouse and the Identity Theft Resource Center, among others, maintain records of reported data security breaches in the United States.

rummaging through garbage cans in search of these documents. Many times, one document does not contain all of the necessary information, but perpetrators combine different pieces of garbage to complete the picture. Several years ago, receipts still contained valuable information including the full credit card and account number, which proved to be an attractive source for perpetrators. Overall, consumers would unwittingly and voluntarily present perpetrators with their valuable personal information. Dumpster diving, as a method, took advantage of the voluntary and active participation of consumers.

More recently, other potential opportunities for perpetrators of financial identity theft have evolved through consumers who dispose of old computers, which contain, yet again, valuable personal information. Even if consumers believe they have cleared their hard drive of all data, they are often wrong. The data erased on their hard drive can easily be recovered by perpetrators. Various authors acknowledge this vulnerability (VALLI, 2004; BENNISON & LASHER, 2004).

As the more 'physical' types of voluntary consumer facilitation fizzle out, the focus turns to the digital arena. Much attention has been devoted to the presence of individuals on social networking sites, and in particular the information shared on such fora. In theory, social networking sites such as Facebook, MySpace, and Twitter provide the ideal outlet to let everyone know nearly everything about oneself. Much research aims to demonstrate how users of social networking sites perceive privacy and potential privacy risks associated with their presence on such sites (see for example GROSS & ACQUISTI, 2005; JONES & SOLTREN, 2005; DEBATIN *et al*., 2009). Such research generally provides conclusions which illustrate a lack of concern with the provision of personal information on the part of consumers and the ability for a wide public to view such information (see, in particular, GROSS & ACQUISTI 2005). This willingness to share personal information surpasses the area of social networking sites. Through an experiment, GROSSKLAGS & ACQUISTI (2007: 14) demonstrate how "[...] most subjects happily accepted to sell their personal information even for just 25 cents, and virtually all subjects waived the option to shield their information."

BILGE *et al*. (2009) furthermore demonstrate how perpetrators of financial identity theft can access personal information maintained on profiles of users. This occurs through, for example, profile cloning where perpetrators 'clone' the profiles of authentic users and request to be added as a friend. Perpetrators send these requests to the social network of the

'cloned' individual rather than to random strangers. From the experiment of profile cloning, BILGE *et al*. (2009: 557) conclude how:

> "[...] the friendship acceptance rate for the forged profiles was over 60% for all the forged accounts (in one case, being as high as 90%). The acceptance rate from unknown users was constantly below 30% [...] These results confirm that by forging profiles, an attacker can achieve a higher degree of success in establishing contacts with honest users than when using fictitious accounts."

The outcomes of the various research projects appear to be relevant since identity theft is mentioned on a regular basis as a potential risk associated with social networking site activity (see DONATH & BOYD, 2004; GROSS & ACQUISTI, 2005; STUTZMAN, 2006; BOYD & ELLISON, 2008; IBRAHIM, 2008; STRATER & LIPFORD, 2008). Whether such a risk is viable depends largely on the type of personal information provided by users of the sites.

Despite the lack of apparent empirical evidence demonstrating misuse of personal information obtained from social networking sites for the purposes of financial identity theft, much discussion focuses on the distribution of responsibility with respect to security aspects of such sites. Based on the results of their experimental research, BILGE *et al*. provide suggestions for improvements of security on social networking sites. In their suggestions, the authors acknowledge how users continue to be the weakest link but improved security requires the involvement of the social networking sites. BILGE *et al*. provide the recommendation for social networking sites to provide more information on the authenticity of the friend request and the user who initiated the request.

Whereas BILGE *et al*. direct suggestions toward the sites as opposed to the users, GRIMMELMAN (2008) focuses on the users. GRIMMELMAN (2008: 1140) states how:

> "It's temptingly easy to pin the blame for these problems entirely on Facebook. Easy - but wrong. Facebook isn't a privacy carjacker, forcing its victims into compromising situations. It's a carmaker, offering its users a flexible, valuable, socially compelling tool. Its users are the ones ghost riding the privacy whip, dancing around on the roof as they expose their personal information to the world."

Grimmelman therefore argues in favor of an educational approach which specifically targets users of social networking sites in an effort to help understand the risks associated with the exposure of their personal information.

Even so, the usage and retention of personal information provided to Facebook by Facebook is a topic of heated discussion. Facebook 'shares' information received from users with third parties. This occurs when users install Facebook applications or gadgets. FELT and EVANS (n.d.) write how:

> "[w]hen Jane installs a Facebook application, the application is given the ability to see anything that Jane can see. This means that the application can request information about Jane, her friends, and her fellow network members. The owner of the application is free to collect, look at, and potentially misuse this information."

The Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2008) filed a complaint against Facebook in 2008 alleging 22 separate violations of Canadian privacy law. These violations included Facebook's failure to inform users of how Facebook discloses their personal information to third parties for advertising and other profit-making activities, and Facebook's failure to obtain permission from its users for such uses and disclosures of the personal information of its members (CIPPIC 2008). The user outrage did not occur until the following year when Facebook made changes to its terms of service which led to increased media attention about the practices of the social networking site (see STELTER, 2009). Facebook changed the terms of service and deleted a provision which allowed members to remove their content at any time. Moreover, the new language added to the terms of service stated how Facebook would retain the content and licenses of users even after they terminated their accounts (STELTER, 2009).

The importance of the current dispute over Facebook and its treatment of the information provided by its members is the distribution of responsibility with respect to the 'exposure' of personal information. The line between consumer as opposed to business facilitation becomes blurry and this in turn also influences the judgment about the 'facilitator.' For if perpetrators obtain the information from a third party which said third party obtained from a Facebook profile page, who facilitates? This is an important argument in particular because consumer awareness primarily focuses on this type of consumer facilitation, the voluntary information dispersion. Even so, important to note is how the potential connection between personal information exposure on social networking sites and the facilitation of financial identity theft remains largely drawn on theoretical risks rather than empirical evidence. Still the information available on social networking sites, such as date of birth, full name, affiliations can provide indirect assistance to potentially commit financial identity theft. From the 'old fashioned' method of dumpster diving to the more innovative method of perusing social networking sites, the argument goes that perpetrators cleverly take advantage of both

the 'carelessness' and the 'cluelessness' of consumers. This is certainly the area over which consumers have a sense of 'control' and an area in which consumer awareness may at least have some success. This category indicates how, especially as consumers become more knowledgeable about the dangers present in contemporary society, there is at least some room for improvement with regard to reducing consumer facilitation. In contrast, the subsequent two categories begin to demonstrate a shift with regard to consumer control and the level of voluntary involvement on the part of consumers.

■ Social engineering

When consumers do not provide the information voluntarily or unprompted, perpetrators themselves have to hunt for it. And they have managed to do so rather well. In contemporary society, phishing has become a well-known concept, especially among those involved in various areas related to digital technology. The underlying principle of phishing, which is gaining personal information through social engineering techniques, is far from new. As DANG (2008: 8) notes:

> "[w]hether it's called social engineering, trickery, confidence tricks, cognitive biases, or scams, the concept of exploiting a person's naivety and trust is as prevalent today as it has been since the dawn of time."

The craft of the con artist has always been present and used for a variety of criminal activities. Before the Internet domination, perpetrators used more traditional means such as calling and ringing doorbells trying to obtain valuable information. Mitnick, one of the most 'infamous social engineers' in the modern era, carefully outlines how con artists used more 'old-fashioned' social engineering techniques, such as calling, to obtain valuable information from businesses. Through the art of persuasion, con artists successfully managed to convince employees of various corporations to surrender pivotal business information, including passwords (MITNICK *et al*. 2002). The ultimate art used by perpetrators is to convince the target, whether a business or a consumer, that they are someone else, someone trustworthy. The Internet provided and continues to provide perpetrators with the ideal platform to update their old techniques and to more efficiently target consumers. The variety of ways perpetrators incorporate social engineering techniques on the Internet is rather impressive, even during the early days. Special Agent RILEY (1998: 7) described how:

> "[o]ne of the most popular things to do to get people to give up their personal information is to offer credit card accounts at a very, very low interest rate, such as 4.9 or 5.9 percent."

Perpetrators developed websites to offer credit card accounts in search of personal information. RILEY (1998: 8) offers another example when she describes how:

> "[i]n addition to the credit card applications themselves, several others of the schemes that are available out there right now include credit rescue operations where pages, again, using very high-quality graphics are made to look legitimate and offer the ability for you to wipe out any credit problems you have simply, again, by providing all of your personal financial information."

Especially during the early days of the Internet, consumer awareness about potential fraud schemes was severely absent. Perpetrators gratefully managed to take advantage of this absence.

The first actual phishing 'attacks' differed greatly from their current counterparts. The term phishing entered the circuit in 1996 when hackers managed to get unsuspecting America On-line (AOL) users to reveal their passwords. With their passwords, the hackers could gain free internet access (RAMASTRY, 2004). Since then, phishing appears to have become an attractive profit making strategy for various perpetrators involved in financial identity theft. In the beginning phishing emails maintained a sense of amateurism, which provided consumers with the opportunity to potentially detect foul play. Emails sent to Dutch consumers, for example, contained errors which automatically carried an air of suspicion. An infamous email sent by perpetrators posing as the Postbank, a former Dutch bank, made the mistake of using the opening *Lieve Postbankklant*, which directly translates into "Dear Postbankclient," except the dear used in the phishing emails is reserved for communication with close friends and loved ones. Furthermore, the email mainly uses the informal "you" (*je*), similar in German *du* and in Spanish *tu* as opposed to the more formal and more appropriate *u*, or in German *Sie* and Spanish *usted*, which is a direct sign that there is something out of the ordinary going on. Despite the apparent errors, the initial attack led some clients to click on the link and as such the bank was forced to replace all usernames, passwords and TAN codes. This also occurred in other European countries. As DIRRO & KOLBERG (2008: 24) note:

> "In the early days, messages were composed in a crude German notation that looked like it was an English or a Russian text translated by Babel Fish. That's probably what happened."

As information on phishing attacks began to grow, perpetrators also expanded and sophisticated their methods. DANTU *et al*. (2008) describe how the nature of phishing attacks changed over time. Whereas initial attacks were passive such as password guessing and eavesdropping, more recent attacks are active through the employment of Trojans, traffic interception, and the adoption of social engineering techniques. The introduction of phishing as a vehicle to commit financial identity theft led to crucial research on consumer behavior and phishing detectability (see, for example, JAKOBSSEN, 2007). Both academic and non-academic researchers aimed to analyze the awareness of consumers with regard to phishing attacks and their ability to recognize phishing emails. DHAMIJA *et al*. (2006) conducted a usability study to determine which phishing strategies proved successful. The best phishing website managed to fool 90% of the participants through its incorporation of padlock in content, Verisign logo and certificate validation seal, and a consumer alert warning.

This is a crucial development with regard to consumer facilitation and the perception held by society about such facilitation. The media, along with policy makers and business professionals, often refer to popular research conducted by, for example, Javelin Strategy & Research. JAVELIN (2005) concluded how consumer awareness of phishing is high. Such a conclusion paints a bit of a deceiving picture of the relationship between phishing awareness and consumer ability. Basically, through proclaiming a high consumer awareness of phishing, Javelin allows the remainder of society to believe consumers can resist the phishing threat. And have the means to do so. This is a potentially misleading conclusion. Awareness itself may be high, but unless consumers realize financial service providers shall only request personal information during the process of a digital transaction, such awareness is worth little in light of the increased sophistication of phishing attacks. As a result, whereas certain rules, such as financial service providers exclusively asking for particular information while in the midst of a transaction, can certainly decrease the likelihood of a successful phishing attack, others which focus on particular indicators cannot compete with the ability of perpetrators of financial identity theft to imitate those same indicators. DANTU *et al*. (2008: 4) acknowledge how:

> "[t]he major factors in any phishing attack are forgery and social engineering. No matter how many authentication techniques we develop phishers always adapt."

Others, however, disagree. BARRETT (Qtd. in Georgia Tech Information Security Center 2009: 8) states how he believes:

> "[...] phishing is a completely preventable crime when you combine technology with education. Our anti-phishing efforts with Yahoo over a 10 month period prevented more than 85 million phishing emails from ever reaching the intended victim. And if we can teach end users some simple rules, it will have a big impact."

DONG *et al*. (2008), on the other hand, reject the value of user education as a means to 'prevent' successful phishing attacks or to solve the problem. Others recognize value in user education, but criticize the ways through which such education is administered (HARLEY & LEE, 2007; MARTIN, 2009). Herein rests perhaps the most promising approach, since, as indicated above, certain simple rules can have a big impact if they focus on the more overarching aspects of digital communication originating from financial service providers.

While phishing remains a popular topic and method for perpetrators of financial identity theft, the increased usage of multiple factor authentication mechanisms [7] obviously diminishes their rate of success. This is since merely obtaining log in information and passwords are insufficient means to access an account, and subsequently complete transactions in an effort to drain the account.

■ Involuntary facilitation

The increased sophistication of phishing proved to be a foreshadowing of a progression into the 'involuntary' state of consumer facilitation. The incorporation of social engineering techniques still heavily relies on the voluntary participation of consumers to surrender their personal information. Such reliance is far from desirable for perpetrators. As a result, perpetrators

[7] For a successful attack on a multiple factor authentication scheme, perpetrators must engage in a man-in-the-browser (MITB) attack, which surpasses merely obtaining the creditentials of the victims. The MITB attack circumvents the two-factor authentication means through placing the perpetrator between the client and the bank. This occurs through the use of Trojan horses. Whereas perpetrators of traditional phishing attacks develop fraudulent websites to obtain the credentials of clients, victims of MITB attacks actually arrive at the legitimate website of their financial service provider. Yet, through interjecting themselves between the client and the bank, perpetrators manage to receive the communication from both sides and divert transactions to different accounts.

managed to develop means to benefit from consumer facilitation without the need of their active participation. While previously introduced methods have not disappeared, the turn to sophisticated methods of involuntary and passive facilitation certainly influences the means, or lack thereof, of consumer control. As LYNCH (2005: 278) notes:

> "[...] recent phishing attacks have become more sophisticated and involve technological devices that may be beyond the ken of even relatively savvy consumers. Some of these attacks, such as those that automatically change a recipient's hostfile, do not even require any action to be taken by the consumer, so she would be hard-pressed to educate herself on how best to protect herself from this type of attack."

The main drive behind involuntary consumer facilitation is the presence of botnets. According to various authors (LEE *et al.* 2007; GRIZZARD *et al*., 2007; HUNTER, 2008), botnets have become one of the largest security threats in contemporary society. HUNTER (2008: 13) explains how "[i]ndeed one of the reasons for the botnet becoming the number one security threat lies not in the innovation of its method of recruitment or attack, but in its resistance to defence." Other authors echo similar concerns (BRAND *et al*., 2007). Its other main attractive feature is its speed. Botnets are:

> "[...] networks of infected end-hosts, called bots, that are under the control of a human operator commonly known as botmaster. While botnets recruit vulnerable machines using methods also utilized by other classes of malware […] their defining characteristic is the use of command and control (C&C) channels" (ABU RAJAB *et al*., 2006: 41).

Through these channels, the botmasters can send out commands to their 'botarmies.' The creation of botarmies is surprisingly easy. IANELLI & HACKWORTH (2007) describe how creating a botnet only requires 'minimal technical skill.' This is predominantly a result of the assistance of the underground community. The community is more than willing to share its vast knowledge through a variety of channels. Seasoned perpetrators, for example, provide training sessions and advice to newcomers through Internet Relay Channels (IRC) (IANELLI & HACKWORTH, 2007). Through the spread of knowledge, seasoned perpetrators can assist in the increasing growth of botnets around the world. The growth leads to a greater challenge for detecting and subsequently taking down botnets.

The introduction of bot software occurred around the start of the millennium (McLAUGHLIN, 2004). Although "Windows internet worms entered the wild in the late 1990s, leading to the automation of malicious code. Bots emerged from this landscape" (DUNHAM & MELNICK, 2008: 1).

Botnets, however, seemed to have gained the most attention during the past few years and have various goals. These fall into three categories, information dispersion, information harvesting and information processing. With regard to financial identity theft, information harvesting and information dispersion are the most relevant goals. GRIZZARD *et al*. (2007: 3) describe how:

> "[…] information dispersion includes sending out spam, creating denial of service attacks, providing false information from illegally controlled sources, etc. The goal of information harvesting includes obtaining identity data, financial data, password data, relationship data (i.e., email addresses of friends), and any other type of data available on the host."

Botmasters create botarmies through the deployment of malware. Perpetrators can manipulate the installation of malware through a variety of channels. They can seduce consumers into downloading an executable file through, for example, a phishing attack or they can send the malware along with another download. More recently, perpetrators have introduced even more undetectable and more involuntary means of installing malware. As PROVOS *et al*. (2008: 1) note:

> "In most cases, a successful exploit results in the automatic installation of a malware binary, also called drive-by-download. The installed malware often enables an adversary to gain remote control over the compromised computer system and can be used to steal sensitive personal information such as banking passwords, to send out spam or to install more malicious executables over time."

Drive-by-downloads are dangerous because detection of such downloads is extremely difficult for consumers. As such these attacks are a significant threat and deserve considerable attention. Through the drive-by-download, perpetrators manage to install malware, which can include keyloggers. These keyloggers function much like cameras and capture all information typed into the computer. This makes the collection of personal information easy and convenient for perpetrators of financial identity theft. Especially, since consumers are most likely unaware of the presence of a keylogger since its installation via the drive-by-download also occurred without the knowledge of the consumer.

The data obtained via keyloggers is subsequently transferred to dropzones. These dropzones are publicly writable directories on an Internet server which serves as an exchange point for keylogger data (HOLZ *et al*., 2008). Important to note, is how:

> "Contrary to conventional wisdom, the malicious pages weren't mostly hosted on the seedier parts of the internet such as adult and gambling websites. While there were a large number of drive-by infections on adult sites, the majority of the malicious data is hosted on sites whose categorisation is more mundane such as finance, home and garden, and business" (POTTER, 2008: 19).

According to SONG *et al*., (2010), drive-by downloads are currently one of the most severe threats for users of the Internet. Moreover, such downloads are presently the number one malware vector (SONG *et al*., 2010).

■ Analysis

What is happening is a shift in various aspects of the potential for consumer facilitation. In previous years, perpetrators appeared to benefit from the 'carelessness' or 'cluelessness' of consumers. Especially those individuals who would toss out important documents without in some way destroying the personal information exposed. Basically, perpetrators could benefit from the unprompted availability of personal information. As financial identity theft, however, moved into the digital realm it appears as though perpetrators smelled the opportunity to hunt for personal information, without running a high risk of getting caught. This allowed them to gain more control over which information they could obtain and from whom.

There is a subsequent movement from voluntary and active to involuntary and passive consumer facilitation. This movement, demonstrated through the continuous evolution of methods used by perpetrators and detected by those trying to counter the problem indicates a diminishing dependability on actual consumer actions. 'Old-fashioned' methods are certainly still in circulation, but the expansion of opportunities allows especially the sophisticated criminals to carry out their operations with the most advanced methods. These perpetrators find an easy 'in' and they can manage to do everything themselves from there on out. Botnets immaculately reflect this current state of affairs. These botnets have become the epitome of involuntary and passive consumer facilitation, especially through the introduction of 'drive-by downloads,' which are according to various sources among the most common methods for spreading malware these days (EGELE *et al*., 2009a).

Whereas with phishing emails, consumers received a prompt to release personal information in an active manner, perpetrators have managed to eliminate this need for active consumer involvement through the introduction of drive-by downloads. The lack of active consumer involvement means consumers may facilitate aspects of financial identity theft without actually having the ability to prevent or control such facilitation. This is a vital aspect to bear in mind with respect to the potential facilitation of financial identity theft, especially in light of countermeasures and the potential for their effectiveness. Certain sources (BRENNER & CLARKE, 2005: 17) appear to neglect the ability factor when they write:

> "We must realize that we are the front line of defense against cybercrime; we must understand that our carelessness could facilitate a successful cyberterrorist or information warfare attack on the critical infrastructures of our society."

This is not about carelessness anymore. Perpetrators have now managed to place their entire operation outside of the reach of consumers, which makes the act of crime repression, let alone prevention, far more challenging. The technological sophistication of current operations requires significant background knowledge which even the savviest consumers often do not posses. They, along with their instruments such as their computers, are used without their knowledge or influence. This movement creates more challenges because old band-aids such as awareness campaigns start to become even less valuable; yet, the consumer remains a primary target of perpetrators of financial identity theft, especially on the electronic superhighway and as such requires attention.

Despite the diminishing amount of consumer control through the evolution in methods used by perpetrators, consumer awareness campaigns remain a popular tool. Consumer education has been a part of the financial identity theft problem since the early days. The United States government incorporated the element of consumer education into its Federal Identity Theft Assumption and Deterrence Act of 1998 through its request for the establishment of a consumer complaint center. This complaint center, which the Federal Trade Commission needed to create, was to dispense consumer education tools in order to make consumers aware and better equipped to combat the increasing threat of financial identity theft. [8] Perpetrators of

[8] See Title 18 USC §5: Centralized Complaint and Consumer Education Service for Victims of Identity Theft which states: "(1) log and acknowledge the receipt of complaints by individuals who certify that they have a reasonable belief that 1 or more of their means of identification (as defined in section 1028 of title 18, United States Code, as amended by this Act) have been

financial identity theft, after all, thrive on the abundance, availability, and accessibility of personal information in order to carry out their operations. Back then, more than a decade ago, such consumer education appeared crucial due to the lack of awareness about the existence of such a crime. The notion of consumer education as a means to raise awareness is evident in various sectors of society (BRUHN, 1997; WOOD & WAHL, 2006) as is empirical research on their effectiveness, or lack thereof (BROWN, 2000). While certainly consumer education is important in an overall action plan to counter financial identity theft, their role and value should not be overestimated.

■ Alternatives

The ineffective nature of consumer awareness campaigns inevitably begs the question as to a more appropriate type of response. This response is necessary because perpetrators of financial identity theft continue to target consumers in order to carry out their activities. And consumers themselves continue to conduct more and more transactions online through the continuous proliferation of electronic services offered by both the public, through electronic government, and the private sector, through electronic commerce and online banking. The focus itself therefore on the individual as the main driver behind the development of solutions is understandable and important, especially since the individual is often considered the weakest link. The main challenge is to focus on the individual yet bear in mind the individual's 'inability' or rather limited ability to conquer the most advanced threats to information security. A glance at the reduction of other crimes provides limited inspiration. VOLLAARD (2009) provides empirical evidence for the success of government intervention in the Netherlands with respect to high-quality locks and burglary-proof windows. Starting in 1999, the government required all new-built homes to have these high-quality locks and burglary-proof windows. Through this government requirement, the Building Code needed to be adjusted accordingly. Vollaard describes how the change in the Building Code reduced the burglary risk in newly built homes by 50 percent. Through these results, Vollaard considers the government regulation for built-in security an effective means to lower crime

assumed, stolen, or otherwise unlawfully acquired in violation of section 1028 of title 18, United States Code, as amended by this Act." (2) provide informational materials to individuals described in paragraph 1.

and also determines how the regulation maintains considerable social benefits. The government regulation also proved more effective than other measures taken to lower levels of crime such as altering the preferences of potential offenders or the preferences of victims for precaution (VOLLAARD, 2009). Such built-in security may also be an attractive option for the threats described in this article. EGELE *et al*. (2009b: 11) elaborate on such a solution when they "[...] propose to have defense mechanisms built into the browser itself to mitigate the threats that arise from drive-by download attacks." Such built-in security takes into consideration the limited ability of consumers to protect themselves against the most recent threats in the digital world. Perhaps the success in the physical world can be transferred to the digital realm.

Even so, as became obvious through the brief reflection on the others above, a comprehensive response to the problem of financial identity theft requires additional measures in an effort to curb the facilitation of the phenomenon. This is precisely because the consumer share only represents a fraction of the problem. One (promising) suggestion, for example, which focuses on the others, is a strict liability approach for financial service providers as a means to develop stronger and direct incentives (HOOFNAGLE, 2009). This focus on incentives is crucial, as Hoofnagle notes, especially since they are "the core of the identity theft problem" (HOOFNAGLE, 2009). The focus on incentives has demonstrated its significance through the introduction of data security breach notification legislation around the world, which in part aims to increase the incentives for organizations to improve their information security practices in an effort to reduce the risk of financial identity theft. Since the facilitation of financial identity theft occurs through the actions of multiple societal actors, its response must also take into consideration these same actors as well as their actions. This article and the suggestion for build-in security are therefore a piece of the puzzle.

■ Conclusion

The introduction of this article provided a brief portrayal of the complexity surrounding the role of *consumers* in the facilitation of financial identity theft. Whereas the threats in the virtual world evolve, the overall discussion about consumers remains focused on the more traditional methods of perpetrators, which means the threat of involuntary facilitation remains largely out of sight.

Those directly involved in the area of information security are acutely aware of the most recent trends and threats, as their valuable research demonstrates. Those in the area of public policy nevertheless appear to have failed to catch on to the changes; at least, if the emphasis on public awareness campaigns geared toward consumers is a reliable indicator. As the above description and analysis demonstrate, the facilitation of consumers is multi-faceted and continuously evolving as perpetrators discover new opportunities. The current trend appears to be a move away from a stage of active and voluntary facilitation to a stage of passive and involuntary facilitation. Through the introduction of botnets and drive-by downloads, perpetrators manage to take advantage of consumers in a largely unnoticeable manner. This shift means that the potential facilitation of consumers is threatening because they might be largely incapable of stopping it, because between *awareness* and *ability* remains a sizeable gap which continues to grow as methods evolve.

References

ABU RAJAB, M., ZARFOSS, J., MONROSE, F. & A. TERZIS (2006): "A Multifaceted Approach to Understanding the Botnet Phenomenon", *Proceedings of ACM SIGCOMM/USENIX Internet Measurement (IMC)*: 41-52.

BENNISON, P.F. & J.P. LASHER (2004): "Data Security Issues Relating to End of Life Equipment", *Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment*.

BILGE, L., STRUFE, T. BALZAROTTI, D. & E. KIRDA (2009): "All Your Contacts Are Belong to Us: Automated Identity Theft Attacks on Social Networks", Paper presented at the *18th International World Wide Web Conference*. Available at: http://www.csd.uoc.gr/~hy558/papers/p551.pdf (last accessed July 14, 2010).

BRAND, M., CHAMPION, A. & D. CHAN (2007): "Combating the Botnet Scourge. Unpublished Manuscript". http://www.cse.ohiostate.edu/~champion/research/Combating_the_Botnet_Scourge.pdf (last accessed July 14, 2010).

BRENNER, S.W. & L.L. CLARKE (2005): Distributed Security: A New Model of Law Enforcement. *SSRN Accepted Papers Series.*

BRUHN, C.M. (1997): "Consumer Concerns: Motivating to Action", *Emerging Infectious Diseases*, Vol. 3 (4): 511-515.

Canadian Internet Policy and Public Interest Clinic (CIPPIC) (2008): "CIPPIC files privacy complaint against Facebook", Press release, May 30, 2008. http://www.cippic.ca/uploads/NewsRelease_30May08.pdf (last accessed July 13, 2010).

CATE, F.H. (2001): "The Privacy Paradox", *76th Annual Winter Newspaper Institute North Carolina Press Association*.

DANG, H. (2008): "The Origins of Social Engineering", *McAfee Security Journal*: 4-8.

DANTU, R., PALLA, S. & J. CANGUSSU (2008): "Classification of Phishers", *Journal of Homeland Security and Emergency Management*, Vol. 5 (1): 1-14.

DAVID, F.M., CHAN, E.M., CARLYLE, J.C. & R.H. CAMPBELL (2008): "Cloaker: Hardware Supported Rootkit Concealment", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA: 296-310.

DEBATIN, B., LOVEJOY, J.P., HORN A-K. & B.N. HUGHES (2009): "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences", *journal of computer-mediated communication*, Vol. 15 (1): 83-108.

DHAMIJA, R., TYGAR, J.D. & M. HEARST (2006): "Why Phishing Works", *Proceedings of the Conference on Human Factors in Computing Systems*: 1-10.

DIRRO, T. & D. KOLBERG (2008): "Germany: Malware learns the language", *Sage*: 22-27.

DONATH, J. & D. BOYD (2004): "Public displays of connection", *BT Technology Journal*, 22: 71-82.

DONG, X., CLARK, J.A. & J. JACOB (2008): "Modelling User-Phishing Interaction", *2008 Conference on Human System Interactions*: 627-632.

DUNHAM, K. & J. MELNICK (2008): *Malicious Bots: An Inside Look*, Auerbach Publications.

EGELE, M., WURZINGER, P., KRUEGEL, C. & E. KIRDA (2009a): "Defending Browsers against Drive-by Downloads: Mitigating Heap-spraying Code Injection Attacks", *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer: 1-19.

EGELE, M., KRUEGEL, C. & E. KIRDA (2009b): "Mitigating Drive-by Download Attacks: Challenges and Open Problems", unpublished manuscript. https://www.iseclab.org/papers/inetsec09.pdf (last accessed July 14, 2010).

FELT, A. & D. EVANS (n.d.): "Privacy Protection for Social Networking APIs". http://www.cs.virginia.edu/felt/privacy/ (last accessed July 13, 2010).

FREDRIKSON, M., MARTIGNONI, L., STINSON, E. & S. J.J. MITCHELL (2008): "A layered architecture for detecting malicious behaviors", paper presented at the *11th International Symposium on Recent Advances in Intrusion Detection (RAID 2008)*.

Georgia Tech Information Security Center, (2009): *Emerging Cyber Threats Report 2009*. http://www.gtisc.gatech.edu/pdf/CyberThreatsReport2009.pdf (last accessed July 14, 2010).

GOLD, S. (2009): "A Newsworthy Year", *Infosecurity*, Vol. 6: 24-28.

GOVERNMENT ACCOUNTABILITY OFFICE (2007): *Personal Information: Data Breaches are Frequent but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*.

GRIMMELMAN, J. (2009): "Saving Facebook", *Iowa Law Review*, Vol. 94: 1137-1206.

GRIZZARD, J.B., SHARMA, V., NUNNERY, C. & B.B. KANG (2007): "Peer-to-Peer botnets: Overview and Case Study", Paper presented at *Usenix Hotbots 2007*.

GROSS, R. & A. ACQUISTI (2005): "Information Revelation and Privacy in Online Social Networks. (The Facebook Case)", pre-proceedings version *ACM Workshop on Privacy in the Electronic Society* (WPES).
http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf
(last accessed July 14, 2010).

GROSSKLAGS, J. & A. ACQUISTI (2007): "When 25 cents is too much: An Experiment on Willingness-To-Sell And Willingness-To-Protect Personal Information", *Workshop on the Economics of Information Security (WEIS*).

HARLEY, D. & A. LEE (2007): "Phish Phodder: is User Education Helping or Hindering?", *17th Virus Bulletin and Conference Proceedings*.

HOLZ, T., ENGELBERTH, M. & F. FREILING (2008): "Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones".
https://www.fehcom.net/fh-frankfurt/vorlesungen/2008_WS/itsec/material/impersonation-attacks-TR.pdf (last accessed July 14, 2010).

HOOFNAGLE, C.J. (2005): "Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors", *in* A. Chander, L. Gelman, M.J. Radin (Eds), *Securing Privacy in the Internet Age*, Stanford, CA: Stanford University Press.

HOOFNAGLE, C.J. (2009): "Internalizing Identity Theft", *UCLA Journal of Law & Technology*, Vol. 13 (2): 1-36.

HUNTER, P. (2008): "PayPal, FBI and others wage war on Botnet armies. Can they succeed?", *Computer Fraud & Security*, Vol. 2008: 13-15.

IANELLI, N. & A. HACKWORTH (2007): "Botnets as a Vehicle for Online Crime", *The International Journal of Forensic Computer Science*: 19-39.

IBRAHIM, Y. (2008): 'The New Risk Communities: Social Networking Sites and Risk', *MCP* 4 (2): 245-252.

JAKOBSSON, M. (2007): "The Human Factor in Phishing", *Privacy & Security of Consumer Information*: 1-19.

Javelin Strategy & Research (2005): "'Phishing: Consumer Behavior and Awareness", Syndicated Report Brochure.

JONES, H. & J.H. SOLTREN (2005): "Facebook: Threats to Privacy", unpublished manuscript.
http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05papers/facebook.pdf
(last accessed July 14, 2010).

LEE, W., WANG, C. & D. DAGON (2007): *Botnet Detection: Countering the Largest Security Threat*, Springer Verlag.

LYNCH, J. (2005): "Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks", *Berkeley Technology Law Journal*, Vol. 20: 259-300.

MARRON, D. (2008): " 'Alter Reality' Governing the Risk of Identity Theft", *British Journal of Crime and Criminology*, Vol. 48 (1): 20-38.

MARTIN, T. (2009): "Phishing for Answers: Factors Influencing a Participant's Ability to Categorize Email", unpublished manuscript. projects.csail.mit.edu.

McLAUGHLIN, L. (2004): "Bot Software Spreads, Causes New Worries", *IEEE Distributed Systems Online*, Vol. 5 (6): 1-5.

MILNE, G.R. (2003): "How Well Do Consumers Protect Themselves?", *Journal of Consumer Affairs*, Vol. 37 (2): 388-402.

MITNICK, K., SIMON, W. & S. WOZNIAK (2002): *The art of deception: controlling the human element of security*, John Wiley & Sons.

OLLMANN, G. (2008): "The evolution of commercial malware development kits and colour-by-numbers custom malware", *Computer Fraud & Security*, Vol. 28: 4-7.

POTTER, B. (2008): How bad is it?, *Network Security*, Vol. 2008: 18-20.

PROVOS, N., MCNAMEE, D., MAVROMMATIS, P., WANG, K. & N. MODADUGU (2008): "The Ghost In The Browser Analysis of Web-Based Malware".
http://www.usenix.org/event/hotbots07/tech/full_papers/provos/provos.pdf
(last accessed July 14, 2010).

RAMASASTRY, A. (2004): "Hooking Phishermen".
http://www.cnn.com/2004/LAW/08/16/ramasastry.phishing (last accessed July 14, 2010).

RILEY, M. (1998): "Statement to the U.S. Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary", *The Identity Theft and Assumption Deterrence Act*, Hearing, May 20, 1998 (Serial 105-779).

SOLOVE, D.J. (2003): "Identity Theft and the Architecture of Vulnerability", *Hastings Law Journal*, Vol. 54: 1227-1273.

SONG, C., ZHUGE, J., HAN, X. & Z. YE (2010): "Preventing Drive-by Download via Inter-Module Communication Monitoring", *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security*: 124-134.

STELTER, B. (2009): "Facebook's Users Ask Who Owns Information", *New York Times*, February 16, 2009.

STONE, D.A. (1989): "Causal Stories and the Formation of Policy Agendas", *Political Science Quarterly*, Vol. 104 (2): 281-300.

STRATER, K. & H. LIPFORD (2008): "Strategies and struggles with privacy in an online social networking community", in *Proceedings of British Computer Society Conference on Human-Computer Interaction*.

STUTZMAN, F. (2006): "An evaluation of identity-sharing behavior in social network communities", Paper presented at the iDMAa and IMS Code Conference, Oxford, Ohio.

SULLIVAN, B. (2005): *Database giant gives access to fake firms: ChoicePoint warns more than 30,000 they may be at risk*. http://www.msnbc.msn.com/id/6969799/ (last accessed July 13, 2010).

VALLI, C. (2004): "Throwing out the enterprise with the hard disk", *2nd Australian Computer, Networks & Information Forensics Conference*, School of Computer and Information Science, Edith Cowan University, Perth, Western Australia: 124-129.

VOLLAARD, B. (2009): "Does regulation of built-in security reduce crime? Evidence from a regression discontinuity approach", paper presented at the *1st Bonn/Paris Workshop on Law and Economics*, September 25-26.

WHITSON, J.R. & K.D. Haggerty (2008): "Identity theft and the care of the virtual self", *Economy and Society*, Vol. 37 (4): 572-594.

WOOD, A.L. & O.F. WAHL (2006): "Evaluating the Effectiveness of a Consumer-Provided Mental Health Recovery Education Presentation", *Psychiatric Rehabilitation Journal*, Vol. 30 (1): 46-53.

The Impact of Public Information on Phishing Attack and Defense

Tyler MOORE & Richard CLAYTON
Harvard University and the University of Cambridge

Abstract: Attackers compromise web servers in order to host fraudulent content, such as malware and phishing websites. While the techniques used to compromise websites are widely discussed and categorized, analysis of the methods used by attackers to identify targets has remained anecdotal. In this paper, we study the use of search engines to locate potentially vulnerable hosts. We present empirical evidence from the logs of websites used for phishing to demonstrate attackers' widespread use of search terms which seek out susceptible web servers. We establish that at least 18% of website compromises are triggered by these searches. Many websites are repeatedly compromised however the root cause of the vulnerability is not addressed. We find that 17% of phishing websites are recompromised within a year, and the rate of recompromise is much higher if they have been identified through web search. By contrast, other public sources of information about phishing websites actually lower recompromise rates. We find that phishing websites placed onto a public blacklist are recompromised less often than websites only known within closed communities. Consequently, we conclude that strategic disclosure of incident information can actually aid defenders if designed properly.

Key words: security economics, online crime, phishing, transparency.

Information security is of growing interest to policy makers as society becomes more dependent on a reliable communications infrastructure. An economic perspective has proven particularly useful in understanding how attackers and defenders operate and identifying ways to influence their behavior (ANDERSON & MOORE, 2006). A flourishing underground economy has emerged, where profit-motivated criminals exploit the Internet's universal addressability and scale to defraud many unsuspecting citizens (MOORE *et al.*, 2009).

Despite the increase in online criminal activity, information on incidents and the losses caused by such crimes have largely remained hidden from public view. There are several reasons for this. First, firms fear negative publicity which may arise if incidents are openly discussed. Second, some argue that disclosing information on incidents actually aids attackers more than it helps defenders. For example, RANSBOTHAM (2010) has found that

vulnerabilities in open-source software are more frequently exploited by attackers than those present in closed-source software.

Yet there are also clear benefits to public disclosure of security incidents. First, while criminals already know how to operate, the 'good' guys could stand to gain from a fuller understanding of how attacks work. This notion – that open discussion of information liable to abuse is valuable – dates to at least the 17th century (WILKINS, 1641). Second, security economics has identified the lack of reliable information on threats as a key barrier to optimal security investment. Better measurement of the frequency and impact of incidents can help firms better allocate security budgets and provide an incentive to improve behavior. Third, bringing incidents to light can help defenders more quickly identify and plug holes.

So is it better to disclose information on security incidents or keep things hidden? The answer to this question is very timely. Some have called on policy makers to require greater transparency from the private sector. Most US states now require companies that lose personally identifiable information to disclose this fact to affected customers. The European Commission is considering revising the Data Protection Directive to adopt a similar requirement. Furthermore, in a report to the European Network and Information Security Agency (ENISA), ANDERSON *et al.* (2008) called for the collection and publication of comprehensive statistics on losses due to electronic crime, as well as data on the levels of malicious traffic emanating from European Internet Service Providers (ISPs). In a report to the US National Academy of Sciences, MOORE (2010) called for the publication of data on computer infection remediation efforts at ISPs, online-banking fraud losses, and control-system incidents at critical infrastructure operators.

Meanwhile, firms have undertaken a number of collaborative efforts to improve security without disclosing results publicly. Google operates a large blacklist of websites currently infected with malware [1], which allows users to verify whether suspected URLs are malicious without revealing the infected websites. ISPs are tinkering with different ways to fight botnets, but to date, most envision arrangements that keep potentially embarrassing details, such as infection rates and time-to-remediation, hidden from public view.

In this paper, we attempt to shed light on the broader questions surrounding public disclosure of information security incidents by empirically

[1] http://code.google.com/apis/safebrowsing/

examining the particular case of phishing. First, we present evidence that attackers do in fact exploit public information about vulnerable web servers to identify new targets. Second, we compare a large public blacklist of phishing URLs to several private ones, finding that websites appearing in the public list are *less* likely to be recompromised at a later date. This suggests that defenders also take advantage of public information on incidents to reduce the exposure to attacks.

Public information in phishing: targeted web search and URL blacklists

Criminals use web servers to host phishing websites that impersonate financial institutions, to send out email spam, to distribute malware, and for many other illegal activities. To reduce costs, and to avoid being traced, the criminals often compromise legitimate systems to host their sites. Extra files – web pages or applications – are simply uploaded onto a server, exploiting insecurities in its software. Typical techniques involve the exploitation of flaws in the software of web-based forums, photo galleries, shopping cart systems, and blogs. The security 'holes' that are taken advantage of are usually widely known, with corrective patches available, but the website owner has failed to bother to apply them.

The criminals use a number of techniques for finding websites to attack. The most commonly described is the use of scanners – probes from machines controlled by the criminals – that check if a remote site has a particular security vulnerability. Once an insecure machine is located, the criminals upload 'rootkits' to ensure that they can recompromise the machine at will (WATSON *et al.,* 2005). They then exploit the machine for their own purposes, or perhaps sell the access rights on the black market (FRANKLIN *et al.*, 2007). If the access obtained is insufficient to deploy a rootkit, or the criminal does not have the skills for this, the website may just have a few extra pages added, which is quite sufficient for a phishing attack.

An alternative approach to scanners, that will also locate vulnerable websites, is to ask an Internet search engine to perform carefully crafted searches. This leverages the scanning which the search engine has already performed, a technique that was dubbed 'Google hacking' by LONG (2004). He was interested not only in how compromisable systems might be located, but also in broader issues such as the discovery of information that was intended to be kept private. Long called the actual searches 'googledorks',

since many of them rely upon extended features of the Google search language, such as 'inurl' or 'intitle'.

In this paper we examine the evidence for the use of 'evil searches': googledorks explicitly intended to locate machines that can be used in phishing attacks. [2] In the following Section we explain our methodology and detail our datasets. Although it is widely accepted that criminals use these techniques, to our knowledge, this is the first study to document their prevalence 'in the wild'. In the 3rd Section we clearly establish 'cause and effect' between the use of evil searches and the compromise of web servers and estimate the extent of evil searching. In the 4th Section we study website *re*-compromise, showing that over 17% of compromised servers host a phishing website on at least one more occasion. We demonstrate a clear linkage between evil search and these recompromises. However, 'findability' is not always bad. We consider the subset of websites that appear in PhishTank's [3] publicly available list of compromised sites and find evidence that being listed in PhishTank substantially decreases the rate of recompromise, demonstrating the positive value of this data to defenders. Finally, we discuss the difficulties in mitigating the damage done by evil searching, and the limitations on using the same searches for doing good.

■ Data collection methodology

We receive a number of disparate 'feeds' of phishing website URLs. We take a feed from a major brand owner, which consists almost exclusively of URLs for the very large number of websites attacking their company, and another feed that is collated from numerous sources by the Anti-Phishing Working Group (APWG) [4]. We fetch data from the volunteer organization 'PhishTank', which specializes in the URLs of phishing websites. We also receive feeds from two 'brand protection' companies who offer specialist phishing website take-down services. These companies amalgamate feeds from numerous other sources, and combine them with data from proprietary phishing email monitoring systems.

---

[2] While we focus on websites used for phishing, once a site is found it could be used for any malevolent purpose (e.g., malware hosting).

[3] http://www.phishtank.com/

[4] http://www.apwg.org/

Table 1 - Categorization of phishing website hosting, October 2007-March 2008

Type of phishing attack	*Count*	*%*
Compromised web servers	88 102	75.8
Free web hosting	20 164	17.4
Rock-phish domains	4 680	4.0
Fast-flux domains	1 672	1.4
'Ark' domains	1 575	1.4
Total	**116 193**	**100.0**

Although by their nature these feeds have substantial overlaps with each other, in practice each contains a number of URLs that we do not receive from any other source. The result is that we believe that our database of URLs is one of the most comprehensive available, and the overwhelming majority of phishing websites will come to our attention. In principle, we could use capture-recapture analysis to estimate what proportion of sites we were unaware of, as attempted by WEAVER & COLLINS (2007). However, the lack of independence between the various feeds makes a robust estimate of coverage impractical to achieve.

Phishing-website demographics

In this paper we consider the phishing websites that first appeared in our feeds during two periods. Primarily, we examine the six-month period from October 2007 through March 2008. When comparing the public PhishTank list to the private lists, we study phishing websites first reported from October 2007 through November 2008. In both cases, we continued to examine the websites for subsequent recompromise through October 2010.

We can split the identified websites into a number of different categories according to the hosting method used. Table 1 summarizes their prevalence for the six-month sample. By far the most common way to host a phishing website is to compromise a web server and load the fraudulent HTML into a directory under the attacker's control. This method accounts for 75.8% of phishing. It is these sites, and the extent to which they can be located by evil searches, that this paper considers.

A simpler, though less popular approach, is to load the phishing web page onto a 'free' web host, where anyone can register and upload pages. Approximately 17.4% of phishing web pages are hosted on free web space, but since there is no 'compromise' here, merely the signing up for a service, we do not consider these sites any further.

We can also distinguish 'rock-phish' and 'fast-flux' attacks, where the attackers use malware infected machines as proxies to hide the location of their web servers (MOORE & CLAYTON, 2007). A further group, we dub 'Ark', appears to use commercial web hosting systems for their sites. All of these attackers use lengthy URLs containing randomly chosen characters. Since the URLs are treated canonically by the use of 'wildcard' DNS entries, we ignore the specious variations and just record canonical domain names. Collectively, these three methods of attack comprise 6.8% of phishing websites. Once again, because the exploitation does not involve the compromise of legitimate web servers, and hence no evil searching is required, we do not consider these attacks any further.

We observe that some entities reporting phishing websites have handled phishing websites appearing on shared hosting providers in a peculiar way. Many smaller firms operate websites with unique domain names, but host the content on a single server shared by many other websites. One consequence of this arrangement is that poorly-configured hosts will resolve paths on any of the domains hosted on the shared server. For example, a phishing website appearing on the URL http://example1.com/~aardvark/bank.html may also appear on http://example2.com/~aardvark/bank.html if both example1.com and example2.com are hosted on the same server. Some firms report as phishing all URLs for every domain hosted on the shared website, even when the attackers have only transmitted phishing emails referring to one domain. We presume this is done either out of an abundance of caution or to inflate the number of reported phishing websites. In any event, we exclude such duplicates from our analysis.

Website-usage summaries

Many websites make use of The Webalizer [5], a program for summarizing web server log files. It creates reports of how many visitors looked at the website, what times of day they came, the most popular pages on the website, and so forth. It is not uncommon to leave these reports 'world-readable' in a standard location on the server, letting anyone inspect their contents.

[5] http://www.mrunix.net/webalizer/

Table 2 - Evil search terms found in Webalizer logs, June 2007–March 2008.

Search type	*Websites*	*Phrases*	*Visits*
Any evil search	204	456	1 207
Vulnerability search	126	206	582
Compromise search	56	99	265
Shell search	47	151	360

From June 2007 through March 2008, we made a daily check for Webalizer reports on each website appearing in our phishing URL feeds. We recorded the available data – which usually covered activity up to and including the previous day. We continued to collect the reports on a daily basis thereafter, allowing us to build up a picture of the usage of sites that had been compromised and used for hosting phishing websites.

In particular, one of the individual sub-reports that Webalizer creates is a list of search terms that have been used to locate the site. It can learn these if a visitor has visited a search engine, typed in particular search terms and then clicked on one of the search results. The first request made to the site that has been searched for will contain a 'Referrer' header in the HTTP request, and this will contain the terms that were originally searched for.

Types of evil search

In total, over our ten-month study, we obtained web usage logs from 2 486 unique websites where phishing pages had been hosted (2.8% of all compromised websites). Of these usage logs, 1 320 (53%) recorded one or more search terms.

We have split these search terms into groups, using a manual process to determine the reason that the search had been made. Many search terms were entirely innocuous and referred to the legitimate content of the site. We also found that many advanced searches were attempts to locate MP3 audio files or pornography – we took no further interest in these searches. However, 204 of the 1 320 websites had been located one or more times using 'evil' search terms, viz: the searches had no obvious innocent purpose, but were attempts to find machines that might be compromised for some sort of criminal activity. We distinguish three distinct types of evil search and summarize their prevalence in Table 2.

Vulnerability searches are intended to pick out a particular program, or version of a program, which the attacker can subvert. Examples of searches

in this group include 'phpizabi v0.848b c1 hfp1' (CVE-2008-0805 is an unrestricted file upload vulnerability) and 'inurl:com_juser' (CVE-2007-6038 concerns the ability of remote attackers to execute arbitrary PHP code on a server).

Compromise searches are intended to locate existing phishing websites, perhaps particular phishing 'kits' with known weaknesses, or just sites that someone else is able to compromise. Examples include 'allintitle: welcome paypal' and 'inurl:www.paypal.com' which both locate PayPal phishing sites.

Shell searches are intended to locate PHP 'shells'. When attackers compromise a machine they often upload a PHP file that permits them to perform further uploads, or to search the machine for credentials – the file is termed a shell since it permits access to the underlying command interpreter (bash, csh, etc.). The shell is often placed in directories where it becomes visible to search engine crawlers, so we see searches such as 'intitle: "index of" r57.php' which looks for a directory listing that includes the r57 shell, or 'c99shell drwxrwx' which looks for a c99 shell that the search engine has caused to run, resulting in the current directory being indexed – the drwxrwx string being present when directories have global access permissions.

■ Evidence for evil searching

So far, we have observed that some phishing websites are located by the use of dubious search terms. We now provide evidence of evil searches leading directly to website compromise. While difficult to attain absolute certainty, we can show that there is a consistent pattern of the evil searches appearing in the web logs at or before the time of reported compromise.

Linking evil search to website compromise

Figure 1 presents an example timeline of compromises, as reconstructed from our collections of phishing URLs and Webalizer logs. On 30 November 2007, a phishing page was reported on the http://chat2me247.com website with the path /stat/q-mono/pro/www.lloydstsb.co.uk/Lloyds_tsb/logon.ibc.html.

Figure 1 - Screenshot and timeline of a phishing website compromised using evil search

1: 2007-11-30 10:31:33 phishing URL reported: http://chat2me247.com /stat/q-mono/pro/www.lloydstsb.co.uk/lloyds_tsb/logon.ibc.html		
2: 2007-11-30	no evil search term	0 hits
3: 2007-12-01	no evil search term	0 hits
4: 2007-12-02	phpizabi v0.415b r3	1 hit
5: 2007-12-03	phpizabi v0.415b r3	1 hit
6: 2007-12-04 21:14:06 phishing URL reported: http://chat2me247.com /seasalter/www.usbank.com/online_banking/index.html		
7: 2007-12-04	phpizabi v0.415b r3	1 hit

We began collecting daily reports of chat2me247.com's Webalizer logs. Initially, no evil search terms were recorded, but two days later, the website received a visit triggered by the search string 'phpizabi v0.415b r3'. Less than 48 hours after that, another phishing page was reported, with the quite different location of /seasalter/www.usbank.com/online_banking/index.html. Given the short period between search and recompromise, it is very likely that the second compromise was triggered by the search. Also, the use of a completely different part of the directory tree suggests that the second attacker was unaware of the first. Figure 1 shows a screenshot from a web search in April 2008 using the same term: chat2me247.com is the 13th result out of 696 returned by Google, indicating an obvious target for any attacker.

We have observed similar patterns on a number of other websites where evil search terms have been used. In 25 cases where the website is compromised multiple times (as with chat2me247.com) we have fetched Webalizer logs in the days immediately preceding the recompromise (because we were studying the effects of the initial compromise). For these sites we are able to ascertain whether the evil search term appears before compromise, on the same day as the compromise, or sometime afterward.

Figure 2 - Timeline of evil web search terms appearing in Webalizer logs

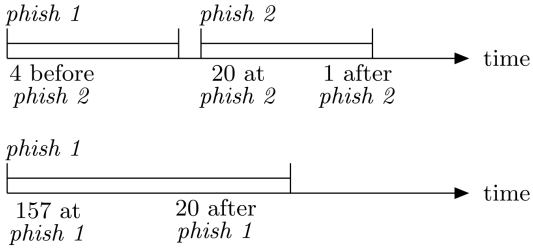


Figure 2 shows a timeline for the 25 websites with Webalizer data before and after a second compromise. For 4 of these websites, the evil search term appeared before the recompromise. For the vast majority (20), the evil search term appeared on the day of the recompromise. In only one case did the evil search term appear only after recompromise. Since most evil terms appear at or before the time of recompromise, this strongly suggests that evil searching is triggering the second compromise. If the evil searches had only occurred after the compromise, then there would have been no connection.

We also examined the Webalizer logs for an additional 177 websites with evil search terms but where the logs only started on, or after, the day of the compromise (see Figure 2). Again, in most cases (157) the evil search term appeared from the time of compromise. Taken together, evil search terms were used at or before website compromise 90% of the time. This is further evidence that evil searching often precedes the compromise of web servers.

Estimating the extent of evil search

We can use phishing websites with Webalizer logs to estimate the overall prevalence of evil search when servers are compromised and used to host phishing websites. Recall that we have obtained search logs for 1 320 phishing websites, and that 204 of these websites include one or more evil search terms in these logs. Frequently, the record shows one visit per evil search. Unfortunately, Webalizer only keeps a record of the top 20 referring search terms. Hence, if a site receives many visitors, any rarely occurring search term will fall outside the top 20. We therefore restrict ourselves to considering just the 1 085 Webalizer-equipped hosts that have low enough traffic so that even search terms with one visit are recorded. Of these hosts, 189 include evil search terms, or approximately 17.6% of the hosts in the sample. Viewed as a sample of all compromised phishing websites, the 95% confidence interval for the true rate of evil searching is (15.3%, 19.8%).

This estimate is only valid if the hosts with Webalizer logs represent a truly random sample. A number of factors may affect its suitability. First, running Webalizer (or programs that it may be bundled with) may affect the likelihood of compromise. We have no evidence for any such effect. Second, sites running Webalizer are not representative of the web server population as a whole. Webalizer typically runs on Unix-like operating systems. Since many compromised servers run on Windows hosts, we cannot directly translate the prevalence of evil web search terms to these other types. Third, evil searches are only recorded in the website logs if the attacker clicks on a search result to visit the site. Using automated tools such as Goolag (Cult of the Dead Cow, 2008), or simple cut and paste operations, hides the search terms. This leads us to underestimate the frequency of evil searches. On balance, we feel sites with Webalizer logs are a fair sample of all websites.

Other evidence for evil searches

There is a substantial amount of circumstantial evidence for the use of evil searches by criminals seeking machines to compromise. Hacker forums regularly contain articles giving 'googledorks', sometimes with further details of how to compromise any sites that are located. However, published evidence of the extent to which this approach has replaced older methods of scanning is hard to find, although the topic is already on the curriculum at one university (LANCOR & WORKMAN, 2007).

LaCour examined a quarter of the URLs in the MarkMonitor phishing URL feed, and was reported (HIGGINS, 2008) as finding that, "75% had been created by using some 750 evil search terms, and the related PHP vulnerabilities". Unfortunately, he was misquoted (LACOUR, 2008). LaCour did collect 750 evil searches from hacker forums, but he did not establish the extent to which these were connected to actual machine compromises.

What LaCour was able to establish from his URL data was that for the October to December 2007 period, 75% of attacks involved machine compromise, 5% were located on free web-hosting and 20% were the categories we have called rock-phish, fast-flux and Ark. These figures are roughly in line with our results in Table 1 above. He then observed, from the paths within URLs, a strong link to PHP vulnerabilities, particularly 'Remote File Inclusion' (RFI) (DAUSIN, 2008). This led him to speculate that evil searches and subsequent RFI attacks may be used in up to 75% of attacks.

■ Phishing website recompromise

Removing phishing websites can be a frustrating task for the banks and other organizations involved in defending against phishing attacks. Not only do new phishing pages appear as fast as old ones are cleared, but the new sites often appear on the web servers that were previously compromised and cleaned up. This occurs whenever the sysadmin removing the offending content only treats the symptoms, without addressing the root problem that enabled the system to be compromised in the first place.

We now provide the first robust data on the *rate* of phishing-website recompromise. Recompromise can serve as a good metric of the effects of public information on both attack and defense. Attackers use evil search terms to discover websites, which could lead to higher recompromise rates. Meanwhile, defenders that identify vulnerable hosts and fix them can lower recompromise rates. In this section we present evidence of how evil search raises the likelihood of recompromise and how public blacklists reduce the incidence of recompromise.

Identifying when a website is recompromised

Websites may be recompromised because the same attacker returns to a machine that they know to be vulnerable. Alternatively, the recompromise may occur because a different attacker finds the machine and independently exploits it using the same vulnerability, or even a second security flaw. We think it unlikely that a single attacker would use multiple security flaws to compromise a machine when just one will do the trick.

The general nature of the security flaw that has been exploited is often quite obvious because the phishing pages have been added within particular parts of the directory structure. For example, when a particular user account is compromised the phishing pages are placed within their file space; when a file upload vulnerability is exploited, the pages are put in sub-directories of the upload repository. However, since it is not always possible to guess what exploit has been used, we instead consider how much time elapses between phishing reports to infer distinct compromises. If two phishing websites are detected on the same server within a day of each other, it is more likely that the same attacker is involved. If, instead, the attacks are months apart, then we believe that is far more likely that the website has been rediscovered by a different attacker. We believe that attackers usually have a relatively small

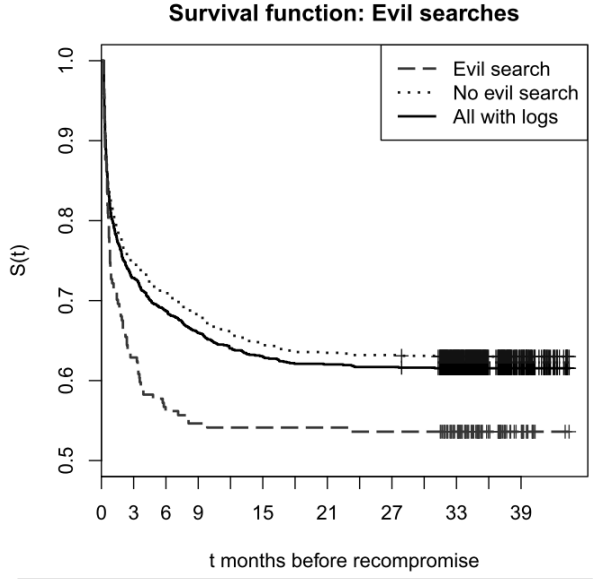
number of machines to exploit at any given moment and are unlikely to keep compromised machines 'for a rainy day' – this is consistent with the short delay that we generally see between detection (evil search logged) and use (phishing website report received).

Our equating of long delays with different attackers is also based on the distribution of recompromises over time. If we treat every phishing site on a particular server as a different attack, whatever the time delay, then we observe a recompromise rate of 20% after 5 weeks, rising to 30% after 24 weeks. If we insist that there is a delay of at least 3 weeks between attacks to consider the event to be a recompromise, then the rates change to 2% after 5 weeks and 15% after 24 weeks. The long term rates of recompromise vary substantially for cut-off points of small numbers of days, which we believe reflects the same attackers coming back to the machine. However, long term rates of recompromise hardly change for cut-off times measured in weeks, which is consistent with all recompromises being new attackers.

An appropriate cut-off point, where there is only a small variation in the results from choosing slightly different values, is to use a gap of one week. We therefore classify a phishing host as recompromised after receiving two reports for the same website that are at least 7 days apart. Using a 7-day window strikes a reasonable balance between ensuring that the compromises are independent without excluding too many potential recompromises from the calculations. As a further sanity check, we note that for 83% of website recompromises occurring after a week or longer, the phishing page is placed in a different directory than previously used. This strongly suggests that different exploits are being applied, and therefore, different attackers are involved.

The rate of website recompromise should only be considered as a function of time. Simply computing the recompromise rate for all phishing websites in the October to March sample would skew the results: websites first compromised on October 1st would have six months to be recompromised, while websites first compromised in late March would have far less time. We handle this in two ways. First, we have continued to check our phishing lists for recompromise through October 2010, so we expect that most recompromises would have occurred by then. However, we cannot state with certainty that a website will never be recompromised. We can only state that it has not yet been recompromised. Fortunately, this is a standard problem in statistics, and we can solve the problem using survival analysis. Websites that have not been recompromised at the end of our study are said to be right-censored.

Figure 3 - Survival analysis shows that websites with evil searches in their logs are recompromised faster and more often than websites without evil searches in their logs



Cox-proportional hazard model
$h(t) = \exp(\alpha + \text{HasEvilSearch}x_1)$

	coef.	exp(coef.)	Std. Err.)	Significance
HasEvilSearch	0.32	1.38	0.12	$p < 0.001$

log-rank test: Q=7.75, $p < 0.01$

Evil searching and recompromise

We established that evil searches can precede website compromise. We now show that the evil searches are linked to much higher rates of recompromise. Figure 3 compares the recompromise rates for hosts in the Webalizer sample. The survival function *S*(*t*) measures the probability that the time between compromises is greater than time *t*. The survival function is similar to a complementary cumulative distribution function, except that the probabilities must be estimated by taking into account censored data points. We use the standard Kaplan-Meier estimator (KAPLAN & MEIER, 1958) to estimate the survival function for recompromise durations, as indicated by the solid line in Figure 3. For instance, *S*(1) = 0.801, which means that 19.9% of websites with search logs are recompromised within one month of the first compromise. The median time before recompromise is undefined, since over half of the phishing websites are not recompromised.

Also noteworthy is that at the maximum time, $S(\max) = 0.615$. Empirical survival estimators such as Kaplan-Meier do not extrapolate the survival distribution beyond the longest observed lifetime, which is just over three years in our sample. What we can discern, nonetheless, is that 61.5% of websites are not recompromised during the span of our investigation.

Figure 3 also plots the survival functions for websites where evil search terms are present in the server logs (dashed line) and where evil search terms are not found (dotted line). Note that $S_{evil}(1) = 0.722$, while $S_{no\ evil}(1) = 0.816$. In other words, 18.4% of websites that have likely not been discovered by evil search are recompromised within one month, compared to 27.8% of websites that have been discovered by evil search. The gap between websites found through evil search and others grows as more time is allowed for recompromise: 37% of websites found through evil search are recompromised within three months, compared to 25% for websites without evil search. After a year, 46% of websites with evil search terms are recompromised, compared to 34% for websites without such terms. We conclude that vulnerable websites found via web search may be repeatedly rediscovered and recompromised until they are finally cleaned up.

But are these differences statistically significant? To compare the recompromise rates of websites with evil search terms in the logs to websites lacking such terms in the logs, we use a Cox proportional hazard model (COX, 1972) of the form:

$$h(t) = \exp(\alpha + \mathrm{HasEvilSearch}x_1)$$

Note that the dependent variable included in the Cox model is the hazard function. The hazard function $h(t)$ expresses the instantaneous risk of 'death' at time t, where in our context 'death' means recompromise. Cox models are used on survival data instead of standard regression models, but the aim is the same as for regression: to measure the effect of different independent factors (in our case, the existence of evil search terms in the server logs) on a dependent variable (in our case, time to recompromise).

The results are presented in the table in Figure 3. The model finds the presence of evil search terms in the server logs to be significantly correlated with shorter time to recompromise. Interpreting the coefficients in Cox models is not quite as straightforward as in standard linear regression; exponentiated coefficients (column 3 in the table) offer the clearest interpretation. The value exp(HasEvilSearch)=1.38 indicates that the presence of evil search terms increases the hazard rate by 38%.

PhishTank and recompromise

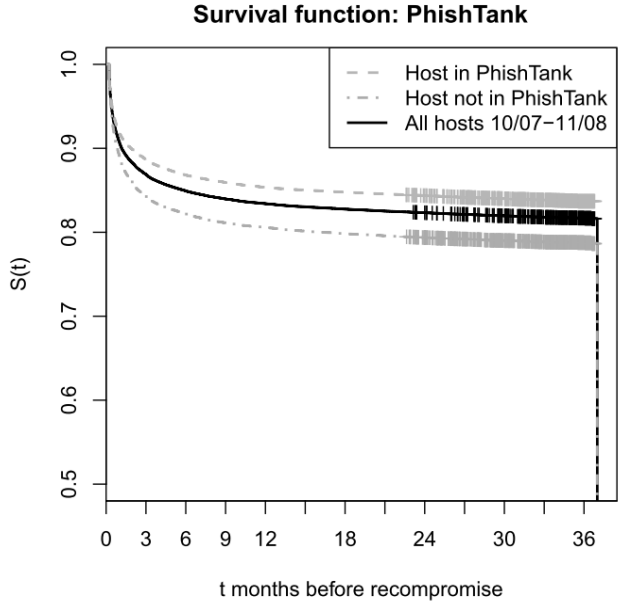
We have shown that attackers use web search to find websites to compromise. We now consider whether they are using public phishing website blacklists as an alternative way to find sites to compromise, or instead if the public nature of the blacklist helps defenders remediate infected hosts.

Phishing-website blacklists provide valuable data for 'phishing toolbars' that block visits to fraudulent websites, and are used by take-down companies to identify websites to remediate. Most blacklists are kept hidden: Google's Safe Browsing API only allows users to verify suspected URLs, while the APWG's blacklist is only available to members. One argument for keeping the lists private is that attackers might mine the lists to identify new targets for recompromise. Another rather different argument is made by the take-down companies who fear that publishing helps competitors to free-ride off their hard work in compiling the lists.

In contrast, PhishTank provides an open source blacklist which is generated and maintained through web-based participation. Users are invited to submit URLs of suspected phishing websites and verify each other's entries. PhishTank argues that by making its blacklist available free of charge, consumers are better protected since more support staff at ISPs and sysadmins are informed of compromised websites in need of cleanup. Other companies sell phishing feeds to aid ISPs in this manner, but PhishTank's free service may be more widely adopted. Furthermore, PhishTank has explicitly designed its blacklist to be helpful to defenders (especially ISP 'abuse teams'), adding features such as searches for phishing sites based on ASNs and RSS feeds of new entries within an ASN.

We set out to empirically test whether publicizing phishing websites helps or harms the cause of defenders, using the recompromise rate as a metric. It is unfair to simply compare recompromise rates for sites PhishTank knows about with those of which it is unaware. While aiming to be comprehensive, in practice PhishTank fails in this aim, and is aware of only 59% of the phishing websites in our collection. Since some of our other URL feeds get some of their data from PhishTank, it is more accurate to view PhishTank as a subset of the phishing URLs we record. So although PhishTank has a roughly even chance of recording a particular phishing incident, there will be further chances to record the host if it is recompromised. This biases PhishTank's record to include a disproportionate number of hosts where multiple compromises occur.

Figure 4 - Survival analysis shows that phishing websites in PhishTank's public blacklist are recompromised less often than phishing websites that only appeared in a private list



Cox-proportional hazard model $h(t) = \exp(\alpha + \text{InPhishTank}x_1)$				
	coef.	exp(coef.)	Std. Err.)	Significance
InPhishTank	−0.29	0.75	0.014	$p < 0.001$
log-rank test: Q=397.4, $p < 0.001$				

Consequently, we apply a fairer test to determine whether a host's appearance in PhishTank makes it more likely to be recompromised. We compare the recompromise rates of new hosts following their first compromise. 100 735 hosts were compromised and used in phishing attacks between October 2007 and November 2008. 59 593 hosts detected by PhishTank during their first reported compromise are compared against 41 142 hosts missed by PhishTank during the first compromise. Because we are interested in measuring the impact of publication in PhishTank, we exclude any hosts that first appeared in PhishTank prior to October 2007.

The results presented in Figure 4 show that new websites appearing in PhishTank are consistently *less* likely to be recompromised than new websites that do not appear in PhishTank. Within one month, PhishTank-aware phishing websites are recompromised 8% of the time, compared to 11% for sites not reported to PhishTank.

A similar trend holds for recompromised websites within 3 months, with recompromise rates around 11% for websites known to PhishTank, compared to 16% for websites not appearing in PhishTank's public list. A roughly five percentage point difference in recompromise rates for websites appearing in PhishTank compared to sites that remain hidden persists as the time allowed for recompromise extends to three years.

Using a Cox proportional hazard model similar to that described above, we again find these differences to be highly statistically significant. The value exp(InPhishTank) =0.75 indicates that publishing phishing websites in PhishTank corresponds to a 25% reduction in the hazard rate.

The black solid line in Figure 4 provides a robust measure of the overall recompromise rate of phishing websites during the 14-month sample. 9% of websites are recompromised within one month of the initial compromise, rising to 13% within 3 months and 17% within one year.

We note that the overall recompromise rate observed here is substantially lower than the recompromise rate observed in Figure 3 when examining only the 1 085 websites where we have access to the Webalizer logs. What might explain the discrepancy in the recompromise rates for the Webalizer sample? One factor is that the sites with Webalizer logs, by definition, were accessible at least once shortly after being reported. This is not the case for all hosts – some phishing websites are completely removed before we are able to access them. [6] Given that the survival function in Figure 4 is based on all 100 000 hosts observed in 14 months, we expect that this measure of overall website recompromise is more reliable.

Based on our data analysis, we conclude that the good offered by PhishTank (better information for defenders) currently outweighs the bad (exploitation of compromised websites by attackers). However, the use of PhishTank by both attackers and defenders might change dynamically over time. Consequently, we believe that continued monitoring is necessary in case attackers begin to leverage PhishTank's public blacklist.

[6] Many sites that are compromised are long-abandoned blogs and image galleries. It is not surprising that a number of these are removed altogether, rather than being cleaned up and left publicly available.

■ Mitigation strategies

Thus far we have demonstrated clear evidence that evil searches are actively used to locate web servers for hosting phishing websites. We have also shown that server re-compromise is often triggered by evil search. Therefore, we now consider how evil searches might be thwarted, in order to make the criminals' task harder. We set out and review a number of mitigation strategies, the first two of which can be implemented locally, whereas the others require action by outside parties. Unfortunately each has drawbacks.

Strategy 1: Obfuscating targeted details

Evil searches could be made less effective if identifying information such as version numbers were removed from web server applications. While this might make it a bit harder for attackers to discover vulnerable websites, it does nothing to secure them.

DAMRON (2003) argued for obfuscation by noting that removing the version numbers from applications is easy for the defender, while adding a significant burden for the attacker. However, defenders also stand to gain from detailed application information, as the presence of a version number can assist sysadmins in keeping track of which of their users continues to run out of date software.

We note that very few of the evil search terms we examined contained explicit version numbers, but merely sought to identify particular programs. The final objection to this obfuscation strategy is that obscuring version numbers still leaves users exposed to 'shotgun' attackers who run all of their exploits against every candidate site without worrying whether or not it is running a vulnerable version.

Strategy 2: Evil search penetration testing

Motivated defenders could run evil searches to locate sites that might be compromised and then warn their owners of the risk they were running. For many evil searches, which only return a handful of exploitable sites amongst many thousands of results, this is unlikely to be an effective scheme. Furthermore, the search results are usually just hints that only indicate the potential for compromise. Confirming suspicions normally requires an active attack, which would be illegal in most jurisdictions.

Strategy 3: Blocking evil search queries

An alternative approach is for the search engines to detect evil searches and suppress the results, or only provide links to law enforcement sites. Given their inherent specificity, constructing a comprehensive and up-to-date blacklist of evil searches is likely to be difficult and costly. Blocking some of the more obvious terms (e.g., those found in Long's popular database [7]) is unlikely to be effective if the terms used by the criminals rapidly evolve. In any event, the search engines are unlikely to have any meaningful incentive to develop and deploy such a list.

Strategy 4: Removing known phishing sites from search results

The low-cost option of removing currently active phishing sites from the search results has almost nothing to recommend it. Search engines suppress results for known child-pornography sites, and Google prevents users from clicking through to sites that are hosting malware (DAY *et al.*, 2008) until they are cleaned up (MAVROMMATIS, 2007). However, phishing presents different circumstances. Malware is placed on high traffic sites where removal from search results is a powerful incentive towards getting it removed, but phishing sites are often on semi-abandoned low traffic sites where the incentive to remove will be limited. Although the evil search will not work while the phishing site is active, the site will be findable again as soon as the fraudulent pages are removed. This approach would also prevent any use of searches by defenders, which means that it does some harm as well as doing little good.

Strategy 5: Lower the reputation of previously phished hosts discoverable by evil search terms

In addition to flagging active phishing URLs, website reputation services such as SiteAdvisor [8] already give a warning for websites that consistently host malicious content. Since we have shown that a substantial proportion of systems that host a phishing website are later recompromised, such services might mark previously compromised hosts as risky. Furthermore, it would be entirely prudent to proactively flag as a much higher risk any hosts used for phishing which can also be found by evil search terms. The

7 http://johnny.ihackstuff.com/ghdb.php

8 http://www.siteadvisor.com/

magnitude of the risk should reflect our finding that about half of these sites will be recompromised within a year of the first compromise.

In contrast to the difficulties in countering evil search, we are optimistic that the use of public blacklists can help defenders in the fight against phishing and beyond. Security firms' refusal to share data on incidents brings with it significant societal costs. For phishing, a refusal to share between take-down firms has greatly slowed down the speed of website removal and increased consumer exposure to attacks (MOORE *et al.* 2009). Openly publishing data on security incidents promises to increase the efficiency of defense at low cost. Unfortunately, the competitive interests of the information security industry may preclude closer cooperation in this manner, so guidance from policy makers may be required.

■ Related work

As indicated earlier, very little academic research has examined the use of search engines to compromise websites. However, researchers have recently begun to recognize the importance of empirically studying electronic crime. THOMAS & MARTIN (2006) and FRANKLIN *et al.* (2007) have characterized the underground economy by monitoring the advertisements of criminals on IRC chatrooms. PROVOS *et al.* (2008) tracked malicious URLs advertising malware, finding that 1.3% of incoming Google search queries returned links to malware-distributing URLs. MOORE & CLAYTON (2007) studied the effectiveness of phishing-website removal by recording site lifetimes. COLLINS *et al.* (2007) used NetFlow data on scanning, spamming and botnet activity to classify unsafe IP address ranges. WARDMAN *et al.* studied common strings in phishing URLs and identified the underlying vulnerabilities (2009). The current work contributes to this literature by measuring the prevalence of evil search terms for compromising websites and the impact on site recompromise.

Another related area of literature is the economics of information security (ANDERSON & MOORE, 2006). One key economic challenge identified by this literature is overcoming asymmetric information. Better measurement of security is needed, from the prevalence of vulnerabilities in competing software to the responsiveness of ISPs in cleaning up infected hosts. Publishing accurate data on website recompromise can identify serial underperformers and highlight opportunities for improvement. Google and

StopBadware [9] publicly disclose infected websites in search resutls, and it has been claimed that this disclosure encourages prompt cleanup (DAY *et al*., 2008). At a policy level, ANDERSON *et al.* (2008) have recommended that regulators collect better data on system compromise and use it to punish unresponsive ISPs.

■ Conclusion

In this paper, we have presented clear evidence that the criminals who are compromising web servers to host phishing websites are using Internet search engines to locate vulnerable machines. We have found direct evidence of these 'evil searches' in 18% of our collection of Webalizer logs from phishing sites, and believe the true prevalence to be even higher.

We have also shown a clear linkage with the recompromise of servers. The general population of phishing websites exhibits a recompromise rate of 17% after one year, but where evil searches are found in the logs, the rate reaches 46%. Although the use of evil searches has been known about anecdotally, this is the first paper to show how prevalent the technique has become, and to report upon the substantial rates of recompromise that currently occur.

In contrast, phishing website URLs that are made public by the PhishTank database currently enjoy a statistically significant reduction in their recompromise rates. This suggests that defenders are able to use information gleaned from the database in order to reduce criminal attacks, and that the sometimes touted benefits of keeping attack data hidden from public view may in fact be harmful.

Other strategies for mitigating evil search that work by limiting attackers' access to information – obfuscating version numbers, filtering search results, blocking evil search queries – we also consider to be flawed. The most promising countermeasure we discuss is to incorporate a website's likelihood of recompromise into the calculation of its reputation. More broadly, our research suggests that policy makers should encourage the publication of more information that can help the Internet's defenders fix problems as they arise.

9 http://www.stopbadware.org/

References

ANDERSON R., BOEHME R., CLAYTON R. & MOORE T. (2008): *Security Economics and the Internal Market*, European Network and Information Security Agency.

ANDERSON R. & MOORE T. (2006): "The Economics of Information Security", *Science*, 314(5799), pp. 610–613.

COLLINS M.P., SHIMEALL T.J., FABER S., JANIES J., WEAVER R., DE SHON M. & KADANE J. (2007): *Using uncleanliness to predict future botnet addresses*, ACM SIGCOMM Conference on Internet Measurement (IMC), pp. 93–104.

COX D.R. (1972): "Regression models and life-tables", *Journal of the Royal Statistics Society*, Series B, 34, pp. 187–220.

CULT OF THE DEAD COW (2008): *Goolag Scanner Specifications*. http://goolag.org/specifications.html

DAMRON J. (2003): *Identifiable fingerprints in network applications*, USENIX; login, 28(6), pp. 16–20.

DAUSIN M. (2008): *PHP File Include Attacks,* Tipping Point. http://dvlabs.tippingpoint.com/blog/2008/02

DAY O., PALMEN B. & GREENSTADT R. (2008): "Reinterpreting the disclosure debate for web infections", in: M.E. Johnson (Ed.), *Managing Information Risk and the Economics of Security*, pp. 179-197, Springer.

FRANKLIN J., PAXSON V., PERRIG A. & SAVAGE S. (2007): "An inquiry into the nature and causes of the wealth of Internet miscreants", 14th ACM Conference on Computer and Communications Security (CCS), pp. 375–388.

HIGGINS K.J. (2008): *Phishers Enlist Google 'Dorks'*, DarkReading. http://www.darkreading.com/document.asp?doc_id=149324

KAPLAN E.L. & MEIER P. (1958): "Nonparametric estimation from incomplete observations", *Journal of the American Statistical Association*, 53, pp. 457–481.

LACOUR J. (2008): Personal communication.

LANCOR L. & WORKMAN R. (2007): "Using Google hacking to enhance defense strategies", 38th SIGCSE Technical Symposium on Computer Science Education, pp. 491–495.

LONG J. (2004): *Google Hacking Mini-Guide*, informIT. http://www.informit.com/articles/article.aspx?p=170880

MAVROMMATIS P. (2007): *Malware Reviews via Webmaster Tools*. http://googlewebmastercentral.blogspot.com/2007/08/malware-reviews-via-webmaster-tools.html

MOORE T. (2010): "The Economics of Cybersecurity: Principles and Policy Options", *International Journal of Critical Infrastructure Protection*, 3(3-4), pp. 103–117.

MOORE T. & CLAYTON R. (2007): "Examining the impact of website take-down on phishing", 2nd Anti-Phishing Working Group eCrime Researcher's Summit (APWG eCrime), pp. 1–13.

MOORE T., CLAYTON R. & ANDERSON R. (2009): "The Economics of Online Crime*", Journal of Economic Perspectives*, 23(3), pp. 3–20.

PROVOS N., MAVROMMATIS P., RAJAB M. & MONROSE F. (2008): "All your iFrames point to us", 17th USENIX Security Symposium, pp. 1–15.

RANSBOTHAM S. (2010): "An Empirical Analysis of Exploitation Attempts based on Vulnerabilities in Open Source Software, 9th Workshop on the Economics of Information Security (WEIS).

THOMAS R. & MARTIN J. (2006): "The underground economy: priceless", USENIX; login, 31(6), pp. 7–16.

WARDMAN B., SHUKLA G. & WARNER G. (2009): *Identifying Vulnerable Websites by Analysis of Common Strings in Phishing URLs*, 4th Anti-Phishing Working Group eCrime Researchers Summit.

WATSON D., HOLZ T. & MUELLER S. (2005): *Know your Enemy: Phishing.* The Honeynet Project & Research Alliance, http://www.honeynet.org/papers/phishing/

WEAVER R. & COLLINS M.P. (2007): *Fishing for phishes: applying capture-recapture methods to estimate phishing populations*, 2nd Anti-Phishing Working Group eCrime Researcher's Summit (APWG eCrime), pp. 14–25.

WILKINS J. (1641): *Mercury: Or the Secret and Swift Messenger*, Maynard and Wilkins, London.

Is Security Lost in the Clouds? (*)

Marjory S. BLUMENTHAL
Georgetown University, Washington, DC

Abstract: "The cloud" can apply to different kinds of services (typically differentiated as platform-as-a-service, infrastructure-as-a-service, and software-as-a-service), and it is the subject of rampant hype about its benefits. This paper draws on extensive readings from the literature (technical, business, and policy) and consultations with a wide range of experts over the past two years. Intended to provide a counter to the cheerleading and a framework for more balanced consideration of public cloud services, in particular, it begins with an exercise in accentuating the negative. In particular, it lays out various ways in which the cloud might be seen as a new platform for malice. The paper enumerates key issues, including kinds and sources of risk (vulnerabilities and threats) associated with providers and/or users and implications for trustworthiness in cloud contexts, as well as the prospects for new technology to counteract apparent sources of risk. It addresses different cloud contexts, and it argues for leveraging cloud concerns to rethink fundamental issues about the nature, handling, and protection of data (which may be stored or processed in the cloud - or not).

Key words: Cloud, privacy, security, cybersecurity, data.

Google's January 2010 news of apparent attacks from China on its Gmail service was a comparatively public alert to the need to rebalance popular thinking about the merits of cloud computing. Touted by its advocates as the next big thing in computing, if not the next incarnation of the Internet, the cloud has a combined market potential that is huge. The market embraces different kinds and extents of cloud service, generally differentiated as (a) the wholly do-it-yourself Infrastructure as a Service (IaaS, such as Amazon Elastic Compute Cloud), (b) the middle ground of Platform as a Service (PaaS, such as Microsoft Azure), and (c) a specific application leveraging the cloud-provider's platform and infrastructure (Software as a Service or SaaS, such as Gmail or

(*) Acknowledgments: This work was supported by a grant from the U.S. Office of Naval Research grant number N000140910037. The ideas were presented at the Telecommunications Policy Research Conference (TPRC), October 2, 2010, Arlington, VA. The author appreciates comments on earlier drafts from Fred B. Schneider, Jim Waldo, Micah Sherr, Jim Fenton, and Scott Charney.

Salesforce.com). [1] Cloud services leverage the technology of virtualization, the use of software to divide up capacity on computing hardware into virtual machines (VMs) associated with specific customers and their data and/or processes. Much of the technology is not new, but the business models are.

Security concerns emerged early for public cloud offerings, which dominate exposure for the general public and for at least smaller enterprise users. [2] By 2008, commercial consortia such as the Cloud Security Alliance (CSA) and conferences for researchers and practitioners were discussing security for the cloud - although implementation of new cloud security ideas lags, [3] at best. This paper responds to these trends by (1) considering the alter ego of the cloud as a platform for malice, and (2) arguing for more syst ematic rethinking about how we handle information.

■ The cloud as a new platform for malice

To balance the hype about the cloud and its benefits, it is a useful thought exercise to consider how we might characterize the cloud as a platform for malice. The negative potential of the cloud spans a range of threats to systems and users.

Perhaps least obvious is the range of concerns associated with the provider: Cloud service providers effectively have access to growing amounts of data and processes. They also have ways of avoiding risk, depending on the type of cloud: users have more control and bear more risk with IaaS offerings than with PaaS or SaaS ones. These two terms-of-service [4] excerpts illustrate how dominant public cloud providers expect their users to bear risks:

---

[1] The cloud is available in various forms (generally described as infrastructure-, platform- or software-as-a-service) offered by different kinds of providers. The National Institute of Standards and Technology (NIST) strove to capture that scope, but cloud definition remains unsettled. See: http://csrc.nist.gov/groups/SNS/cloud-computing/.

[2] Larger enterprises are more likely to be able to afford a private cloud solution, with greater control corresponding to private ownership.

[3] The ideas emerging from research have been characterized, not unreasonably, as "academic" (as opposed to practical) (CACHIN, 2009).

[4] A practical comparison of cloud offerings and the nature of terms of service can be found in WAYNER (2008).

> "Google AppEngine: 5.5. You agree that Google has no responsibility or liability for the deletion or failure to store any Content and other communications maintained or transmitted through use of the Service. You further acknowledge that you are solely responsible for securing and backing up your Application and any Content."
>
> "Amazon Web Services: 7.2. Security. We strive to keep Your Content secure, but cannot guarantee that we will be successful at doing so, given the nature of the Internet. [...] We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications."

Although legal (including contractual) mechanisms are an important vehicle for protecting users, the appropriate balance of interests between providers and users is likely to take time to emerge, given the relative newness of cloud offerings and the relatively rapid development ongoing in the marketplace. Some of the balancing will arise from the ways that the inherent principal-agent problems get worked out (FRIEDMAN & WEST, 2010). But as the termination of Amazon service to WikiLeaks illustrates, many factors - including some exogenous to the user-provider relationship - can be at play, and a provider can act quickly to protect its own interests (FOWLER, 2010). The fact that technology for auditing what goes on in a cloud remains immature at best adds to the handicap burdening the user.

CSA and, in more detail, the European Network and Information Security Agency (ENISA) encourage users to assess their tolerance for the risk associated with specific deployment and service alternatives (ENISA, 2009). That guidance is new, abstract, and lengthy, with ENISA's top ten cloud security risks covering a lot of territory. [5] Meanwhile, there has already been at least one case of a provider shutting down after an egregious error caused substantial customer data-loss (KRIGSMAN, 2008), and there is reputational damage to providers even when lost data is recovered, as in the case of the T-Mobile/Sidekick loss of stored personal data resulting from a server failure (WINGFIELD, 2009).

Errors, of course, are only the beginning. Providers can and do go rogue, and history with outsourcing illuminates both the potential problems and ways of coping. What is different with today's clouds from yesterday's timesharing and outsourcing is the intervening growth in criminal exploitation of the Internet. ENISA suggests that the growth in cloud use implies that

---

[5] Loss of governance, lock-in, isolation failure, compliance risks, management interface compromise, data protection, insecure or incomplete data deletion, malicious insiders. See ENISA (2009).

provider employees are increasingly likely to be targeted by criminal gangs (ENISA, 2009). More generally, insider threat may be a particular concern for the cloud, given the growing value of what goes on in the cloud - including the intellectual property associated with both proprietary algorithms and data - and the expectation that providers will try to provide some security. According to ENISA, there is a medium probability of insider abuse of privilege, but a very high impact if it happens.

Provider-based threat may be subtle. For example, many who focus on privacy are troubled by the content-scanning of e-mail by Google in support of its advertising placement, or the analytical tool provided by Twitter for public analysis of data from its service (for which there is less presumption of privacy than for e-mail). Users trust providers like Google, but they know too little about what might be done with their data to judge the real risks, especially when that data endures for long periods of time on the provider's servers.

Industry structure raises indirect concerns: Given that there appear to be significant economies of scale in the provision of cloud services, how concentrated will cloud supply be, and how might that concentration translate into undesirable competitive conduct? For example, observers already remark on high switching costs: the difficulty of moving data to competing providers has led one commentator to characterize cloud computing as the "Hotel California of technology" (ASAY, 2009). There is also the more straightforward concern that a few dominant players may lead to a smaller number of very large data centers that provide economies of scale for the providers but also large targets for attackers. [6] Further, to the extent that, as in other quarters of the information-technology sector, there is a first-mover advantage, one might expect premature commercialization of cloud technology/ies and the possibility of a stream of adjustments if the offering succeeds, a known route to security problems. This has been seen with social media, where incentives aim providers in directions other than user security and providers capitalize on user assumptions of security:

> "[C]onsider a choice before a hypothetical social network: (1) spend time and money securing personal information against unauthorized access by corrupt insiders, or (2) spend time and money exposing personal information to advertisers to increase the value of their ads

[6] Scott Charney points out (personal communication) that a factor mitigating data-aggregation risks may be the corresponding aggregation of expertise, which in cybersecurity remains comparatively scarce.

> [...] [A] social network must allow information sharing in order to be useful. […] [T]his sharing often depends on the assumption of effective access control. […] [S]ocial networks are fun and easy to use, but their access control schemes are tedious and incomprehensible." (ANDERSON & STAJANO, 2009).

Wittingly or unwittingly, cloud providers may enable new ways for malicious users to hide in the cloud. Consider two possibilities:

- Clouds as cutouts or fronts. The rise of "hacking as a service" suggests that clouds may have the same kind of appeal to the malicious as to the conventional user (POULSEN, 2009). Users select providers based on what they have to offer, and the model of certain kinds of ISP supporting the likes of the organization formerly known as the Russian Business Network is not too hard to extrapolate. [7] That prospect raises questions about how the industry is monitored and the interplay of legal and technical mechanisms. Of course, the law itself may be a kind of enabler, as those who focus on digital rights management argue: If copyright holders can invoke the law to scan a cloud for content that violates their rights, what other kinds of scanning might be done, and by whom? For example, some kinds of monitoring of VMs are being developed to enhance security, [8] yet one can wonder about unintended, malign uses as well. After all, the history of filtering technology points to its being put to uses unintended by their developers (notably for surveillance).

- Clouds as havens. Although today cloud infrastructure is concentrated in the United States, there is a general expectation of it spreading in other countries, not least because of the desires of governments for local infrastructure. This presents the prospect, as Stewart Baker once quipped, of "the cloud fleeing the subpoena," or more generally, the cloud providing a haven for those eluding scrutiny of some kind. Cloud technology development has included the ability to move VMs between servers, a feature intended to enhance reliability and/or to support maintenance. How dramatic might such moves be, and what other uses of such features are possible? Governments have come to appreciate that the physical points of presence of cyberspace provide loci for intervention, which limits the potential for havens (and may also drive policy that limits the efficiency of

---

[7] Stefan Savage was quoted as saying, "For providers, cloud infrastructure is a cyber-criminal's dream world, with plenty of ambiguity and anonymity behind which to hide. What could be more ideal for the cyber-criminal than paying for a huge amount of un¬traceable computing infrastructure with a stolen credit card?" See: SAVAGE (2009).

[8] See, for example, the discussion of secure introspection of VMs as a means of detecting malware: CHRISTODORESCU *et al*. (2009).

cloud services) (GOLDSMITH & WU, 2006). But those limits are as effective as the governments themselves, and investigations of cyber-attacks in China and Eastern Europe demonstrate that there are regions in which providers may operate under a blind or winking surveillance eye.

As the above examples suggest, users present the second, and arguably bigger, source of concern in contemplating the cloud as a platform for malice. Public clouds provide new places for malicious users to hide, and such users may undertake new and undesirable secondary uses of the data and processes originally generated by others. Indeed, perhaps the most striking illustration of possibility comes from recent research that makes clear that the cloud may be less cloudy than represented by advocates. First, there are possibilities for "cloud cartography" - for mapping the multi-tenant terrain, and then for manipulating the process for locating VMs (RISTENPART *et al*., 2009). Second, there are possibilities for monitoring what is going on in the cloud, after one has situated a VM, exploiting side channels (e.g., time-shared caches or keystroke activity) and covert channels (e.g., cache-load measurements where cooperative processes run on different VMs) to support reverse-engineering, infiltration, exfiltration, certain kinds of encryption cracking (GREENBERG, 2009), and other attacks (RISTENPART *et al*., 2009). More generally, technically skilled people are looking for ways to exploit whatever they find. As an analysis of hypervisor vulnerabilities observed, "VMware isn't an additional security layer - it's just another layer to find bugs in" (KORTCHINSKY, 2009).

Google's adoption of encryption for Gmail (the automatic https mode) in response to its Chinese attacks illustrates that defenses must both be available and used - the story of cybersecurity is one of known problems remaining untreated, and known solutions remaining unused. For this reason, optimism that reports of research demonstrating vulnerabilities, threats, and attacks will motivate the deployment of existing technology as well as development of new technology must be bounded.

Meanwhile, the cloud landscape is becoming more complex, which is likely to facilitate malice more quickly than defenses are likely to be mounted. Although the above discussion focused on issues presented by a given cloud, the security challenge is magnified by the prospect of a cloud ecosystem - different kinds of cloud with different kinds of interaction or intersection. At one level, there will be more efforts to facilitate interaction among applications within a given cloud. See, for example, GEAMBASU & LEVY (2009). At the consumer level, this can be seen in efforts to allow individuals to exchange information among different applications offered by a

single provider (such as Google's Gmail, Picasa, and YouTube). For enterprises, there is research into securing query processing for competitive users of cloud-based aggregation services, mitigating threats in the cloud environment relative to conventional Web portals (ZHOU *et al*., 2010). Even more challenging are the possibilities for interactions that bridge clouds, whether public cloud offerings, private clouds established by large organizations, community clouds that support specific groups of users, and/or hybrid clouds combining public and private aspects. Work has begun on standards to foster inter-cloud exchanges, and the debate about openness vs. proprietary technology has begun (OpenCloudManifesto.org, 2009).

The activity on multiple fronts to promote the use of standards and interoperability among clouds points to the potential of an intercloud, a cloud of clouds as an internet is a network of networks. The intercloud today is a topic for speculation. Nelson sketches three scenarios: one with a few separate and unconnected platforms, one with proprietary platforms permitting data but not software interchange, and one that is maximally open and Internet-like, enabling data and software sharing (NELSON, 2009). Not only does an intercloud present technical interoperability challenges, it also raises questions about the interoperability of security policies across services (CREESE & HOPKINS, 2009). Regardless of how the future plays out in terms of structure and technology, it is clear that if it is hard to gauge risk in a given cloud, it is much harder in an interconnected cloud complex, [9] which would increase the potential number of interdependencies. The challenge will be even greater as that complex becomes more international, as is inevitably the case. [10] ENISA, for example, has recommended consideration by national governments and European Union entities of a "European Governmental cloud as a supra national virtual space" featuring interoperability and other standardization (CATTEDDU, 2011).

[9] The Government Accountability Office has suggested that the opportunity for attacks grows with interconnections. See: WILSHUSEN (2010).

[10] International coordination raises the spector of national policies limiting flow of data originating locally, especially data deemed privacy-sensitive. A balkanized, location-aware cloud is to some technologists not a true cloud, inasmuch as the most efficient use of the technology seems to imply ready movement of resources as demand and load evolve in real time.

■ The devil's in the data

The possibilities for the public cloud to be a platform for malice argue for more deliberate thinking about what we entrust to the (public) cloud and what we keep outside of it. Other things equal, [11] economics and the appeal of cloud functionality and dynamic scalability will make the choices steadily harder. They are also likely to change our judgments about what is secure enough - about how we gauge risk. This is evident when it comes to some aspects of personal use of the public cloud. For example, social media applications (e.g., Facebook, Twitter) are fundamentally about sharing information that might otherwise be kept private, and they involve personal decisions that the benefits of sharing outweigh at least some concerns about protecting some kinds of data.

The legal framework is both evolving and highly varied among nations, with varying attention to and protections for privacy [12] and the security of data generally. A risk-averse perspective might deem that whatever is in the public cloud - like whatever is e-mailed - is effectively public. Among the proponents for updating relevant U.S. laws are those (like the Digital Due Process coalition) who note that the laws originated when far less content was communicated or stored, let alone when the technology was less sophisticated. Many are hopeful that evolving technical and legal mechanisms will support higher expectations for data protection. In the meantime, contractual (procurement) mechanisms provide the frontlines for protection, and as discussed above, themselves may be targets for improvement. ENISA, for example, characterizes European perspectives in outlining how service-level agreements can be structured to promote greater security (CATTEDDU, 2011). The discussion in Europe focuses in part on issues arising from data-storage facilities that are outside of a given country or even the region, which is to be expected in the context of efficient, large-scale public cloud operation. The associated jurisdictional concerns provide impetus for efforts to harmonize law and policy across countries, if not globally - which, given the history of efforts to harmonize other instances of cybersecurity law and policy, may be easier said than done.

---

[11] Technology development should drive some progress on security, notwithstanding the challenges discussed above. Notable in the technical community are the attempts to use cryptography (See, for example: KAMARA *et al*. (2010). There is particular excitement about the prospects for homomorphic encryption, which would allow processes to act on encrypted data, but practical challenges to implementing this approach remain significant.

[12] Forrester Research developed an "Interactive Data Protection Heat Map" to illustrate this legal variation. See: http://www.forrester.com/cloudprivacyheatmap.

The strong appeal to the cloud (public or private) for organizations in part reflects the fact that storing data (or hosting applications) in a cloud can be cheaper than local alternatives. This is especially true for enterprises moving away from legacy applications with specialized data structures and associated databases, which require enterprises to address the inconsistencies (data "deconflicting"). Public cloud storage services (e.g., Amazon Simple Storage Service (S3)) can be an efficient substitute for customers building and operating private storage. And most simply, there can be security benefits where the cloud alternative results in less use of removable and therefore easy-to-steal media (e.g., CDs/disks, thumb-drives). But depending on a third party is inherently risky, and that is the point that needs explicit recognition:

> "Placing core business applications and data into the cloud doesn't really have a suitable backup plan unless you're maintaining local backups of all that data and can afford to bring the applications and data back online quickly during an outage - but what's the point of leveraging a cloud if you have to run all that gear locally anyway just in case? [...] If a third-party company falls down on the job and takes your data with them, your only failure was believing that you could safely farm out highly important data and applications and let them deal with it." (VENEZIA, 2010).

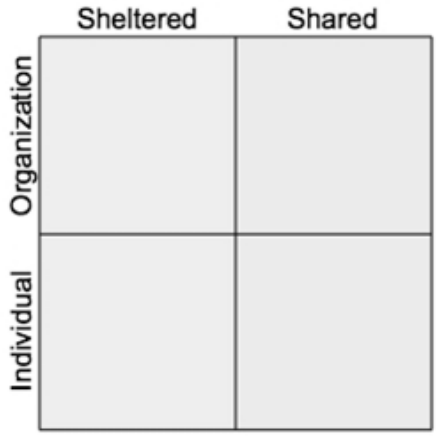
As the above quotation suggests, what data or applications are truly core to an organization (or an individual) needs to be thought through more explicitly than may have been the case with more centralized, local, and/or directly controlled infrastructure.

Given the proliferation of cloud types and applications, it is useful to differentiate the issues by kind of user - individual or enterprise / organization - and by kind of information - nonpublic and sheltered or at least semipublic and shared. See figure 1.

The traditional domain of cybersecurity (and privacy) is represented by the left column in the table - data that individuals and organizations seek to protect or shelter. As discussed in the earlier portions of this paper, the rise of the public cloud raises questions about how well the cloud can shelter data that its owners want sheltered. Because new kinds of applications and associated business models fundamentally involve sharing, even for organizations, there are also new questions about what should be shared and how that determination may evolve. For example, NASA, a U.S. government organization (agency), has a cloud pilot project called Nebula,

which shares scientific data after an initial review. [13] The government of Washington, DC, made a wide variety of data available to the public online, inviting the public to develop its own visualizations and applications using that data and facilitating certain visualizations via Google maps. These examples - and their architects - build on experience with open-source development of software, which has demonstrated benefits and business cases for sharing of technology insights and expertise. It seems that new kinds of data are being made public daily in the public cloud, supporting new uses and new ways of thinking about data, demonstrating benefits from relaxing some expectations for data sheltering.

Figure 1 - Data Status Taxonomy



Meanwhile, the WikiLeaks saga may have two kinds of effect. First, since government data was at issue, a backlash that will roll back recent progress on sharing data among government organizations is likely; it is the most predictable risk-averse response. Second, what it should do is hone thinking about the kind of data that truly must be sheltered "at all costs." Spaulding has remarked on how difficult that can be for governments (and companies) accustomed to treating secrets as assets, even when it is counterproductive:

> "Moreover, a strategy based on keeping information from the prying eyes of your competitors often means not sharing information with those who could use that information to help you. An especially

[13] Currently a private cloud, the system is expected to become a hybrid cloud, with interconnections to other clouds. See: http://nebula.nasa.gov/about/.

> egregious example of this is when intelligence products based entirely on open sources are then stamped "classified." Limiting dissemination of information often means only your friends or potential collaborators don't have it while your enemies do." (SPAULDING, 2010).

Some data compromises seem intolerable and are likely to be so seen indefinitely. These would relate to truly core organizational data or perhaps certain health data for individuals (e.g., re infectious diseases). In theory, homomorphic encryption - a technology for supporting applications to act on data while it is encrypted - could provide an ideal compromise, enabling both sheltering and use of the cloud for applications (IBM Research, Homomorphic Encryption). But the concept, while proven recently in theory, remains short of practical implementation, and even with meaningful implementation other issues would remain. That ENISA (2009) points to the continuing need for research to support end-to-end data confidentiality in the cloud through encryption of search, processing, and tools for social applications is indicative of the limitations of encryption as a tool for sheltering data in the cloud. Under current conditions, the most critical data should remain out of the cloud.

One path forward may involve differentiating and acting upon different stages of the data lifecycle. [14] With the cloud, more data is in transit - up and down-loading or transfers (sometimes across jurisdictions) - and these moves have risks. Provenance of data may become more useful as a tool. Although cloud systems are not designed to store or use provenance or other kinds of meta-data (MUNISWAMY-REDDY *et al*., 2009), research has begun to address the challenge of distributed provenance (since data is distributed across nodes and applications) and the need to protect the integrity of provenance data, itself a potential target for malice (ZHOU *et al*., 2010). And there is new work on different architectural approaches to shape where and by whom information is held and accessed, holding out the promise of more user control (and less provider control) over data that is used in cloud-based applications. [15] Or, using decoy data or otherwise mixing less-valuable with high-value data could build on prior thinking about

---

[14] Encryption is commonly proposed (the Amazon Web Services Terms of Service recommend it, for example, as does CSA for data in transit, at rest, and on back-up media and ENISA as a vehicle for end-to-end data confidentiality). Of course, there is the well-known risk of seeing encryption as a panacea and overlooking the challenges of getting it right, avoiding compromises or end-runs.

[15] For example, the "Lockr" system uses encryption to separate content from other aspects of social networks, supporting choice by social media users over where to store data and whether to disclose their social networks. See: TOOTOONCHIAN, AMIN *et al*. (2009).

honeypots and about how adding noise may make finding the signal - the truly valuable data - harder. Yet another approach is to rethink storing large blocks of data and shift toward seeking out the data that is needed when it is needed. Such a model complements the rise of sensor-systems and sensor-nets, making use of more powerful processing systems in a cloud.

Meanwhile, the cloud adds to longstanding concerns about data durability. In particular, it generates new concerns about phantom deletions. Sometimes it is good to forget, and there is considerable uncertainty about whether or when deletions (of data or algorithms) actually happen. Research on self-destructing data may provide means for data owners to protect against retroactive disclosures and attacks. But 2009-2010 saw an interesting cycle of proposed approach to data self-destruction followed by successful attack and then revision of proposed approach, a familiar cycle of measure-countermeasure that underscores how difficult it is to secure data in a network-accessible system. [16]

■ Conclusions

Cloud computing seems to be advancing inexorably, with active support within the US government based on the economics, the benefits of aggregation, and the need to move beyond legacy systems; within organizations generally based on the economics; and for individuals, based on the appeal of applications such as social media and their interconnection. For both organizations and individuals, mobility - the ability to do transactions on, say, a smart-phone - is a big driver of the public cloud. As we do more and more using cloud technology, we should remember the 2007 cyber attacks on Estonia and the vulnerability that came with having so much online. A cloud-dependent society should be aware of the risks, including how the public cloud can be a platform for malice, rethink key decisions about data, and plan for contingencies. Policy can be expected to lag - it already has - and to be impelled, as it often is, by adverse experiences. One path forward, as suggested by ENISA, may be to begin to see at least some cloud infrastructure, notably that which supports e-government applications and services, as critical information infrastructure,

[16] This history, involving a system called Vanish, began http://vanish.cs.washington.edu/ and continues with "Unvanish" challenges http://z.cs.utexas.edu/users/osa/unvanish/.

subject to protection regimes that do or will exist for critical infrastructures (CATTEDDU, 2011).

If the cloud, specifically the public cloud, is a platform for malice, individuals may have the most to lose. From an individual's point of view, the cloud, if acknowledged at all, enables personal services - Web-based e-mail, social networking, and, increasingly, mobile services and various smart-phone applications. The distance that the public cloud interposes between a user and data and/or processes is hard for most people to understand. Individuals understand even less about the technology choices of entities with which they do business, to which they give their data. Hence they are unlikely to appreciate their full exposure to the public cloud and what that implies for personal or other sensitive information. The occasional system failure - which tends to get a lot of publicity if it involves a consumer system - is a helpful reminder not to trust the public cloud too readily and to be more intentional in the handling of the data one cares most about.

Public cloud providers and their advocates would have people adopt the cliché of putting one's eggs in a basket (the cloud) and watching that basket. For the foreseeable future, it seems that we will continue to have trouble doing the necessary watching. Hence, the sister cliché about not putting all one's eggs in the same basket may be more apt. That is, absent better security mechanisms, being particularly careful about data or processes assigned to the public cloud is important. More attention to the public cloud as a platform for malice should motivate more research into better defenses, alternative architectures for data, meaningful economic comparisons of the costs and risks of traditional enterprise systems and cloud systems, and how to achieve control in the absence of the kind of control that is provided by direct ownership of infrastructure. Given governmental interests in both government uses of the cloud and the impact of everyone's uses of cloud infrastructure on the economy, governments should support relevant research. In the meantime, more awareness of risks associated with the public cloud should stimulate more careful choices about what people do with their data and the updating of legal frameworks for protecting data as information infrastructures evolve.

Might proper attention to security erode the apparent economic advantages of the public cloud? The history of cybersecurity is one of reluctance to pay the cost of security, whether that cost is in obvious dollar terms (e.g., more money for security features) or in utility (e.g., slower performance or loss of certain kinds of functionality); the market for insurance has lagged along with the market for security goods and services.

Although that history suggests a negative answer to the above question, this article has also suggested that it is possible to change the risk equation by changing choices about the use and valuation of data - changing how much of what is deemed to be at risk. It also illuminates a need for research into the economics of different scenarios, addressing alternative industry structures (notably the effects of concentration and different approaches to interconnection), the incidence of different kinds of costs (including for security expertise), and the valuation of different kinds of benefits.

References

ANDERSON, J. & STAJANO, F. (2009): "Not That Kind of Friend: Misleading Divergences Between Online Social Networks and Real-World Social Protocols" (Extended Abstract).
http://www.cl.cam.ac.uk/~fms27/papers/2009-AndersonSta-divergences.pdf
(accessed January 12, 2011).

ASAY, M. (2009): "Is cloud computing the Hotel California of tech?", *CNET News,* October 5. http://news.cnet.com/8301-13505_3-10367052-16.html
(accessed January 12, 2011).

CACHIN, C. (2009): "Trusting the Cloud", *ACM SIGACT News* (40:2), pp. 81-86, June. http://www.zurich.ibm.com/~cca/papers/trust-cloud.pdf
(accessed January 12, 2011).

CATTEDDU, D. (Ed.) (2011): *Security and Resilience in Governmental Clouds*, European Network and Information Security Agency (ENISA), January 17.
http://www.enisa.europa.eu/act/rm/emerging-and-future-risk/deliverables/security-and-resilience-in-governmental-clouds/ (accessed January 25, 2011).

CHRISTODORESCU, M., SAILER, R., SCHALES, D.L., SGANDURRA, D. & ZAMBONI, D. (2009): "Cloud Security Is Not (Just) Virtualization Security", *Proceedings of the 2009 ACM Workshop on Cloud Computing Security*,Chicago, IL.
http://portal.acm.org/citation.cfm?id=1655008.1655022&coll=ACM&dl=AMC&type=series&idx=SERIES320&part=series&WantType=Proceedings&title=CCS (accessed January 12, 2011).

CREESE, S. & HOPKINS, P. (2009): "Global Security Challenges of Cloud Computing – Extended Abstract", *Workshop on Cyber Security and Global Affairs*, August 309, St. Peter's College, Oxford, UK, Draft v0.7, July 27.
http://icc.ite.gmu.edu/sc/Global_Challenges_in_Cloud_Security_v07.pdf
(accessed January 12, 2011).

European Network and Information Security Agency (ENISA) (2009): *Cloud Computing: Benefits, risks and recommendations for information security*, Nov. 20.
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment
(accessed January 12, 2011).

FOWLER, G. (2010): "Amazon Says WikiLeaks Violated Terms of Service", *The Wall Street Journal*, December 3.
http://online.wsj.com/article/SB10001424052748703377504575651321402763304.html
(accessed January 12, 2011).

FRIEDMAN, A.A. & WEST, D.M. (2010): "Privacy and Security in Cloud Computing", *Issues in Technology Innovation*, Number 3, October, Washington, DC: Center for Technology Innovation, Brookings Institution.

GEAMBASU, R., GRIBBLE, S. & LEVY, H. (2009): *CloudViews: Communal Data Sharing in Public Clouds*, USENIX, San Diego, June 15.
http://www.usenix.org/event/hotcloud09/tech/full_papers/geambasu.pdf
(accessed January 12, 2011).

GOLDSMITH, J. & WU, T. (2006): *Who Controls the Internet? Illusions of a Borderless World*, New York: Oxford University Press (USA).

GREENBERG, A. (2009): "Why Cloud Computing Needs More Chaos", *Forbes*, July 30. http://www.forbes.com/2009/07/30/cloud-computing-security-technology-cio-network-cloud-computing.html (accessed January 12, 2011).

KAMARA, S. & LAUTER, K. (2010): *Cryptographic Cloud Storage*, Microsoft Research Cryptography Group, January.
http://research.microsoft.com/en-us/people/klauter/cryptostoragerlcps.pdf
(accessed January 12, 2011).

KORTCHINSKY, K. (2009): "Cloudburst: A VMware Guest to Host Escape Story", Presented at BlackHat USA 2009, Las Vegas.
http://www.blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Cloudburst-SLIDES.pdf (accessed January 12, 2011).

KRIGSMAN, M. (2008): "MediaMax/TheLinkup: When the Cloud Fails", August 27 [Web log post]. http://blogs.zdnet.com/projectfailures/?p=999 (accessed January 12, 2011).

McMILLAN, R. (2010): "China: Google Attack Part of Widespread Spying Effort", *Macworld*, January 13.
http://www.macworld.co.uk/digitallifestyle/news/index.cfm?newsid-28293
(accessed January 12, 2011).

MUNISWAMY-REDDY, K.-K. & SELTZER, M. (2009): "Provenance as First Class Cloud Data", *3rd ACM SIGOPS International Workshop on Large-Scale Distributed Systems and Middleware (LADIS '09)*, Big Sky, MT, October.
http://www.cs.cornell.edu/projects/ladis2009/papers/muniswamy-reddy-ladis2009.pdf
(accessed January 12, 2011).

NELSON, M.R. (2009): "Building an Open Cloud", *Science*, v.324, pp.1656-1657, June 26. http://www.sciencemag.org/cgi/content/short/324/5935/1656?rss=1
(accessed January 12, 2011.

OpenCloudManifesto.org (2009): *Open Cloud Manifesto*.
http://www.opencloudmanifesto.org/open%20cloud%20manifesto.pdf
(accessed January 12, 2011).

POULSEN, K. (2009): "Future of Cybersecurity: Hackers Have Grown Up", *Wired*, July 28. http://www.wired.com/dualperspectives/article/news/2009/07/dp_security_wired0728
(accessed January 12, 2011).

RISTENPART, T., TROMER, E., SHACHAM, H. & SAVAGE, S. (2009): "Hey, You, Get Off of My Cloud", *Proceedings of the ACM Conference on Computer and Communications Security*, Chicago, November 9-13, pp. 199-212. http://portal.acm.org/citation.cfm?id=1653662.1653687&coll=GUIDE&dl=&type=series&idx=SERIES320&part=series&WantType=Proceedings&title=CCS.
(accessed January 12, 2011).

SAVAGE, S. (2009) "Are Cloud Privacy and Security Possible?", *HotCloud09: Workshop on Hot Topics in Cloud ComputingI*, San Diego: USENIX, June 15). http://www.usenix.org/publications/login/2009-10/openpdfs/hotcloud09.pdf (accessed January 12, 2011).

SPAULDING, S. E. (2010,): "No More Secrets: Then What?", *The Huffington Post,* June 24. http://www.huffingtonpost.com/suzanne-e-spaulding/no-more-secrets-then-what_b_623997.html (accessed January 12, 2011).

TOOTOONCHIAN, A., SAROIU, S., GANJALI, Y. & WOLMAN, A. (2009): "Lockr: Better Privacy for Social Networks", *ACM CoNEXT (Conference on Emerging Networking Experiments and Technologies)*, Rome, December 3. http://conferences.sigcomm.org/co-next/2009/program.php (accessed January 12, 2011).

VENEZIA, P. (2010): "McAfee's blunder, cloud computing's fatal flaw", *InfoWorld*, April 26. http://www.infoworld.com/t/software-service/mcafees-blunder-and-cloud-computings-fatal-flaw-742 (accessed January 12, 2011).

WAYNER, P. (2008): "Cloud versus cloud: A guided tour of Amazon, Google, AppNexus, and GoGrid", *InfoWorld*, July 21. http://www.infoworld.com/d/cloud-computing/cloud-versus-cloud-guided-tour-amazon-google-appnexus-and-gogrid-122 (accessed January 12, 2011).

WILSHUSEN, G.C. (2010): "Testimony Before the Committee on Oversight and Government Reform and its Subcommittee on Government Management, Organization, and Procurement, House of Representatives", GAO-1-855T, U.S. Government Accountability Office, July 1. http://www.gao.gov/new.items/d10513.pdf (accessed January 12, 2011). [relates to the May 2010 GAO report, *Information Security: Federal Guidance Needed to Address Control Issues with Implementing Cloud Architectures*. [http://www.gao.gov/new.items/d101513.pdf].

WINGFIELD, N. (2009): "Microsoft, T-mobile Stumble with Sidekick Glitch", *The Wall Street Journal*, October 11. http://online.wsj.com/article/SB10001424052748703790404574467431941990194.html (accessed January 12, 2011).

ZHOU, W., SHERR, M., MARCZAK, W.R., ZHANG, Z., TAO, T., BOON, T.L. & LEE, I. (2010): "Toward a Data-centric View of Cloud Security", Presented at *CloudDB 2010: Second International Workshop on Cloud Data Management*, October 30, Toronto. http://delivery.acm.org/10.1145/1880000/1871934/p25-zhou.pdf?key1=1871934&key2=0028684921&coll=DL&dl=ACM&CFID=5858714&CFTOKEN=74278797 (accessed January 12, 2011).

Web References:

Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2/ (accessed January 12, 2011).

Amazon Simple Storage Service (Amazon S3). http://aws.amazon.com/s3 (accessed January 12, 2011).

Amazon Web Services Customer Agreement. http://aws.amazon.com/agreement/ (accessed January 12, 2011).

Cloud Security Alliance. http://www.cloudsecurityalliance.org/ (accessed January 12, 2011).

Digital Due Process. http://digitaldueprocess.org/index.cfm?objectid=37940370-2551-11DF-8E02000C296BA163 (accessed January 12, 2011).

District of Columbia Government, Office of the Chief Technology Officer. http://data.octo.dc.gov/ (accessed January 12, 2011).

Forrester Research, *Interactive Data Protection Heat Map*. http://forrester.com/cloudprivacyheatmap (accessed on January 12, 2011).

Google App Engine Terms of Service. http://code.google.com/appengine/terms.html (accessed January 12, 2011).

IBM Research, Homomorphic Encryption. http://domino.research.ibm.com/comm/research_projects.nsf/pages/security.homoenc.html (accessed January 12, 2011).

National Institute of Standards and Technology, Computer Security Division, Computer Resource Center. http://csrc.nist.gov/groups/SNS/cloud-computing/ (accessed January 12, 2011).

NEBULA Cloud Computing Platform. http://nebula.nasa.gov/about/ (accessed January 12, 2011).

Salesforce.com. http://www.salesforce.com/ (accessed January 12, 2011).

Twitter. http://search.twitter.com/ (accessed January 12, 2011).

Unvanish – Reconstructing Self-Destructing Data. http://z.cs.utexas.edu/users/osa/unvanish/ (accessed January 12, 2011).

U.S. General Services Administration, Apps.gov. https://apps.gov/cloud/advantage/main/start_page.do (accessed January 12, 2011).

Vanish – Self-Destructing Digital Data. http://vanish.cs.washington.edu/ (accessed January 12, 2011).

Windows Azure: Microsoft's Cloud Services Platform. http://www.microsoft.com/windowsazure/ (accessed January 12, 2011).

Might Governments Clean-up Malware?

Richard CLAYTON
University of Cambridge

Abstract: End-user computers that have become infected with malware are a danger to their owners and to the Internet as a whole. Effective action to clean-up these computers would be extremely desirable, yet the incentives conspire to dissuade ISPs (and others) from acting. This paper proposes a role for government in subsidising the cost of clean-up. The organisations that tender for the government contract will factor in not only the costs of the clean-up, but also the profits they can make from their new consumer relationships. A model is proposed for what the tender price should be – and, by plugging in plausible values, it is shown that the cost to the tax payer of a government scheme could be less than a dollar per person per year; well in line with other public health initiatives.

Key words: malware, cybersecurity, security economics.

This paper looks at the problem of dealing with end-user computers that have, in a variety of ways, become infected with malware. This can sometimes be a serious security issue for the owner of the computer in that malware is often capable of copying confidential files, stealing online banking credentials, or of fraudulently redirecting traffic for financial gain (POLYCHRONAKIS *et al.*, 2008). Additionally, it is almost invariably a security issue for the rest of the Internet, because the infected computer can be combined with others into a 'botnet' which is then used for a large range of criminal activity, from distributed denial of service attacks, through click fraud, to the bulk sending of email spam (MOORE *et al.*, 2009).

Quite clearly, for the Internet to be safer for everyone, 'something must be done' to clean-up the infected computers, but there are a number of barriers to this – mainly to do with incentives. Since the incremental effect is small and responses rare, no-one may be interested in collating lists of botnet members and submitting reports to ISP 'abuse' desks. The ISPs, who must be involved to map IP addresses to customer identities, gain little from handling the reports. They risk alienating customers by simultaneously threatening disconnection and refusing to provide free technical help to deal with the problem. If the report does reach the customer they may not appreciate the need to act and, indeed if the malware does not steal data

from them, inaction makes little difference to their Internet experience. Furthermore, removal of malware costs time and/or money that the end-user may feel that they can put to rather better use.

The financial cost of cleaning up malware can be daunting to many – the perception of it being a complex task, with expert help expensive and essential, goes a long way towards explaining why customers delay malware removal and why ISPs are generally so reluctant to offer any assistance. Of course some malware is extremely trivial to remove, but effective clean-up may be difficult, it may need specialist knowledge or tools, and hence it can indeed be rather costly when done on a one-off basis.

This paper suggests that governments should consider stepping in and subsidising the clean-up – with the analogy being with their role in protecting public health. We believe that such a subsidy will go a long way towards improving the incentive issues – it will no longer be quite such an expensive nuisance for an ISP, or their customer, to learn of a malware problem. Furthermore, by reducing the cost of clean-up to the end-user, it would also make it fairer (and more politically acceptable) to introduce regulations to compel ISPs and customers to ensure that malware is removed in a timely manner, and this in turn may incentivise the reporting of botnet membership.

Clearly, by bulk purchasing clean-up services through a tendering system, a government will be able to reduce the cost of their subsidy. Additionally, since the suppliers should be able to sell further products (anti-virus software would be an obvious example), they should be treating the referrals as a valuable 'sales lead', and tendering lower for the contract as a result. Hence, we argue in this paper, tax-payers will end up with a rather smaller bill than might have been expected at the outset.

The rest of the paper is arranged as follows. In the following Section we discuss the nature of malware in more detail, and outline existing initiatives for malware removal. In the 3rd Section we set out how a government sponsored scheme would work, and in the 4th Section we model the costs and set out the basis for our belief that it will not be as expensive as it might initially seem; and then in the last Section we conclude.

■ Malware

One of the most important ways that criminals make use of the Internet is by distributing malware (malicious software). Ordinary consumers are tricked into running these programs on their computers, and the malware will then compromise online banking sessions, steal passwords for email accounts so they can be exploited for sending spam; and almost invariably cause the computer to join a 'botnet'. The botnet is the 'swiss army knife' of Internet wickedness, allowing criminals to command the individual botnet members to send email spam, participate in advertising 'click fraud', take part in denial of service attacks, or assist in hosting illegal web content.

It was once useful to distinguish different types of malware: a 'worm' is a self-replicating program that spreads from computer to computer without user intervention; a 'virus' attaches itself to a genuine program or email, executing only when the user runs the program or opens the email attachment; and a 'trojan' is a program that claims to do something useful and secretly does something wicked.

These days, these distinctions are of limited value – and the categories have blurred considerably. The main vector of infection at present is visiting websites which contain malware, either because the site was specifically constructed for that purpose, or because a legitimate website was insecure and someone has broken in to plant the malware.

Malware infection

The user will become infected either because they deliberately install software from the website (they may believe a video will not play because their system needs extra components installed) (PROVOS *et al*., 2009), or the site automatically downloads content to exploits flaws in system components (so-called 'drive by' infection (PROVOS *et al*., 2008)).

Users can improve their protection against malware by keeping the software on their computer up-to-date and by never running a program provided by an untrustworthy site. It is also useful to employ anti-virus software with a current list of threats to scan for; although technical advances by the malware writers mean that a great deal of malware now completely fails to be detected by these programs. Using a firewall, or as most consumers will, connecting to the Internet via a network address

translation (NAT) device, has value in protecting against 'worms', albeit these are an unusual type of threat nowadays. Even with a totally secure and up-to-date system, and with impeccable online behaviour, consumers can still become infected with malware through no real fault of their own; perhaps by visiting a reputable site that has been recently compromised, having their browser automatically download malicious content, and thereby falling victim to a '0-day exploit', for which no countermeasure yet exists.

Malware detection

Consumers become aware that their computer is infected with malware in two main ways. The first is by running a malware detector on their computer; the second is by being told that there must be a problem by someone else who has noticed that their computer is behaving inappropriately.

It is often the case that newer versions of anti-virus software will detect malware that has been present on a computer for some time. If a particular malware program is widespread enough, the anti-virus vendors will ensure that their products are able to detect and remove it. However, malware will often arrange for anti-virus updating to fail, so that the anti-virus software continues to run with outdated information of what is to be detected. The user will have a false sense of security – and will continue to operate a compromised computer.

The other major malware detector is Microsoft's 'Malicious Software Removal Tool' (MSRT), part of the monthly 'Windows Update' programme. [1] Microsoft takes steps to detect and deal with malware if it is especially widespread, and/or when there is particular disruption being caused by the botnets that the malware makes possible.

Although the user may not themselves notice that their computer is infected with malware, this may come to light because of the bad things which it is doing are detected elsewhere on the Internet. Occasionally a researcher will be able to enumerate all members of a botnet, or a spam email may be sent to a special 'trap' address which is unused, so that any incoming email must be unsolicited. Whatever the mechanism, the report will be made to the user's ISP, who is then expected to deal with their customer.

1 http://www.microsoft.com/security/malwareremove/

The reason that reports have to be made to the ISP is that for consumers and small businesses there is no publicly available directory to map the IP address of the misbehaving computer into a contact address for its owner. Provided that the correct technical details are given to the ISP, it can use its own private records to work out which customer is causing the problem, and can then communicate with that customer. By convention (CROCKER, 1997), the email address used to reach the ISP is abuse@ispdomain and the personnel who deal with this mailbox are called the ISP abuse team.

Malware removal

Once the user is aware that they have malware on their computer then they should always wish to remove it, and if well-enough informed they will generally do so. This is not only because they want to be good Internet-citizens, but also for self-protection – malware often contains a keylogger, so that important information, such as online banking credentials, is at risk. Once the user has removed the malware, they must immediately change all of their passwords (and additionally all their password recovery questions, to prevent the criminals changing the password straight back).

Some malware is relatively easy for anyone to remove – the Microsoft MSRT program is very effective for the malware it targets; and anti-virus companies provide removal software as well as detection software. However, where a custom removal tool is not available, then generic techniques will be needed, and these can pose difficulties for non-experts. To remove malware, the basic steps are to find all running copies of the program and stop them; remove all system start-up instructions that would cause the malware to run at the next reboot; and delete all copies of the malware on the computer's disk, perhaps disentangling it from legitimate files. Once the malware is gone, the computer may need to be reconfigured because the malware may have disabled the anti-virus system or messed with the firewall settings. In extreme cases it can be simpler to reinstall the entire operating system from scratch, and indeed to avoid lingering problems the super-cautious will do this as a matter of course.

The economics of dealing with malware

Because malware can be difficult for consumers to deal with, they will look for help in cleaning their computers. The main sources of help are

friends and family (some of whom may have technical skills); computer shops, especially the one they bought their computer from; and their ISP. Customers have a strong expectation that their ISP will help them deal with problems whose origin was on the Internet; especially if it was their ISP who relayed the report that they had a malware problem in the first place.

However, ISPs are seldom set up to do generic technical support, and because their support is offered over the phone and by email, removing malware is especially difficult for them. Hence, their response is either to point at 'how to' documents on the Internet, or to suggest contacting the shop where the computer was bought. This can leave customers upset, and they may erroneously conclude that if their ISP does not seem to care whether they remove the malware, then they need not care either.

ISPs are not just extremely reluctant to offer technical support in dealing with malware, but they may be reluctant to handle incoming malware reports either. The provision of Internet access to consumers has become a commodity, and this has meant that ISPs find it essential to compete on price. To keep prices low, they have to eliminate costs from their organisations, and one of the areas where it is very tempting to attempt to save money is within the abuse team. Processing incoming reports, determining which customer is involved and then talking to that customer is expensive – it is widely claimed that just one communication with a customer eats up the profits on that customer for the year. [2]

In principle, the market should deal with ISPs who skimp on abuse team activity. Their customers will be added to third party blacklists. As the

---

[2] The cost of communicating with customers is widely claimed to be comparable with the annual profit they generate, but substantiating this claim turns out to be difficult.
The Help Desk Institute (HDI), a membership/certification organisation for technical support professionals, hosts a 2003 white paper (SHERRILL, 2003) which discusses the complexities of determining what the cost of a call might be. The paper concludes that, "Industry average for cost per call (fully burdened) within the help desk industry is $20–$40". It might be thought that this figure could be on the low side for calls relating to malware, and of course costs will have risen, some seven years later.
The other part of the equation, profit per ISP customer, is hard to assess. Many major ISPs bundle television or telephone services, or provide dial-up services (where the cost base is different from broadband). Earthlink's Q1 2010 figures (EARTHLINK INC, 2010) show a net profit of 25.7 million USD, and that broadband revenue was 59% of their revenue. Assuming (and it is an assumption) that broadband has the same profit margin as dial-up, each of their 900,000 customers yields a profit of 67 USD per annum.
As another data point, McPherson, in a detailed blog post on just this issue – the cost to ISPs in communicating with customers about botnet membership – estimated the profit per annum to be 60 USD and the cost of a support call to be 50 USD (McPHERSON, 2007).
This evidence shows that the "profits for a year" claim is excessive, albeit not greatly so.

number of entries grows, those blacklists will add larger and larger blocks of the ISP's address space. Because these blacklists are used by many spam blocking systems, this will impact the ability of the ISP's customers to have their email delivered, and the general impression of uncleanliness may reduce the amount of free peering that the ISP can negotiate. However, the impact of these measures is relatively small, the process is slow, and there is considerable asymmetry – a large ISP suffers little loss from blocking a small ISP, whereas the small ISP would lose considerably by blocking the large ISP (SERJANTOV & CLAYTON, 2005). Hence one cannot look to the market to ensure optimal expenditure on abuse teams, except over very long timescales.

Malware removal today

In an effort to improve the situation, a number of initiatives are currently under way. For several years Qwest, in the United States has been putting malware infected customers into a 'walled garden' with limited Internet access (QWEST INC, 2007); more recently the largest US cable provider, Comcast, has developed an automated scheme for detecting botnet traffic and notifying customers (Comcast Corporation, 2009). In Australia (HILVERT, 2009), the Netherlands (EVRON, 2009) and Germany (ECO, 2009), ISPs have mutually agreed to deal with botnets; this mutual action means that all ISPs will incur similar costs and so should not be at a competitive disadvantage. In the United Kingdom, an influential all-party Parliamentary group has recommended that the UK ISPs come to a similar mutual agreement (Apcomms, 2009).

Agreeing to handle abuse reports and pass them on to customers is only one part of the solution, because it is also necessary for the customers to have their computers cleaned up and – as just discussed – ISPs will not be enthusiastic about being involved. The most likely customer assistance mechanism will be partnerships with third parties – Comcast has formed a partnership with McAfee for online assistance; and if the computer needs to be worked on by a skilled technician the user will be charged 89.95 USD for this service. Similarly, one of the Luxembourg ISPs recommends a local home visit service that charges Euro 18.95 per quarter hour. [3]

[3] This sounds especially cheap, but the technicians are alleged to be under strict instructions that they are never to be so quick as to avoid charging for less than half an hour. Hence the price is more realistically portrayed as Euro 37.90, approximately 52 USD.

How users actually deal with malware problems is not widely studied. One of the few reliable datapoints we have is the 2006 Consumer Reports 'State of the net' survey of two thousand US households which found that 39% of those surveyed had a problem with a "virus" in the previous two years. Of these, 34% dealt with the problem by reformatting their hard drives, and 8% replaced their computers (Consumer Reports, 2006).

Purchasing a new computer might at first sight appear like a waste of money – but for many users it may well cost little more to purchase a new computer (which will almost certainly be faster and better) than spend a fair proportion of the price in cleaning up the old one. Since the new computer will come with a modern operating system (better able to resist infections), and 'free' anti-virus and anti-spyware products, it is perhaps surprising that the figure was as low as 8%.

■ A government-funded scheme for malware removal?

It is envisaged that a government subsidised scheme for cleaning up computers infected with malware would work as follows:

- The ISP abuse team learns that one of their customers has a computer that is a member of a botnet, which is sending spam, or has some other indication of malware infection.

- The ISP identifies the customer and informs them of their problem. The customer is provided with links to educational material (why their computer might be infected, and why this matters) along with some self-help data for the particular problem they seem to have (e.g. a Conficker-infected customer would be given links to the Conficker Working Group website [4]). The customer is also told the details of the government sponsored clean-up scheme, which they are entitled to use if they wish.

- Ideally, the customer uses freely available tools to clean-up their computer themselves. This will often be the best and most effective thing to do. Large businesses, with in-house IT Departments, are also likely to choose to deal with the problem internally.

- If the customer does not have success with these tools, then a technician will visit their home (or for a lower price, the end-user can visit a

[4] http://www.confickerworkinggroup.org

local shop). Their computer will then be cleaned up for them. There will be a charge for this service, to prevent the 'moral hazard' of consumers deciding not to take any precautions at all, but this charge will be nominal (perhaps 20 USD, or 30 USD for a home visit) with the government paying for the rest of the service.

- The consumer is strongly encouraged to follow 'best practice' advice in installing anti-virus software and ensuring that their software is entirely up-to-date, using programs such as Secunia's 'Personal Software Inspector'. [5] The consumer will also be advised to change their online passwords (and password recovery questions), and to keep an eye on their bank and credit card statements for suspicious transactions.

- The technician's company bills the government to receive the subsidy. This subsidy will be set at a flat rate – in much the same way as health care is often funded (both by governments and by insurance companies), with preset prices for visits to clinics, dental check-ups or the filling of cavities.

If this scheme works as described then there are clear benefits.

There is of course the reduction of infected computers, albeit action in one country may not be significant on a global scale. More important will be the reduction in data loss by citizens – malware usually includes a keylogger – so the quicker that a computer is cleaned up, the less likely that passwords will reach the criminals, and the smaller the time window for exploitation.

Perhaps most importantly of all, the rapid, and hopefully painless, correction of the malware infection should prevent any loss of confidence in using the Internet. Most governments are now looking to the Internet as a way of cutting their own costs in communicating with citizens, and for benefits to the wider economy from having an online population. Keeping confidence in the Internet high is an essential prerequisite to tempting people online, and keeping them there.

Last, but by no means least, if the scheme is effective then other countries (other governments) will look to implement their own version – this means that early adopters will find their international standing enhanced, and their views will carry more weight in this policy area.

---

5 http://secunia.com/vulnerability_scanning/personal/

Who will do the cleaning up?

There are a number of candidates for the task of cleaning up computers (since it will clearly not be done by the politicians or the civil servants!):

- Computer retailers – small computer shops have long been set up for computer repair, and larger companies have increasingly turned to this area as a new source of revenue. The large retailers increasingly offer on-site installation and repair, using brands such as 'Geek Squad'.

- Community groups – many countries provide free computer services for their citizens through local government initiatives, based around councils or communes. These institutions could extend their activities to include malware removal services.

- Utility companies – the utilities (electric, gas, etc.) have moved away from just maintaining their own infrastructure and now provide a range of consumer services such as emergency plumbers, central heating servicing, etc. Training some of their existing operatives to deal not only with gas boilers and leaky taps, but also with the relatively narrow field of malware removal is not entirely far-fetched.

Possible objections to the scheme

Cleaning up malware infected computers cannot be anything other than a good thing. Hence, provided that the work is of adequate technical quality, there is no apparent downside.

However, it is far from obvious that ISPs will be delighted to pass their customers' details on to a third party (the clean-up company) with whom they cannot directly negotiate contractual safeguards. Suppose that a third party not only removed malware, but – for an introduction fee – they persuaded the customer to move to another ISP. It will clearly be appropriate to identify this type of commercial concern early on and to place restrictions on the marketing of directly competitive services, lest ISPs decide that they will not co-operate.

The co-operation of the ISPs is of course essential, because they must handle the initial reports about malware infestation, and must make the initial communication with their customer. The proposed scheme is designed to try and simplify these tasks, and to allow ISPs to use automated systems. An IETF working document written by Comcast engineers (LIVINGOOD *et al.*,

2010) considers nine different ways of communicating with a user – their deployed system currently arranges for the user to see a warning in their web browser (Comcast Corporation, 2009).

Naturally, governments could take themselves out of the loop altogether, and invite companies to set up independent malware cleaning schemes. Clearly, if these companies charge a sufficiently high price to the users for their service then computers will be cleaned and profits will be made. However, the risk is that this approach is far less likely to be successful, and not just because of a lower take-up caused by the non-subsidised price. The involvement of the government makes it easier to cajole ISPs into doing their part, and provides important assurance to citizens that the scheme is bona fide and that quality controls will be in place.

Of course, individual political philosophies differ significantly – so some would see any role at all for government as an anathema. It is only necessary to look around the world at the different approaches that were taken to handling the recent influenza epidemic to see these different philosophies at work.

Even where governments have an interventionist approach to dealing with public health problems (and dealing with malware is much the same sort of issue), many have a lamentable record of purchasing IT services, or preventing fraudulent claims for subsidy, and that might be felt to doom the proposed scheme from the start. However, the government's task within the proposed scheme is restricted to picking out the low tender(s) that are consistent with appropriate quality controls, and thereafter ensuring that the system is appropriately audited by independent experts to prevent any fraud. These limits on involvement are not all that dissimilar to governments' role in many other sectors and so it is reasonable to assume that they will not be especially awful in this particular sphere of action.

A different type of doubt would be whether a government-sponsored scheme for cleaning up malware might reduce the market for technical innovations that would make the scheme unnecessary. Since the government's subsidy is fairly limited (the calculations below suggest that it will be less than a sixth of the total cost), this distortion of the market is not substantial, but it might nevertheless mean that some people will reject the scheme on philosophical grounds.

■ Likely costs of the scheme

In this section we build a model for the costs of the malware removal scheme and make some estimates for what these costs are likely to be. As will be seen, many of the cost estimates are extremely rough. It would be possible to pin some of them down by means of consumer surveys or pilot implementations, and doubtless a government considering this scheme as a policy option would promptly perform such investigations.

The model

The proposed scheme will involve costs for set-up, publicity, monitoring, audit and a wide range of other incidentals. These are not considered here. What is modelled and estimated covers what is likely to be the bulk of the money involved – the costs incurred per reported malware incident.

The model is that a malware report reaches an ISP who passes it on to their customer. Some customers will choose to deal with it themselves, whereas others will take advantage of the government subsidised clean-up scheme. If they choose to use the scheme then they pay a nominal amount for the service, with the remainder of the cost paid by the government.

Using variables for the various values we have:

A proportion, s, of customers receiving reports will use the scheme.

Hence (1 – s) of reports are dealt with outside the scheme 'for free'.

The cost per clean-up event is C, with the end-user paying e and the government paying (C – e).

Hence, the government puts the scheme out for tender. The various organisations who wish to operate the scheme naïvely calculate what they expect *C* to be (including an element of profit), and they put in a tender for (*C* – *e*) and hope to be the low bidder.

There is of course going to be some significant price sensitivity, in that higher values of *e* lead to lower values of *s* – that is end-users may eschew an expensive scheme in favour of a do-it-yourself solution. Also, if *e* is the same as *C* (or higher) then the tenders submitted should all be zero (or negative, viz: organisations compete as to how much they are willing to pay for the contract).

However, there is potentially a lot more going on here than this initial naïve analysis would suggest. Recall the US survey (8% of computers are replaced when there is a problem), and it can be seen that a certain proportion of end-users will not pay *e* at all, but will instead spend a considerable amount on a new computer, giving a profit of *N* to whoever supplied it. Clearly, the higher the value of *e*, the more likely this is to occur.

Furthermore, it will be possible to persuade a sizeable proportion of the end-users who stick with their old computer that, once it has been cleaned up, they should enhance it by the purchase of anti-virus software (or even just a new mouse). Looking further ahead, making sure that all the scheme users are added to appropriate marketing lists should make it more likely in future that they can be sold new products – after all, they will be buying from those nice people who were so good at fixing their computer last year.

These opportunities to profit from supplying other products mean that an organisation which thinks itself capable of doing this type of selling should lower their tender amount to ensure that they get the contract.

Expressing these further items as variables we have:

A proportion, n, purchase a new computer; each yielding a profit of N.

A proportion, v, purchase anti-virus (etc.); each yielding a profit of V.

A proportion, f, will buy in the future, for a (net present value) profit of F.

Putting all of this together:

*Those who choose a new computer bring in a profit of n * N.*

*The others will incur a cost of (1 – n) * (C – e).*

*The profit from selling anti-virus etc. is (1 – n) * (v * V).* [6]

*The profit from future business is f * F.*

*So the tender can be as low as: (1 – n) * (C – e – (v * V)) – (n * N) – (f * F).*

Putting some numbers into the model

It is possible to make some plausible estimates of the numbers in the model, in order to estimate what values are likely to be tendered. We start by assuming that *C* (the clean-up cost) is 70 USD and that *e* (the amount to be paid by the end-user) is to be 30 USD.

6 Note that new computers come bundled with anti-virus.

Objections might reasonably be raised as to where these numbers come from. The examples given above were from the USA (89.95 USD) and Luxembourg (52 USD [7]). Arbitrarily, the mid-point of these two values has been chosen – dubious readers may plug in their own value. Similarly, a reasonable case can be made for *e* being anywhere between 20 USD (much lower and perceptions of moral hazard might make the scheme politically unworkable) and 40 USD (any higher and the scheme hardly involves a subsidy any more). Once again the midpoint (30 USD) has been chosen.

It's also worth observing at this point that *C* is nothing like constant, and for any company doing significant volumes of work (as they might expect to do, having been awarded a government contract for an entire country) there is ample scope for research into automated systems that will result in substantial cost-saving. In particular, the reports flowing through the ISPs are likely to be for large numbers of instances of small numbers of particular malware variants – viz: with a little preparation clean-up can be made very simple for the vast majority of cases. [8]

We know from the US that with e about 90 USD then *n* (the proportion of end-users buying a new computer) is 0.08 and *N* (the profit from such a sale) is about 100 USD. It's hard to say how elastic the demand for a new computer might be, but let us assume that with *e* at 30 USD then *n* is 0.05.

The end-user price of commercial anti-virus products is highly variable and there are many discounts. It is plausible to assume a price of 70 USD and a profit of 42 USD (i.e. 60% trade discount). Hence *V* is 42, and we will assume that, given the circumstances of the sale, there will be a sale in 50% of cases (i.e.: $v = 0.5$). Note that if it was an anti-virus manufacturer offering the service then the discount could be almost 100% rather than 60%.

Finally, we have to estimate the likely future profit from the customer relationship ($f * F$). This isn't easy, but the going price in Google Adwords for

---

[7] In fact this should be 47 USD because there's a kickback of 10% to the ISP for every customer they refer.

[8] To labour this point about economies of scale – there is a substantial difference between the participants in the proposed scheme and how individuals deal with malware infection today. The individual must identify the infection, research the topic, find specialist tools, scan the machine for further problems and work one-on-one to educate the user. The technician from the removal company would arrive knowing what the malware was (from the report that went via the ISP). They'd have the removal tools immediately to hand, they would know if other remediation is needed (and modern malware seldom damages user files), and they could leave the user with booklets, videos, or other professionally produced training material.

'new laptop' is estimated at 1 to 4 USD. It might be assumed that appropriate relationship management would yield just as good a result as buying the most expensive clicks, so we will put this value in at 4 USD. Plugging these values into the model we find that the naïve tender value ($C - e$) would be 40 USD and the more sophisticated one, taking account of all the other factors, would be 11.05 USD.

Quick inspection shows that the most significant contribution to the lowering of the price is the sale of anti-virus software, which is reducing the tender price by 19.95 USD all on its own. Hence there's significant sensitivity here to both the sale price and the conversion ratio: if v was only 33% then the tender price should be 17.70 USD. Quite clearly, this dependency on the sales of extra products alongside the clean-up service means that any organisation contemplating a low tender will have to implement an effective plan to train their technical operatives to be competent at end-user selling.

The final calculation worth doing would be the government's costs. Assuming that an organisation was indeed prepared to tender 11.05 USD per clean-up, what should the government budget to spend? Estimates of malware infection vary considerably from a few percent of the online population, [9] up to scare-mongering 25% plus values. [10] Some of the most reliable data comes from the Microsoft MSRT programme, which expresses infection rates in CCM (computers cleaned per thousand runs of their scanning software). The CCM values are also very variable, but are typically under 10 for first world countries – the USA is 8.6, the UK 4.9 and Finland 2.3. Converting CCM values to overall infection rates is complex, but it does suggest that about 1% of the computer population will need the clean-up

[9] Panda Security provide per country information, which distinguishes types of malware. Presently about 3.1% of UK computers have a serious problem (as do 7.3% of US computers). http://www.pandasecurity.com/img/enc/infection.htm

[10] The 2008 OECD report on Malware (OECD, 2008) contained the sentence "Furthermore, it is estimated that 59 million users in the US have spyware or other types of malware on their computers". News outlets picked up on this, e.g. The Sydney Morning Herald (SYDNEY MORNING HERALD, 2008) who divided the 59 million figure into the US population, and then concluded that around a quarter of US computers were infected (assuming that each person owned one computer). The OECD published a correction in the online copy of the report a few days later. They were actually quoting PEW Internet research on adware/spyware (which is a subtly different threat) from 2005 (which was a while earlier than 2008). The sentence should have read "After hearing descriptions of 'spyware' and 'adware', 43% of internet users, or about 59 million American adults, say they have had one of these programs on their home computer". Of such errors in understanding the meaning of data is misinformation made.

service per month. [11] Assuming that *s* (the proportion of malware infected computers that are dealt with by the service) is 0.5 this means that about 1 in 200 computers will be using the service each month at a cost to the government of 11.05 USD, i.e. the annual cost per computer will be about 66 cents. The total cost clearly depends on the number of actively used computers in the country, which will be roughly equal to the population. Putting this in context, this amount is rather less than the cost of water fluoridisation of about 92 cents (in today's money) per person (Centers for Disease Control and Prevention, 2001), and debates about that particular public health policy are seldom about the cost.

It might finally be noted that there are potential financial assistance opportunities for early adopters. For example, within the European Union, a successful scheme in one Member State is very likely to lead on to deployment elsewhere. It might therefore be possible to seek money for prototyping from central EU funds, particularly if this speeded up any aspect of deployment.

■ Conclusions

It has long been obvious that there are no effective schemes in place for ensuring that end-users who are infected with malware have their computers cleaned up; a conclusion that can also be found within the Conficker "lessons learned" report (Conficker Working Group, 2011).

Some countries are now beginning to see agreements being brokered between ISPs to deal with the problem – addressing some of the negative incentives by agreeing to act in a consistent and, sometimes, collaborative manner. However, there are considerable externalities to malware infection, and hence strong arguments have been made for regulatory action to compel effective malware removal (ANDERSON *et al*., 2008).

This paper has suggested an intermediate scheme – falling short of compulsion – which involves a government subsidy for clean-up schemes.

[11] Microsoft's general approach is to tackle widespread malware infections – viz: the high volume events. The work left over, which needs to be dealt with by the clean-up system, will concern a minority of people who have failed to enable the Microsoft tool, and malware with lower populations. Hence, assuming that Microsoft have already dealt with half the problem is a reasonable working estimate.

Some political philosophies will of course dismiss this out-of-hand, but there are clear analogies with government initiatives for improving public health, which is often seen as an entirely appropriate milieu for government action.

Although subsidies might initially be thought to be substantial, modelling the opportunity to sell extra products alongside the main service suggests that with some plausible assumptions the cost to the public purse could be under a dollar per computer per annum – well in line with other public health initiatives. The proposal cannot of course be seen in isolation. Unlike the initiatives to eradicate smallpox or polio, which tackle a fairly static threat, malware is constantly evolving and so this initiative will need to be accompanied by other initiatives which tackle the criminals. However, given that almost every wickedness on the Internet is underpinned by the use of malware-infected computers – and given the slow and patchy Internet industry response – this is clearly a legitimate area for governments to consider getting involved in, and putting up money to improve.

References

ANDERSON R., BOEHME R., CLAYTON R. & MOORE T. (2008): *Security Economics and the Internal Market*, European Network and Information Security Agency.

Apcomms (2009): *Can we keep our hands off the net?*, All Party Parliamentary Communications Group Inquiry Report.
http://www.apcomms.org.uk/uploads/apComms_Final_Report.pdf

Centers for Disease Control and Prevention (2001): *Recommendations for using fluoride to prevent and control dental caries in the United States*, MMWR Recommendation Report 50 (RR-14): pp. 1–42.

Comcast Corporation (2009): Comcast Unveils Comprehensive "Constant Guard" Internet Security Program. Press Release, 8 Oct 2009.

Conficker Working Group (2011): *Lessons Learned*.
http://www.confickerworkinggroup.org/wiki/uploads/Conficker_Working_Group_Lessons_Learned_17_June_2010_final.pdf

Consumer Reports (2006): *State of the net*.
http://web.archive.org/web/20060820182702/http://www.consumerreports.org/cro/electronics-computers/online-protection-9-06/overview/0609_online-prot_ov1.htm

CROCKER D. (1997): "Mailbox Names for Common Services, Roles and Functions", RFC2142, IETF.

Earthkink Inc. (2010): "EarthLink Announces First Quarter 2010 Results". http://ir.earthlink.net/releasedetail.cfm?ReleaseID=463674

ECO (2009): *Anti-Botnet-Projekt des eco – Verband der deutschen Internetwirtschaft mit Unterstützung des BSI*, Press Release, 10 Dec. http://www.eco.de/verband/202_7268.htm

EVRON G. (2009): "Dutch ISPs Sign Anti-Botnet Treaty", Dark Reading, 29 Sep. *http://www.darkreading.com/blog/227700601/dutch-isps-sign-anti-botnet-treaty.html*

HILVERT J. (2009): "eSecurity code to protect Australians online". http://iia.net.au/index.php/section-blog/90-esecurity-code-for-isps/757-esecurity-code-to-protect-australians-online.html

LIVINGOOD J., MODY N. & O'REIRDAN M. (2011): "Recommendations for the Remediation of Bots in ISP Networks", IETF Internet-Draft, version 10. http://tools.ietf.org/html/draft-oreirdan-mody-bot-remediation-10

McPHERSON D. (2007): "ISP Death By A Thousand Duck Bites", Arbor Networks Security Blog. http://asert.arbornetworks.com/2007/09/isp-death-by-a-thousand-duck-bites/

MOORE T., CLAYTON R. & ANDERSON R. (2009): "The Economics of Online Crime", *Journal of Economic Perspectives*, 23(3), pp. 3–20.

OECD (2008): *Malicious Software (Malware): A Security Threat to the Internet Economy*, Organisation for Economic Co-operation and Development Ministerial Background Report, DSTI/ICCP/REG(2007)5/FINAL.

POLYCHRONAKIS P., MAVROMMATIS P. & PROVOS N. (2008): "Ghost turns Zombie: Exploring the Life Cycle of Web-based Malware", *1st Usenix Workshop on Large-Scale Exploits and Emergent Threats* (LEET), pp. 1–8.

PROVOS N., MAVROMMATIS P., RAJAB M.A. & MONROSE F. (2008): "All your iFRAMEs point to Us", *17th USENIX Security Symposium*, pp. 1–15.

PROVOS N., RAJAB M.A. & MAVROMMATIS P. (2008): "Cybercrime 2.0: when the cloud turns dark", Comm. ACM, 52(4), pp. 42–47.

QWEST INC. (2007): "Qwest Customer Internet Protection Program Increases Security For Broadband Customers, Combats Spread Of Viruses And Malware", Press Release, Oct 2.

SERJANTOV A. & CLAYTON R. (2005): "Modelling Incentives for Email Blocking Strategies", *4th Annual Workshop on Economics and Information Security* (WEIS05).

SHERRILL K. (2003): "Cost Per Call: Are we comparing apples to apples?", Help Desk Institute Library. http://www.thinkhdi.com/library/deliverfile.aspx?filecontentid=234

Sydney Morning Herald (2008): "A quarter of US PCs infected with malware: OECD", 2 June. http://news.smh.com.au/world/zombies-and-botnets-oecd-warns-of-hidden-armies-in-cyber-wars-20080601-2kel.html

Cybersecurity at European Level: The Role of Information Availability

Fabio BISOGNI, Simona CAVALLINI, Sara DI TROCCHIO
Fondazione FORMIT, Rome, Italy

Abstract: This paper aims to analyse the cybersecurity issue, taking into account the investment behaviour of operators managing ICT infrastructures and providing ICT services and trying to investigate which kind of actions must be implemented to increase their security level. The main finding is that information availability plays a key role in the cyber-risk assessment for ICT operators and is also critical for improving the cybersecurity behaviour of other ICT stakeholders. From the ICT operator perspective, lack of information affects the real perception of cyber-threat occurrence, the vulnerability of his system and the potential loss in case of cyber-attack. As ICT systems have to be regarded as a network of different actor categories, regulation efforts at the European level should focus on spreading information among all ICT stakeholders in order to reduce failures of the cybersecurity market. Virtuous behaviour of other ICT stakeholders may increase the level of cybersecurity also by reducing the current lack of information on cyber-attacks of ICT operators and pushing their investments.

Key words: cybersecurity, information lacking, risk assessment, investment behaviour, European cybersecurity policy.

The first years of the 21st century have been characterized by the appearance of brand new threats in the most developed western economies. Terrorist attacks such as those of New York 2001, Madrid 2004, London 2005, Mumbai 2006 and 2008 have illustrated the relevance of the issue of infrastructure security and citizens' safety [1]. In addition, the development of information and communication technologies (ICT) and their pervasiveness in everyday life have created new opportunities for malicious attacks with huge potential impact on social and economic services. The diffusion of computers among citizens throughout the globe and the

[1] Although security and safety are often used as synonymous, in this paper safety is strictly related to assets (such as infrastructures managed by operators) and their components (such as computer servers). Safety is intended as the preservation of health. Impacts of a terroristic attack in terms of security can be measured in economic losses and public effects, impacts in terms of safety through casualties. For a review of the different security and safety definitions see CAMBACÉDÈS & CHAUDET (2010).

automation of productive services have created a world-wide network in which all kinds of users operate. On the one side, a complex set of interconnected networks allows real-time data exchange thus increasing the efficiency of communications, but, on the other side, it increases the risk of accessibility to confidential information and to critical systems able to control physical assets. In particular, the importance and the need to protect information infrastructures have largely increased in the political debate of global security over the last decade. Because most critical infrastructure services rely on ICT systems remotely accessible via public networks that are vulnerable to cyber-attacks, the potential damages in terms of economic effects, public effects and casualties [2] may be amplified at the societal level.

The case of Stuxnet, a Windows-specific computer worm discovered in June 2010 able to spy and reprogram ICT systems of critical industrial infrastructure, shows that industrial processes controlled and monitored through Supervisory Control And Data Acquisition (SCADA) computer systems are affected by vulnerabilities that can be exploited. The specific targets of this particular cyber-attack were nuclear facilities in Natanz and the Bushehr Nuclear Power Plants in Iran, showing a narrow distance between virtual effects and potential physical damages (KEIZER, 2010). To this purpose, the necessity for prevention of and protection against cyber-crime has arisen once remotely-managed control systems have become a clear target for malicious attackers. The growing awareness about global cyber-threats has increased the need for accurate information about their features, ICT infrastructures vulnerabilities, cyber-risk management approaches and socio-economic effects of successful cyber-attacks.

The current European policy debate and the most advanced studies [3] on the economics of cybersecurity have recently included the issue of responsibilities of protection and the attribution of the associated costs (KOLFAL *et al*., 2010). To this aim, different actor categories with specific roles in cybersecurity can be identified: citizens, public bodies/authorities,

---

[2] Within the framework of the European Programme for Critical Infrastructure Protection (EPCIP), the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection qualifies which kind of impacts should be investigated. The policy focus is on economic effects (e.g. economic loss, degradation of services) and social effects (e.g. potential number of fatalities, disruption of daily life, loss of public services).

[3] For example, the study for the "Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – CIIS", (CAVALLINI *et al*., 2010) carried out for the DG Information Society and Media of the European Commission.

ICT operators, operators of other critical infrastructures. Citizens, intended as general private end-users, carry the social interest in using ICT infrastructures and services provided by other critical infrastructures. In the event of a cyber-attack on the mentioned infrastructures, the society, as the aggregation of all citizens, would suffer larger negative externalities since it has less direct capacity to contain cyber-crime effects. Public bodies and authorities have the main goal to protect the social interest and can directly support prevention, protection and reaction to cyber-attacks through regulation (top-down approach) [4] or action (bottom-up approach) [5] that encourage all stakeholders to bear part of the cybersecurity costs. ICT operators, intended as operators who directly manage Internet connections (such as Internet Service Providers and telecom operators), are directly involved in the cybersecurity issues and considered the most liable actors. Due to the fact that they manage ICT infrastructures and connected services, in the case of a successful cyber-attack, they would suffer the most direct consequences, but wide damages would also affect the rest of society. Operators of other critical infrastructures in the cybersecurity framework have a double damage-spreading role that has recently increased their responsibilities. On the one hand, if an operator of a critical infrastructure affecting ICT operators (e.g. an electricity provider) becomes a cyber-crime target, its failure may cause a large disruption of ICT services. On the other hand, if an ICT operator suffers a cyber-attack cascading effects on other critical infrastructures (e.g. hospitals) might be spread to the entire society with relevant impacts for non-ICT users.

This paper faces the issue of the relationship between security investments and costs suffered as consequence of cyber-attacks. Starting from the analysis of the cybersecurity investment behaviour of ICT operators, the paper aims at proposing effective actions to public decision makers able to overpass potential market failures related to the security market of the cyber-world. The proposed model concerns the lack of information that characterizes ICT operators' investments in cybersecurity and provides indication on policy actions that may improve the cybersecurity level involving all the identified actor categories.

---

[4] An important aspect of the governments' response to cyber-crime is the development of laws and rules focused on the improvement of security provisions, the readiness in dealing with catastrophic incidents and the capacity to assure prompt recovery after incidents.

[5] A bottom-up approach relies on the initiative of each single actor to protect himself from cyber-attack effects. Governments can indirectly support this process, defining and setting up a clear liability framework and assigning negative externality costs to the specific categories of involved actors.

The next Section describes the economic framework of cybersecurity and how ICT operators would behave in terms of optimal investment behaviour with complete information on cyber-attacks. The following Section depicts the effective investment behaviour of ICT operators who assess cyber-risk with a lack of information. The Section after briefly summarizes the current institutional and regulation framework at the European level for increasing the availability of cybercrime-related information and provides suggestions to European policy makers on how cybersecurity could be increased not only directly involving the ICT operators. The concluding remarks summarize the main findings and suggest new investigation areas for the economics of cybersecurity.

■ The theoretical framework: the optimal level of cybersecurity

In recent years, with the spreading of information and communication services and the emergence of related threats and vulnerabilities, cybersecurity has evolved from a valuable economic good to a societal need. Business users, public authorities and citizens demand secure information systems, and ICT operators have set up investment strategies in order to provide ICT services at a suitable level of security. In the theoretical framework, the societal demand of cybersecurity provides an indication to ICT operators of their costs in terms of losses related to the lack of security and, consequently, the needed amount of investment. For an ICT operator, the optimal level of investment in cybersecurity is the level providing a protection that minimizes its expected costs in case of cyber attack events. This optimal solution occurs when marginal security investments equal the expected marginal costs that the operator would sustain. Nevertheless, market failures may impede the pursuit of the optimal level of investments and the consequent optimal level of security (BRUCK *et al*., 2006,).

Approaching a similar issue, GORDON & LOEB (2002) defined a model to determine the optimal amount of investment needed to protect a given set of information. Considering the vulnerability of an information system, the main finding is a biased behavior on the part of the operator: a firm spends only a small fraction (approximately 37%) of the potential loss that would result in case of a breach occurrence. According to this model, the level of cybersecurity investment of the ICT operator can be defined on the basis of the expected loss *E(L)* associated with its available information set, with *L*

representing the incurred loss in case of cyber-attack. The expected loss *E(L)* is the result of the probability of the threat occurrence, *t*, times the vulnerability of the system, *v* (which is the probability of threat effectiveness), and the potential loss due to the threat realization, λ [6]. In order to avoid huge unexpected losses, the ICT operator sets up a level of security *S* as a function of the implemented security investments I_s and of the level of vulnerability of the system *v*.

To illustrate the investment choice of Gordon and Loeb's model, the relationship between of the optimal investment choice of the ICT operator and loss can be drawn (Figure 1) with the level of investment in security I_s on the x-axis and with the expected loss *E(L)* on the y-axis. As common sense suggests, a lower level of investment corresponds to a higher expected loss in case of cyber-attacks and vice-versa. The ICT operator chooses the level of cybersecurity investment according to his risk attitude and his risk assessment. In fact, the level of chosen investment depends on the operator's risk propensity: if the operator is risk adverse, he would prefer a lower level of expected loss increasing current costs; otherwise, if the ICT operator is risk loving, he would accept a high risk situation increasing of current benefits (e.g. reduced security costs).

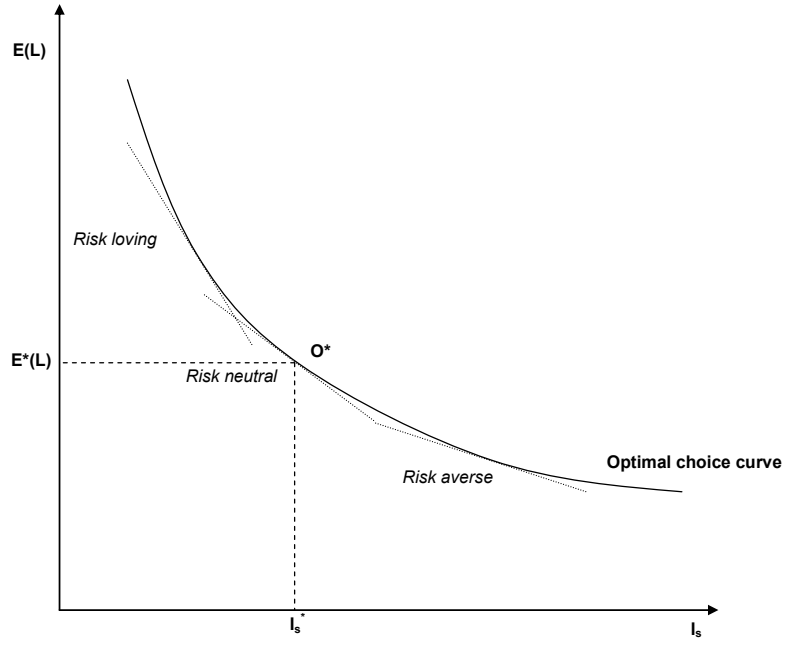
The assumption adopted in this paper is the risk neutrality of the operator [7]. Risk neutrality implies that the value of the level of cybersecurity investment is equal to the value of the expected loss, so that the optimal investment level chosen by the operator is represented by the intersection point between the optimal choice curve and the tangent representing the risk attitude of the agents. In Figure 1, the intersection point is *O**, the optimal cybersecurity choice, with a level of implemented investment I^*_s and consequent expected costs *E(L)** for cyber attacks.

---

[6] The random effect of the exogenous factors affecting the model structure could be addressed inserting an uncertainty variable into the model. The most likely uncertainty factors would be the probability of threat realization t and the potential loss λ. Both of them affect the expected value of loss due to the lack of information randomly affecting the ICT network actors. Assuming that the uncertainty variable would be inserted in the form of white noise, with zero average value independent and identically distributed, (which implies no autocorrelation), expected value of this uncertainty would not affect the final outcome of the model. For reference, see GREENE (2007).

[7] An agent is risk neutral when he/she is indifferent to sustaining current expenses in order to implement cybersecurity provisions or to bear the same expected expenses in the future to recover the losses caused by a cyber-attack. The idea of the risk aversion/propensity could be linked to inter-temporal choice, but it is crucial to consider the presence of a choice between certain and uncertain choice and not only between current options and future option. For reference, see KREPS (1991) and MAS-COLELL *et al*. (1995).

Figure 1 – The optimal level of investment in cybersecurity



■ The optimal cybersecurity choice with lack of information

The described optimal choice in the cybersecurity framework relies on the assumption that the ICT operator possesses complete information on cyber-crime effects and makes a proper assessment of cyber-attack risk. In fact, the expected loss and the following investment choice are defined as the result of the proper estimation of the probability of threat occurrence (t), of effectiveness in breaching the information system (v) and economic consequences of their impact (λ).

In the real world, complete information on cyber-attacks and related risk is not available to ICT operators, first of all, because cyber-attack techniques evolve rapidly and are becoming increasingly sophisticated. In addition, ICT operators targeted by cyber-attacks are reluctant to publicly communicate and report to the authorities any disruption in services, the causes, frequencies and costs. This operator behavior can be ascribed to the concern of suffering reputational damages, breaking confidentiality

obligations and being addressed on grounds of liability. Moreover, the particular sensitivity of information on cybersecurity incidents makes information sharing a particularly risky issue, hindering the development of a confident and fruitful environment [8]. In fact, from the perspective of a single operator, there are no immediate advantages in sharing information on past attacks [9], although all ICT operators and other critical infrastructure community members would gain from better information on cyber-attack framework.

The reluctance to share information about cyber-attacks experienced entails a biased knowledge on cyber-risk, leading to an under-estimation of cyber-attack probability and impacts. These circumstances influence the extent of implemented security provisions and the realized security investment: because ICT operators are not properly aware of the real extent of cyber-risk, the chosen level of investment is lower than that which would be desired by the operator himself.

These assumptions are supported by the results of a leading study on information sharing by GAL-OR & GHOSE (2004). The analysis made in the article "The Economic Consequences of Sharing Security Information" investigates the competitive implications of information sharing on breaches and the level of investment dedicated to security. The main conclusion is that market characteristics affect incentives for information sharing among competing firms, but information sharing encourages additional security investments.

---

[8] In this work the antitrust concerns related to information sharing are not discussed. However, speaking about information sharing, juridical criticalities that can arise in most of the western countries have to be mentioned. Due to confidential information flows among firms operating in the same market competitive issues may arise. For example, art. 101 and 102 of the Maastricht Treaty (respectively ex art 81 and 82 of the treaty establishing the European Union, generally known as the Treaty of Rome) pursue the goal of ensuring a competitive environment in the European union's markets prohibited "all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market". Information sharing, characterized by restricted disclosure of sensitive information, could be misinterpreted by an enforcement agency or used to hide the flow of information for anticompetitive purposes.
For a general overview of the antitrust issue in information sharing, among the main reference works there are "Information Exchanges Among Firms and their Impact on Competition" by KÜHN & VIVES, "Overcoming impediments to information sharing" by AVIRAM & TOR and "Information sharing, innovation, Antitrust" by TEECE.

[9] In the perspective of the operator, the immediate advantages of sharing information are not enough to overcome the potential risk of reputation loss coming from breaches or improper disclosure.

In cybersecurity management, availability of information guarantees proper risk-assessment essential for an efficient protection strategy. For the single ICT operator, any security investment choice depends on the evaluation of the balance between potential costs due to disruptions and benefits arising from a proper risk evaluation as a result of the assessment of threat probability, of its vulnerability and of potential threat damage. Limited information on cyber-attack potential damages may lead to underestimate the effective risk lowering desired investments. In addition, a large amount of literature, starting from the seminal contribution of DIXIT & PINDYCK (1994), regards the uncertainty of market conditions (for example, the probability of occurrence of threats) as a costly condition in case of investments. An ICT operator investing in security in a specific moment loses the possibility to wait for better market conditions, thus bearing higher costs. Empirical studies highlighted that there are situations where such costs are very high and particularly affected by the market uncertainty degree, leading to a remarkable security underinvestment compared to the theoretically optimal level [10].

The effect of lack of the adequate operator's awareness on cyber-risk is represented in Figure 2 with the *perceived* optimal choice curve under the optimal choice curve. The threat probability and the cyber-attack impact, which contribute to the shape of the optimal choice curve, are biased by the absence of a proper level of information and are perceived by the operator equal to $t^p<t^*$ and $\lambda^p<\lambda^*$ [11]. Assuming the ICT operator risk neutral, the resulting optimal level of investment (I^{**}_s) is lower than the previous (I^{*}_s) implying an expected cost $E^{**}(L)$ according to the operator's perception. Considering the real level of threat probability (t^*) and the real cyber-attack impact (λ^*) for a level of investment I^{**}_s, the expected loss that operator would sustain is $E^{*}(L)'$ which is higher than that estimated.

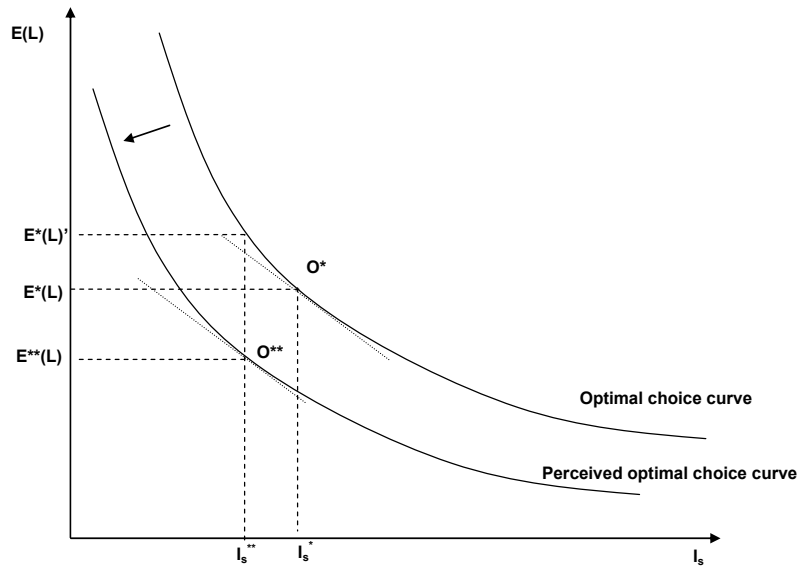
This analysis shows that the lack of information on cyber-attacks may cause an inadequate awareness of related risk (represented in the position of the perceived optimal choice curve) which leads each ICT operator to

[10] On this topic interesting articles have been written by CABALLERO (1991) and ABEL & EBERLY (1999).

[11] The vulnerability variable, v, composing the expected loss, is considered constant at least in the short term. In fact, it is assumed that the vulnerability of the ICT operator is a technological concern linked to the variability of the cybersecurity environment, where dangerousness and frequency of cyber-attacks change only in the long-term. In this study, vulnerability is considered constant as "protective capacity" and can be effectively modified in the mid-term only through current security investments implemented by the ICT operator.

invest in cybersecurity in a suboptimal way, with a level of implemented security provision insufficient not only for social demand but also for the ICT operator's preferences.

Figure 2 – The effect of lack of information on the optimal level of investment in cybersecurity



In this context, cyber-attacks cause greater economic damages than expected by the ICT operators themselves, with amplified consequences on other critical infrastructure operators, public authorities/bodies and citizens.

■ The improvement of information availability on cyber-attacks: potential measures at European level

The strategic role of ICT services in the current European economies is increasing the policy makers' interest towards protection against cyber-attacks and towards possible measures to reduce related market failures.

One of the possible regulation solutions is suggested by GARCIA & HOROWITZ (2007) in "The potential for underinvestment in internet security: implications for regulatory policy", where incentives and obstacles to security provisions in the Internet market are investigated. Their model confirms the security underinvestment (from a social perspective) by Internet providers:

the social value derived from Internet largely exceeds potential and actual revenues associated with the telecommunication companies. GARCIA & HOROWITZ sustain appropriate, at least in the long term, the implementation of regulatory instruments focusing on a standardized security risk analysis for Internet companies even if there are difficulties due to the inability to measure the current level of security, the evolution of cyber-attackers' tools, the implementation of homogeneous security tools, the capacity of ranking security risks and the different organisations' financial readiness and technological profile to support security of the internet infrastructure.

For this purpose, the starting point of institutional efforts against the spread of this threat at the European level is the Convention on Cyber-crime, composed and signed by the Council of Europe in November 2001 in Budapest [12]. It represents the first recognition of the necessity to protect society, industry and citizens' life from cyber-crime by harmonizing national laws, improving investigative techniques and increasing cooperation among nations.

In addition, the Communication on "Network and Information Security: Proposal for a European policy approach" [13] stimulated a structured approach to the Information system protection. In recognition of the ever growing importance of the issue, the European Commission revitalized its 2001 approach and developed a new strategy for a secure Information Society which was adopted on May 31, 2006 [14].

In 2009, the European Commission adopted the Communication on Critical Information Infrastructure Protection [15], which develops a structured European policy on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs.

---

12 Convention of Cybercrime, Budapest, 23 November 2001.

13 COM (2001) 298 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region. "Network and Information Security: Proposal for a European policy approach".

14 COM (2006) 251. Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Region. "A Strategy for a secure information society - Dialogue, partnership and empowerment".

15 COM (2009) 149 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large scale cyber-attacks and disruption: enhancing preparedness, security and resilience".

More recently, the Communication on "A digital agenda for Europe" [16] aimed at delivering sustainable economic and social benefits from a single digital market. Particular attention is addressed to reinforcing Network and Information Security Policy in the Chapter on Trust and Security. The communication suggests an intervention to modernize ENISA [17] and to set up a Computer Emergency Response Team (CERT) specifically for EU institutions.

All the regulatory initiatives against cyber-attacks undertaken at the European level are focused on the critical role of information on cyber-crime and on the network nature of information systems and its consequence on security. Most of the proposed measures aim to increase the social awareness of cyber-attack effects and to reduce the biased optimal choice behaviour of ICT operators, targeting with policy indications also the other actor categories as stakeholders able to impact directly on the security provisions.

In order to improve cybersecurity, an incentive framework can be set up by policy makers for:

- Sharing technical information through a bottom-up approach essentially involving ICT operators and other critical infrastructure operators to better assess the cybersecurity risk at the organization level
- Sharing technical information through a top-down approach essentially involving ICT operators and public authorities/bodies to set up measures to prevent cyber-attacks and to better assess cybersecurity risk at the social level
- Spreading information on the cyber-crime phenomenon, increasing the knowledge for each category of ICT stakeholder (ICT operators, other critical infrastructure operators, public authorities/bodies and citizens)

16 COM (2010) 245. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. "A digital agenda for Europe".

17 The renewal of the mandate of ENISA and its modernization have been regulated through the "Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration" (COM (2010) 250 final) and by the "Proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)" (COM (2010) 251 final).

The following paragraphs review potential actions at the European level able to reduce the lack of information on cyber-attacks and to increase the cybersecurity level not only through the higher investments of ICT operators.

How information sharing on cyber-attacks may raise security investment

ICT stakeholders' active interaction is necessary to exchange information on experienced incidents and breaches in order to be effective in increasing the level of knowledge and control of cyber-attacks. A positive impact on the improvement of Network Information Security and on the minimization of the potential disruption effects is given by the sharing of information on threats, vulnerabilities, risk assessment and response best practices (e.g. including investment strategies) among ICT operators and other critical infrastructure operators (ENISA, 2007).

Institutionally, important steps have been taken at the European level to facilitate information sharing. The Resolution 2007/C68/01 of the European Council of 2007 invited Member States to "encourage where appropriate in co-operation with ENISA, effective exchanges of information and co-operation between the relevant organizations and agencies at the national level" referring in particular to Network Operators, service providers and rest of the private sector [18].

To this purpose, introduction of circles as platforms and forums to share information enhances preparedness and resilience. These circles are groups of ICT operators and other critical infrastructure operators (at national or international level) available to spread information on cybersecurity within the restricted group. Participation is subject to compliance with requisites set by the circle: trust among members, value and concreteness of the content of the information sharing, absence of biased and of competitive behaviors, and guarantee of non disclosure.

Information sharing circles may be led by government bodies and/or authorities and in most of the cases can be considered voluntary and

[18] According to the "Good Practice Guide for Information Sharing" (ENISA 2009a), "an Information Exchange is a form of strategic partnership among key public and private stakeholders. In the NIS field, these can sometimes be referred to as 'Network Security Information Exchanges' (NSIEs) although it is recognised that alternative names can also be used."

bottom-up initiatives. Although information sharing circles may include informal and formal groups, recent evidence in the European context has been driven towards the latter option [19], organizing information circles as "trusted forums" or "trusted platforms" in which operators and stakeholders meet regularly. Formal structures with the participation of public entities and a mixed composition (e.g. ICT operators and other infrastructure operators) guarantee a regulated framework around information sharing circles avoiding an untrustworthy atmosphere hampering valuable exchange of information and good practices [20]. Information sharing circles may represent one of the most efficient tools to solve limitations related to the lack of information and data on cybersecurity for the ICT operators and partially for other critical infrastructure operators. At the organization level, the improvement of cybersecurity related information allows a better assessment of the risk of disruptions and supports more effective investment choices both to improve preparedness and to respond to emergencies.

The exchange of information may increase security awareness of ICT circles' members and result in benefits for individual stakeholders and for the network security of the society as a whole. Applied to the model described before, reduction in the lack of information has the immediate effect of diminishing the distance between the perceived level of damage of cyber-attacks (λ^p) and the actual (λ^*) and the mid-term effect of increasing the ICT operator's awareness of its vulnerability v, bringing the perceived optimal choice curve closer to the actual and pushing I_s^{**} towards I_s^*. Information sharing circles provide information for short-term intervention in the event of emergencies and for long-term perspective reducing costs of potential disruptions with a benefit for all other mentioned ICT stakeholders through an increased level of cybersecurity on the part of ICT operators.

[19] Within the project "Availability and Robustness of Electronic Communications Infrastructures - ARECI", formal approaches for sharing information seem to be the most effective to improve protection of infrastructures critical to the reliability of telecommunications services.

[20] The National Computer Emergency Response Teams (CERTs), which are regulated by public entities, contribute effectively to dissemination of security information. For example, an integrated platform among national contexts would also permit prevention actions of potential disruption and effective management of cyber-attacks at European level. For further details on a concrete realisation, see the project "National and European Information Sharing and Alerting System - NEISAS".

How disruption reporting may reduce cyber-attacks effects

The increase of shared information on threats, vulnerabilities and incidents among CIIs operators' and main stakeholders may refine the risk assessment activity on which security and resilience investment rely. Among the several ways to address the lack of information issues, one solution is the implementation of homogenous practices for disruption reporting, allowing competent authorities to have a complete overview of the emerging threats and related vulnerabilities and to collect significant data for the social risk evaluation.

Through the Telecommunications Regulatory Package (article 13.a.3 of the amended Directive 2002/21/EC) a strong indication has been already provided to Member States in order to:

> "[…] ensure that telecom operators notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of their networks".

The telecommunication sector in particular is led by universal service provision rules and Member States have to ensure all users minimum service level provisions according to the current development of technology at an affordable price, irrespective of their geographical location.

As per the ENISA's study on "Good practices on reporting security incidents" (ENISA 2009b):

> "Reporting plays an important role in these efforts as it contributes in improving stakeholders' knowledge of the actual security problems at stake. An effective incident reporting system contributes to the collection of reliable and up-to-date data on information security incidents and ensures: a) quick dissemination of information among interested parties, b) a coordinated response, c) access to a wide pool of expertise about such incidents, d) that national authorities can follow up with the infrastructure managers in a regulatory capacity, e) threat analysis; and f) identification of good practices".

A key-element for overcoming lack of information at European level is therefore a common strategy for collecting detailed data and widening reliable sources (e.g. main ICT stakeholders). In spite of the effort made by the European institutions and bodies to adopt appropriate measures to harmonize incident reporting procedures, existing practices at Member States level remain extremely heterogeneous reducing the effectiveness of

the collected information. [21] Consequently, appropriate reporting schemes and data shared at the European level may impact positively on security and resilience disclosing the effective extent of the cyber-threats. Apart from the effects similar to information sharing, reporting activity [22] of ICT operators to public authorities/bodies may reduce the distance between the perceived probability of cyber-threats (t^p) and the real probability of threats (t^*) spurring the implementation of adequate actions against potential cyber-attacks (e.g. imposition of security standards, cooperation at international level). The entire society would benefit from an increase of cybersecurity sustained by additional investments by ICT operators (towards I_S^*) and other critical infrastructure operators.

How competence may increase cybersecurity level

The consistent development of ICT networks, as well as the technological pervasiveness in all the socio-economic activities, requires a continuous update of technological skills. Education in security is needed to prevent, to face and to react to cyber-crime attacks. Due to the network features of ICT systems and the presence of the weakest link, the development of baseline security technological skills for the largest part of the population may improve the overall security of the ICT systems and those strictly connected. Filling the gap in terms of technological skills with the aim of increasing cybersecurity would mean setting up different education measures for citizens according to their potential user role: home user, ICT professional and worker.

The creation of a cybersecurity culture implies the involvement of society as a whole. Mass actions to communicate essential information on the potential impacts of cyber-attacks ranging from the individual perspective to the public one may represent an effective tool to spread awareness on security issues (ENISA 2009c). In the USA, the National Cyber Security Awareness Month (NCSAM), conducted every October since 2004, is a national public awareness campaign to encourage everyone to protect their computers and the USA's national critical cyber-infrastructure. According to

[21] According to the report "Good practices on reporting security incidents" (ENISA 2009b), differences in incident reporting exist between countries especially in terms of objectives such as emergency response, incident response, incident prevention, legal rectification.

[22] Incident reporting may add value to all the parts involved in the process. Efficient and fast access to valuable information is one of the main benefits for the reporting organizations.

the Department of Homeland Security (DHS), the National Cyber Security Alliance (NCSA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC), cybersecurity requires constant action to coordinate what home users, businesses and governments need to do in order to protect themselves against attacks. [23]

As technology is involved at every level of life, professional ICT education on security issues is essential. Most education systems in Europe have developed ICT skills among future professionals. This awareness should move to encompass security because it is not efficient to divide ICT and security specialists. The need for e-skills certification and e-skills is a moving target modeled after the market. Within this area, specific skills pertaining to ICT security have long been identified but little training effort is currently devoted to security and resilience in the large panel of e-skills certifications throughout Europe. At present, ICT operators and other critical infrastructure operators lack qualified security professionals and academic courses on ICT security represent a preliminary answer to this need of competence.

In addition, it is fundamental for companies and their employees to understand ICT threats, vulnerabilities and risks able to damage their business. For this reason, "training on the job" and "learning-by-doing" are necessary tactics to better protect the employee's daily work from cyber-attacks. Employees tutored through training courses in order to become aware of cyber attack risks and mitigation strategies may avoid severe consequences also due to unintentional internal actions. A provision of constant training (typically in house, i.e. within companies and government agencies) can be conceived at the European level through lifelong learning programmes in which ICT may constitute the core support to reduce potential impacts of cyber-disruptions (both malicious and caused by human error). According to the theoretical representation, the creation of a cybersecurity competence through different channels (awareness of citizens, creation of ICT security professional profiles and cybersecurity training on the job) reduces the gap between the perceived probability of cyber-threat (t^0) and the real probability of threats (t^*). Furthermore, in the mid-term, an increase in cybersecurity competence is advisable to reduce the real probability of threats (t^*). In fact, cyber-threats due to involuntary human errors (and not to malicious attacks) may be consistently reduced through education [24].

---

[23] The USA National Cyber Security Awareness Month, http://www.staysafeonline.org/ncsam.

[24] GORDON & LOEB (2002) mention this effect also in their model.

■ Concluding remarks

Cyber-attacks are gaining in the ranking of global threats for their potential devastating socio-economic impact. Together with cyber-crime fighting, measures to increase the general level of cybersecurity have to be adopted by all relevant stakeholders related to ICT networks. At the European level, regulation efforts are supported by bottom-up actions aimed at reducing market failures of the security-market. In addressing the investment behavior of ICT operators, improvement of their cybersecurity level can be obtained by reducing the current lack of information on cyber-attacks.

An effective cybersecurity investment relies on information on the probability of the threat occurrence, the vulnerability of the system and the potential loss due to the threat realization. Lack of information generates a biased cyber-risk assessment and an underestimation of the potential loss.

Furthermore, increased cybersecurity can be obtained through more efficient behaviour of the other main ICT stakeholders. Formal information sharing practices, homogeneous breach-reporting procedures at the European level and the improvement of the social cybersecurity competence may positively affect the structural conditions in which ICT operators make their cybersecurity investment choice.

Additional research on the cybersecurity topic is needed to deeply investigate the network nature of the ICT world, the related security behaviours of its main actor categories and the extent of the effect of each analysed measure to increase information availability on cyber-attacks to ICT operators.

References

ABEL A.B. & EBERLY J.C. (1999): "The impact of uncertainty on capital accumulation", *Journal of Monetary Economics*, Vol. 44, pp. 330-377.

ACOCELLA N. (2000): *Foundations of Economic Policy. Values and Techniques*, Cambridge Press.

Alcatel-Lucent's Bell Labs and professional services (2007): "Availability and Robustness of Electronic Communication Infrastructures - ARECI", Final Report of the ARECI project supported by DG Information Society and Media of the European Commission.

ANDERSON R. (2001): "Why Information Security is Hard – An Economic Perspective", *Proceedings of the 17th annual Computer Security Application Conference*. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=991483.

ANDERSON R. & MOORE T. (2006): "The Economics of Information Security", *Science*, Vol. 314 no. 5799 pp. 610-613.

ARTHUR S. & SHEFFRIN S.M. (2003): *Economics: Principles in Action*, Pearson Prentice Hall.

AVIRAM A. & TOR A. (2004): "Overcoming impediments to information sharing", Harvard Law school discussion paper, *Alabama Law Review*, Vol. 55.

BORG S.

- (Forthcoming): *Cyber attacks. A Handbook for Understanding the Economic and Strategic Risks*, US – CCU.
- (2005): "Economically complex cyber attacks", *IEEE Security and Privacy*, Vol. 3.
- (2009): "The Economics of Loss" in *Enterprise Information Security and Privacy*, edited by C. Warren AXELROD, Jennifer L. BAYUK & Dainel SCHUTZER.

BRUCK T., KARAISI M. & SCHNEIDER F. (2006): "A survey of the economics of security", NEAT Economics of Security working paper 1.

CABALLERO R.J. (1991): "On the sign of the investment-uncertainty relationship", *American Economic Review*, Vol. 81, No. 1, pp. 279-288.

CAMBACÉDÈS L.P. & CHAUDET C. (2010): "The SEMA Referential Framework: Avoiding Ambiguities in Security and Safety Issues", presentation at the 4th Annual IFIP Working Group 11.10 International Conference on Critical Infrastructure Protection, Fort McNair, Washington, DC, USA, March 14-17, 2010.

CAVALLINI S., DI TROCCHIO S., BISOGNI F., TANCIONI M. & TRUCCO P.C. (2010): *Study for the Development of a Methodology and Research of Quantitative Data on the Economics of Security and Resilience in Critical Communications and Information Infrastructures – CIIS – SMART-SEC*, Final Report of the SMART-SEC project supported by DG Information Society and Media of the European Commission.

CHOI J.P., FERSHTMAN C. & GANDAL N. (2004): "Internet Security, Vulnerability Disclosure, and Software Provision", 4th Workshop on the Economics of Information Security, Harvard University, Cambridge.

European Parliament:

- COM (2001) 298. Communication from the Commission to the Council, the European Economic and Social Committee and the Committee of the Region, "Network and Information Security: Proposal for a European policy approach".
- COM (2006) 251. Communication from the Commission to the Council, the European Economic and Social Committee and the Committee of the Region, "A Strategy for a secure information society - Dialogue, partnership and empowerment".
- COM (2009) 149 final. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the

Committee of the Regions on Critical Information Infrastructure Protection – "Protecting Europe from large Scale Cyber-Attacks and Disruption: Enhancing Preparedness, Security and Resilience".

- COM (2010) 245. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, "A digital agenda for Europe".

- COM (2010) 250 final. Proposal for a regulation of the European Parliament and of the Council amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration

- COM (2010) 251 final. Proposal for a regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA)

Council of Europe:

- (2001): Convention of Cybercrime, Budapest, 23 November. http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm

- (2008): Directive 2008/114/EC, 8 December, "On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection".

- (2002): Directive 2002/21/EC of the European Parliament and of the Council, 7 March, "On a common regulatory framework for electronic communications networks and services" (Framework Directive).

DIXIT A.K. & PINDYCK R.S. (1994): *Investment under Uncertainty*, Princeton University Press.

ENEA (2011): "National and European Information Sharing and Alerting System - NEISAS", project supported by the Prevention, Preparedness and Consequence Management of Terrorisms and Other Security Related Risk Programme of the European Commission's Directorate Home Affairs.

ENISA:

- (2007): "Examining the feasibility of a data collection framework", ENISA Report.

- (2009a): "Good Practice Guide for Information Sharing", ENISA Report.

- (2009b): "Good Practices for Reporting Security Incidents", ENISA Report.

- (2009c): "The growing requirement for information security awareness", ENISA Report.

FORMIT (2009): "The Vulnerability of Information Systems and its iInter-sectoral, Economic and Social Impacts – VIS", project supported by the Prevention, Preparedness and Consequence Management of Terrorisms and Other Security Related Risk Programme of the European Commission's Directorate Justice, Freedom and Security.

GAL-OR E. & GHOSE A. (2004): "The Economic Consequences of Sharing Security Information", *Advances in Information Security*, Vol. 12.

GARCIA A. & HOROWITZ B. (2007): "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy", *Journal of Regulatory Economics*, Vol. 31.

GORDON L.A. & LOEB M.P. (2002): "The Economics of Information Security Investment", *Advances in information security*, Vol. 12.

GREENE W.H. (2007): *Econometric Analysis*, Prentice Hall.

HAUSKEN K. (2006): "Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability", *Information SystemsFrontiers*, Vol. 8, no. 5, pp. 338-349.

KANNAN K. & TELANG R. (2005): "Market for Software Vulnerabilities? Think Again", *Management Science*, Vol. 51, no. 5, pp. 726-740.

KEIZER G. (2010): "Is Stuxnet the 'best' malware ever?", *Infoworld*, 16 September. http://www.infoworld.com/print/137598

KOLFAL B., PATTERSON R. & YEO M.L. (2010): "Market impact on it security spending", Workshop on the Economics of Information Security, Arlington, USA. http://weis2010.econinfosec.org/papers/session1/weis2010_kolfal.pdf

KREPS D. (1990): *A Course in Microeconomic Theory*, Princeton University Press.

KÜHN K.U. & VIVES X. (1995): "Information Exchanges Among Firms and their Impact on Competition", Institut d'Anàlisi Econòmica (CSIC).

LIU D., JI Y. & MOOKERJEE V.M. (2005): "Information Security Investment with Different Information Types: A Two-Firm Analysis", *AMCIS 2005 Proceedings*.

MARKUSEN A.R. (2003): "The Case Against Privatizing National Security Governance", *International Journal of Policy, Administration and Institutions*, Vol. 16, Issue 4, pp. 471–501.

MAS-COLELL D., WINSTON M. & GREEN J. (1995): *Microeconomic Theory*, Oxford University Press

POWELL B. (2005): "Is Cybersecurity a Public Good? Evidence from the Financial Services Industry", *Journal of Law, Economics and Policy*, Vol. 1, pp. 497-510.

TEECE D. (2003): "Information sharing, innovation, Antitrust", in *Essay in technology management and policy*, World Scientific.

The USA National Cyber Security Awareness Month. http://www.staysafeonline.org/ncsam

VARIAN H.R. (2004): "System Reliability and Free Riding", in *Economics of Information Security*, Springer.

WILLEMSON J. (2006): "On the Gordon & Loeb Model for Information Security Investment", Workshop on the Economics of Information Security, Cambridge, England. http://weis2006.econinfosec.org/docs/12.pdf

Negotiating a New Governance Hierarchy: An Analysis of the Conflicting Incentives to Secure Internet Routing

Brenden KUERBIS & Milton L. MUELLER
Syracuse University, School of Information Studies

Abstract: New security technologies are never neutral in their impact; it is known that they can alter power relations and economic dependencies among stakeholders. This article examines the attempt to introduce the Resource Public Key Infrastructure (RPKI) to the Internet to help improve routing security, and identifies incentives various actors have towards RPKI implementation. We argue that RPKI requires ISPs to achieve security at the expense of autonomy, requires all actors to tradeoff simplified global compatability and centralization of power, and affects the policies and business models of the Regional Internet Registries and their relationship to the Internet Corporation for Assigned Names and Numbers. While the Internet remains a space where authority is highly distributed, elements of hierarchy do exist, especially around critical resource allocation, and it is likely that security and other concerns will lead to continuing efforts to leverage those hierarchies into more powerful governance arrangements.

Key words: routing, internet addresses, security, RPKI, ICANN, Regional Internet Registries, ISPs.

Routing and addressing are at the core of how the internet works. Every second, routing arrangements must be able to successfully move trillions of individual data packets from any originating network in the world to any one of millions of destinations anywhere in the world. Some of the most important cybersecurity problems relate to the way networks acquire address blocks and exchange routing information among each other. Efforts to solve routing-related security problems reveal how complex and difficult it can be to attain global acceptance and implementation of security-enhancing standards and practices.

The original Internet routing protocol assumed that all routers in all networks were trustworthy. Today, the existence of malicious actors on the Internet is a given. Additionally, the routing infrastructure is vulnerable to unintentional misconfigurations that can cause harmful results. (ENISA, 2010; BARBIR, MURPHY & YANG, 2006) One security flaw was illustrated

vividly in 2008 when a Pakistani ISP's attempt to block YouTube within their country propagated false routing information to ISPs around the world, effectively knocking YouTube off the Internet for a short period. [1] Several other well known misconfigurations that led to temporary routing outages have occurred in the past, although the overall extent and severity of the routing security problems network operators' deal with is not empirically documented in any publicly accessible, systematic way. The perceived need for greater security in routing has led to an attempt to create a Public Key Infrastructure for Internet protocol addresses and routes. Resource Public Key Infrastructure (RPKI) is a security technology that would create a hierarchy of digital certificates which would be used to authenticate both the holder of address blocks and the origination of route announcements using those blocks.

This paper begins with the premise that implementations of security technologies are never neutral in their impact; they alter power and economic relations and raise strategic and policy issues. (ANDERSON & MOORE, 2006) This is particularly true with the internet, where the interdependence of many autonomous, diverse stakeholders can make it especially difficult to devise effective security solutions. (BAUER & VAN EETEN, 2009) This paper considers two research questions generated by that theory. First, what kind of shifts in power relations and cost-benefit distributions are produced by efforts to make Internet routing more secure using RPKI? Once these reconfigurations have been identified, one can then understand the incentives various actors have towards RPKI implementation. This leads to our next research question: is the implementation of RPKI facilitated or impeded by those incentives? In other words, are its prospects for implementation good, or will its adoption likely be blocked due to the unwillingness of actors to accept the power shifts and altered economic distributions?

In the next section, we briefly describe the prevailing state of internet routing. After that, we describe how RPKI proposes to solve these problems using digital certificates to bind IP address blocks issued by the extant allocation hierarchy to ISPs and internet routing information. The next section analyzes the ways in which RPKI produces shifts in power relations and cost-benefit distributions. In the concluding section we summarize our findings.

---

[1] See http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.

■ Routing and security

Routing is the automated process that directs Internet protocol packets from their origin to their destination. IP addresses can be described as part of the language that routers speak to each other. Internet routing protocols consider the IP address to be composed of two parts: the address of the network (the prefix) and the address of the connected computer (the host). Routing through the Internet is based on the network portion of the address. For each prefix, a router stores information telling it how to find a path to it and uses this information to construct a forwarding table (the routing table) that controls the movement of each incoming packet to the next hop in its journey. Routers also transmit announcements to other routers about the address prefixes to which it is able to deliver packets, and this information is incorporated into the tables of other routers. Thus, routers are engaged in constant, automated conversations with each other that exchange network prefixes and other routing policy information to keep every router informed about how to reach tens of thousands of other networks on the Internet.

Currently, interactions among routers are based on an Internet standard known as Border Gateway Protocol (BGP). As originally described in RFC 1771 (1995), and as later updated by RFC 4271 (2006), BGP is the dominant inter-domain routing protocol of the Internet (REKHTER & LI, 1995; REKHTER *et al*., 2006). As noted earlier, the original BGP protocol assumed that all Autonomous Systems (ASes) were trustworthy. As the Internet grew, the assumption of ubiquitous trust made less and less sense (HU, McGREW *et al*., 2006). Extensive work has been done in the technical community exploring the issue of routing security and proposing various solutions to improve it (BUTLER, FARLEY, McDANIEL & REXFORD, 2010).

Some assessments of this problem are more alarmist than others. Some observers ridicule the existing state of affairs as "routing by rumor" (Internet Architecture Board [IAB], 2010) and emphasize the fragility of the whole system (BUSH, AUSTEIN & BELLOVIN, 2010). Other voices are less alarmed. They note that a variety of measures are already in place by ISPs to filter out false route announcements. They claim that the same network operators who don't currently filter BGP announcements properly are not likely to deploy new security solutions such as RPKI. A major breakdown such as the Pakistan case, they claim, applied only to one site and was remedied in about two hours; routing takes place reliably in the vast majority of cases.

■ RPKI as a proposed solution

RPKI uses digital resource certificates to authenticate the possession and use of IP address blocks, Autonomous System (AS) numbers, and route announcements. (KENT, 2006) Certificates bind a resource holder of IP address block prefixes to its public cryptographic key and possibly other information like Autonomous System (AS) numbers that have been allocated to the organization. Subsequently, resource holders can create route origin authorization (ROA) statements, or standardized verifiable attestations that the holder of a certain prefix authorizes a particular Autonomous System (AS) to announce that prefix. Using these certificates and ROAs, network operators (e.g., ISPs) can validate that 1) a specific network, as indicated by a unique AS, is the legitimate holder of an IP address block, and 2) the AS that originates a route announcement using a particular prefix is authorized to do so. Like all PKIs, authenticating certificates therein (and subsequently the associated allocation and routing information) would rely on the system having one or more Certification Authorities (CAs) [2], which could publish a public key(s) or "trust anchor" to be used to authenticate other certificates.

The Secure Inter-Domain Routing (SIDR) Working Group of the Internet Engineering Task Force, which was initiated in November 2005, produced an architectural specification for a Public Key Infrastructure for validating address holders, AS numbers and route authorizations. The critical feature of the proposed RPKI solution is the attempt to link resource certificates to the institutions that issue internet resources, namely ICANN and the RIRs. [3]

As Figure 1 shows, IP address resources are allocated and assigned on a hierarchical basis. By virtue of its U.S.-government granted contract to perform the Internet Assigned Numbers Authority (IANA) function, ICANN sits at the top of the delegation hierarchy. It makes large delegations (usually

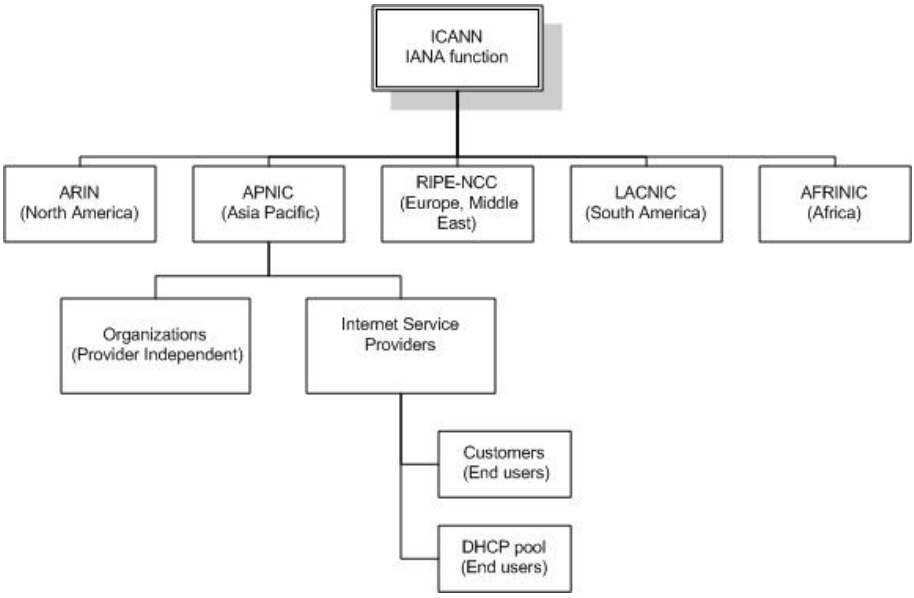
---

[2] Most users are familiar with digital certificates through their use of Certification Authorities (CAs) for web sites. CAs are third parties who are trusted by the subject (publisher) of the certificate and the parties interacting with the subject who rely upon the certificate for authenticating it (the relying party). This allows relying parties to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. Many private sector companies offer CA services commercially. Government agencies may also act as CAs, or organizations can set up their own, internal CA. A 2009 market share report determined that VeriSign and its acquisitions (which include Thawte and Geotrust) have a 47% share of the certification authority market, followed by GoDaddy (23%), and Comodo (15%). See Wikipedia http://en.wikipedia.org/wiki/Certificate_authority.

[3] See *An Infrastructure to Support Secure Internet Routing*. http://tools.ietf.org/html/draft-ietf-sidr-arch-11.

one or more /8 blocks of about 16.7 million individual IPv4 addresses) to the Regional Internet Registries (RIRs). The five RIRs, each roughly corresponding to a recognized geographic region, receive applications for addresses from Internet service providers, hosting services, and corporate networks within their region. The RIRs assign a unique Autonomous System Number (ASN) to each recipient and delegate address blocks to each AS based on technical need criteria. Internet service providers and organizations in turn sub-delegate address blocks to their customers or departments, respectively. The SIDR working group proposed that the RPKI mirror this delegation hierarchy. It did so because, in its own words, "existing resource allocation and revocation practices have well-defined correspondents in this architecture." [4]

Figure 1 - IP address allocation hierarchy



In a February 2010 official statement, the Internet Architecture Board (IAB), the chief supervisory body of the IETF, expressed its support for the linkage between the trust anchor hierarchy and the address allocation hierarchy:

[4] See Section 1 of *An Infrastructure to Support Secure Internet Routing*. The statement was partly inaccurate because there are few established practices and few precedents for resource revocation in current policies.

> "The IAB considers a properly designed and deployed RPKI to be an absolute prerequisite to having a secure global routing system, which is in turn a prerequisite to having a reliable worldwide Internet. ... The SIDR architecture and protocols have been designed to support a single trust anchor as well as multiple trust anchors. The IAB however, [believes that]: 1. the RPKI should have a single authoritative trust anchor; 2. this trust anchor should be aligned with the registry of the root of the allocation hierarchy." (IAB, 2010)

We now examine the way actor incentives interact in the current institutional environment. Implementation of RPKI depends on the actions of four distinct classes of actors: internet service providers (ISPs), the Regional Internet Registries (RIRs), the Internet Corporation for Assigned Names and Numbers (ICANN) [5], and the US Government. The actions of these globally distributed entities are not centrally coordinated or subject to any single hierarchical authority.

Below, we identify and briefly analyze four distinct ways in which RPKI's design and implementation shift power relations and cost-benefit distributions. The four points are:

- RPKI requires ISPs to trade off security and autonomy
- RPKI requires all actors to trade off simplified global compatibility and centralization of power
- RPKI affects the policies and business models of the RIRs
- RPKI affects the RIRs' relationship to IANA

The incentives of ISPs: trading autonomy for security?

ISPs are the most important and the most numerous set of actors. Their routing operations are the place where RPKI must be implemented if routing is to be secured using this technology. This class of actors includes not only large commercial service providers who sell internet access on the retail and wholesale level, but also thousands of private sector organizations that run their own networks and thus acquire address blocks. There are approximately 35,000 distinct autonomous systems connected through the global Internet.

[5] ICANN is a nonprofit corporation formed in 1998 to serve as the coordination and policy making institution for Internet domain names and IP addresses. It is a U.S. government-shepherded evolution from the Internet Assigned Numbers Authority (IANA) operated by Jon Postel at the Information Sciences Institute with support from other early Internet developers.

ISPs have mixed incentives to adopt such a technology. On the positive side, a generalized capacity to authenticate route announcements and address block holdings could provide a more efficient, more automated method for handling routing information in a secure way. At its best, RPKI would not only help to prevent bogus route announcements and address hijacking, it would also facilitate the smooth transfer of ipv4 address resources from one party to another after the free pool is depleted. A fully functional, globally compatible RPKI system would act as an effective property title for IP address blocks, giving the address holder legitimate claim to acquire or transfer address resources, and allow third parties to verify legitimate holders of addresses.

There are however externalities in the adoption and implementation of RPKI. As other literature has recognized, network externalities – or what has more accurately been termed demand-side economies of scope (ECONOMIDES & WHITE 1994; MUELLER, 1997) – can act as both facilitators and obstacles to security technology adoption (LELARGE, 2009). ISPs can only reap security benefits when its digital certificates for routes are reciprocally recognized by at least one other ISP. At a minimum, a pair of ISPs can achieve minimal security improvement by agreeing to authenticate each other's route announcements. The scope of the security increases as more ISPs join in a compatible network of certificate exchange. These network externalities have many of the features of a two-way network as defined by Economides (ECONOMIDES, 1996, p. 675), in that there is a distinction between originating a route and accepting a route announcement from another ISP. Because this scope can be widened incrementally, through pairwise agreements among ISPs, and still deliver some benefits with each additional partner, network externalities by themselves do not seem to pose an insurmountable hurdle to RPKI adoption.

But a universal RPKI regime that is tightly bound to the authoritative IP address allocation hierarchy does raise some serious risks for ISPs. If ISPs are required to obtain a certificate for their existing address blocks, there is a risk that the issuance of a certificate could be perceived as requiring a new assessment, by the RIR, as to whether the ISP qualifies for the address blocks it already has. [6] The ISP would have to pay careful attention to the

[6] In the ipv4 space, where the RIRs issued most of the allocations years ago, the RIRs could be thrust into the role of auditing each network's address usage with the implicit threat of taking away the resources if the allocation is no longer consistent with policy. As one RIPE-NCC document admitted, "Many resources are now used for other purposes than they were originally assigned for. Certifying such resources would seem to imply that the RIPE NCC has validated

terms and conditions regarding the revocation of the certificate. But more importantly, getting a certificate from an RIR greatly changes the power relationship between the ISP and the address allocation authority. The internet has evolved in a way that detaches responsibility for address allocation from operational responsibility for routing. The RIRs, which are membership organizations of ISPs, register and record address block assignments in order to keep them unique. While ISPs use the RIRs' address allocations database, Internet service providers wholly control and authorize what routes they announce, and decide for themselves which other ISPs' routing announcements they trust or filter. Indeed, the RIRs' authority over address usage is almost completely a byproduct of the ISPs' willingness to use their registries as coordination tools.

RPKI changes all that. It has the potential to give RIRs direct, operational impact on routing. IAB member Danny McPherson first called attention to the way RPKI might give an RIR control over what is routed – and therefore stronger influence over what information is accessible over the internet. Reinforcing this view, David Conrad, at that time the head of IANA, wrote on the SIDR list:

> "Today, RIR influence on routing is essentially advisory in nature -- if an address holder (say) fails to pay their address maintenance fee, RIRs can, at most, remove the address holder's blocks from Whois databases. However, as I understand it, this has limited effect on existing [routing arrangements]. The RIR could potentially reallocate the space, but this would likely be a good way of annoying multiple parties (not just the folks the address space was reclaimed from). …[I]f filter lists are built or routers check origin authenticity in real-time by traversing the RPKI tree(s), there would seem to be significantly more control vested in each parent node in the path up to the root of the RPKI hierarchy. My fear is that this will simply be unacceptable in a political or business sense." [7]

Confirming Conrad's point, a university network operator objected to the way RPKI altered "the balance of power" between network operators and the RIRs:

> "Today if there is a legal dispute between an allocator [RIR] and an organization with an allocation, it will be solved through existing civil means. This may take some time. In the meantime the status quo

this re-assignment." See RIPE document 070206, "Outline new and current services affected by certification." Draft v1.5 https://ripe59.ripe.net/ripe/maillists/archives/ca-tf/2007/doc00000.doc.

[7] David Conrad, post to SIDR WG list 17 September 2009. http://www.ietf.org/mail-archive/web/sidr/current/msg01098.html.

> continues (from a technical/operational perspective). With RPKI the allocator can revoke the organization's certificate while the civil process takes its time, causing harm to the organization that is now unroutable. Don't think they won't do the revocation. I have personally seen situations where if one party has 'the switch' to enforce their will, they use it." [8]

Predictably, revocation of certificates has emerged as a critical point of contention in the ISP community's debates over RPKI. For example, when RIPE-NCC proposed implementing resource certification, its members refused to support it due to concerns about the length of certificate validity and the linking of certificate revocation to RIPE membership status. Participants commented that "people will be reluctant to [use resource certificates] if they have reasons to fear that routing may be stopped due to unexpected events relating to certificates' revocation." [9] Clearly, RPKI diminishes the autonomy of ISPs. It could be used to replace a looser, networked form of governance based on decentralized associative choices among Internet service providers with a more centralized and hierarchical governance form.

Trust model and global compatibility

An RPKI relies on a hierarchical chain of trust. This raises an important question: what organization or institution serves as the root-level trust anchor for the certification hierarchy? If there is no such centralized root, how does one ensure global compatibility and trust? This is the problem that creates divergent incentives for the other three actors (the RIRs, ICANN and the U.S. Government).

In the classical PKI scenario, everyone trusts a single Certification Authority (CA) and the sender and recipient of the information rely on the same CA. This kind of centralization is relatively easy to achieve in a single organization. [10] It becomes harder and harder to achieve as the set of

---

[8] Jeff Schiller, MIT network operator, post to the SIDR WG email list, September 20, 2009. http://www.ietf.org/mail-archive/web/sidr/current/msg01117.html.

[9] See http://www.ripe.net/ripe/maillists/archives/ca-tf/2009/msg00013.html.

[10] "In the classical PKI scenario, someone receives a document signed with a digital certificate. The recipient must trust the creator of that certificate (the Certification Authority - CA) to be able to confirm the identity of the sender. This is simple if the sender and recipient are using the same CA. The need for interoperability arises where the document has been signed with a certificate from a CA that the recipient does not know. The obvious approach is to centralise as much trust as possible and avoid this problem entirely. This is reflected in the root CA and

organizations using it becomes larger and more diverse. Even the U.S. government could not agree on a single CA for all its PKI activities. The global internet, which involves approximately 35,000 autonomous systems and hundreds of thousands more sub-delegations of address resources across hundreds of different language groups and political systems, the goal of a centralized and unified trust anchor may be unrealistic – and potentially even disruptive and dangerous, as the political battles over the root of the domain name system (DNS) have already demonstrated (MUELLER, 2010, KUERBIS & MUELLER, 2007). Insofar as one uses a centralized, strictly hierarchical trust model, one is also creating the potential for centralizing political and regulatory authority over the Internet.

The SIDR working group – significantly influenced by researchers supported by U.S. military contracts – wanted to map the resource allocation hierarchy directly onto the PKI, to make it as technically simple and unambiguous as possible. However, its deliberations explicitly noted the political and governance issues associated with that. In an attempt to square the circle, SIDR's architectural specification allowed organizations to choose their own trust anchor. The RPKI standard codified its reliance on the IANA-RIR allocation hierarchy; at the same time, its design was described as "capable of accommodating a variety of trust anchor arrangements." (HUSTON, WEILER, MICHAELSON & KENT, 2010) A statement by the SIDR WG's co-chair summed up the policy in a colorful way – and also revealed how ambiguous the underlying attitudes and specifications were:

> "[…] the ability of a relying party to choose a trust anchor is a big get-out-of-jail-free card for those who are allergic to the idea of one root. NOT that I'm recommending using that card." [11]

While the ability of ISPs to choose their own trust anchor might lead to a more heterogeneous yet compatible certification system, it is also possible that once the system achieves a critical mass of adopters, network effects will lead to convergence on a single, centralized trust anchor. In that case, ISPs who do not use the same trust anchor will face compatibility problems that could literally break their routing arrangements, cutting off their users from global connectivity. That risk would force everyone to rely on the dominant certification hierarchy and its trust anchor. As long as it is unclear

hierarchy PKI models discussed below. However, those models require tight central control and unanimous support." (Galexia, 2005 p. 4).

11 Sandra Murphy in post to SIDR WG list, 1 December 2008. http://www.ietf.org/mail-archive/web/sidr/current/msg00733.html.

how RPKI achieves compatibility among multiple roots, it is disingenuous to pretend that RPKI allows ISPs a free choice of trust anchors – just as it is disingenuous to pretend that anyone who wants to create an alternate DNS root can easily do so.

The incentives of the USG and ICANN

The U.S. government (USG), through the IANA contract, controls the top level of the address allocation hierarchy. ICANN is the party that the USG has chosen to perform the IANA functions.[12] The same contract gives ICANN control of the root of the domain name system hierarchy as well as the address space. While the USG's control of the IANA functions does contribute to the implementation of an effectively globalized governance regime, it is also a persistent source of political controversy, in that it elevates one national government over others.[13] It may also create advantages for US military[14] and surveillance capabilities, as well as providing economic and technological advantages for specific U.S. businesses. The U.S. government has made it clear that it considers retaining unilateral control of the IANA contract a matter of high-level national interest.[15] It has also funded much of the research work on RPKI. The U.S. Department of Homeland Security's Internet Infrastructure Security (IIS) program, part of its National Strategy to Secure Cyberspace, made its support for RPKI explicit: as part of the IIS program, DHS expected to "develop and deploy a Public Key Infrastructure (PKI) with the American Registry for Internet Numbers (ARIN)" by 2008, and to "conclude PKI deployment activities with global registries" by 2010.[16] Researchers and organizations that are part of the U.S., or are contractual agents of the U.S.

---

12 The contract between the Department of Commerce and ICANN and its various revisions is available at http://www.ntia.doc.gov/ntiahome/domainname/iana.htm.

13 See DRAKE (2005); MAYER-SCHÖNBERGER & ZIEWITZ (2007); and MUELLER (2010) for a discussion of the role of U.S. unilateral control over IANA in sparking geopolitical controversy during and after the World Summit on the Information Society (2002-2005).

14 Some of the political implications were noted by IAB member D. McPherson, who wrote "If some country holding the keys (TA) goes to war with another and decides they want to revoke all of their allocations, then ISPs would have zero control over this outside of their own routing domain." Danny McPherson, post to SIDR WG list 11 March 2008, http://www.ietf.org/mail-archive/web/sidr/current/msg00346.html. The concern over "bringing down national network infrastructures" and the relationship to a single authoritative trust anchor residing with IANA (which maintains a contractual relationship with a single government) were expressed again in a recent European study (ENISA 2010b).

15 See http://www.ntia.doc.gov/ntiahome/domainname/usdnsprinciples_06302005.htm.

16 See http://www.dhs.gov/xlibrary/assets/SandT5yearplan.pdf, pp. 3 and 53.

such as ICANN, support a RPKI hierarchy completely tied to the address allocation hierarchy, with IANA as the single root at the top of the hierarchy. The U.S. has an incentive to bring about a single-root hierarchy because it maintains and reinforces its own control over critical internet resources.

The organizational ambitions of ICANN also point in the direction of a single-root RPKI hierarchy with the IANA at its apex. Currently, ICANN plays a diminished role in address allocation. Until now the linkage between IP address governance and ICANN's governance of the domain name system has been fairly loose. The three major RIRs (RIPE, ARIN and APNIC) actually predate ICANN, and obtained most of the address resources they administer prior to the creation of ICANN in 1998. ICANN's Address Supporting Organization has never been formally established as an independent entity and the RIRs' trade association, the Number Resource Organization, has never signed a formal contract with ICANN that binds the NRO to ICANN's rules or contracts. Instead, the RIRs and ICANN are joined through a loose and noncommittal memorandum of understanding. Indeed, whereas ICANN gets over $50 million a year in fees from its contracts with domain name registries and registrars, it collects less than a million in "voluntary contributions" from the RIRs. Whatever fees they do pay are set by their own decisions and processes, not ICANN's. The relatively autonomous position of the RIRs emerged accidentally, as an artifact of the Internet's unplanned emergence in the mid-1990s. From the standpoint of the decentralization of power over Internet governance, these informal relationships are a good thing in certain respects. But RPKI threatens to reconfigure them.

There is some fear on the part of the USG-aligned interests that the NRO has ambitions to take control of the address space away from IANA/ICANN. If this happened it would diminish ICANN's stature and potential for revenue. Thus it is not surprising that we see ICANN eagerly embracing RPKI and pushing for a more centralized trust anchor located in the IANA. In its most recent Plan for Enhancing Internet Security, Stability & Resiliency ICANN's staff wrote that "ICANN, through management of the IANA functions, acquires the strategy and the responsibility of the stability, security and resiliency of the Internet number allocation system and ultimately, through the application of Resource Public Key Infrastructure (RPKI), the global Internet routing system. This responsibility manifests in the need to implement a technically ideal application of the RPKI Single Trust Anchor, as noted by the IAB and NRO, and results in ability to fully certify the validity, right of use, and uniqueness of Internet number resources." (ICANN 2010) In June 2008, ICANN's Security and Stability Advisory Committee (SSAC)

indicated its interest in "management of certificates for the addressing system (RPKI)." Indicating the alignment of interests between ICANN and the U.S. government, the U.S. Department of Homeland Security's IIS program manager was added to ICANN's Security and Stability Advisory Committee, and ICANN's 2010-11 fiscal budget included financial support for managing RPKI certificates.

The incentives of the RIRs

RPKI puts the RIRs in the center of many internet governance issues by dramatically expanding their authority over the day to day use of Internet number resources. It also heightens the tensions surrounding their relationship to ICANN/IANA.

The RIRs favor linking certificates to the address allocation hierarchy but they are also uncomfortable with a RPKI scheme that has a single trust anchor located at the IANA. Their preferred solution is to have six co-equal roots, one operated by the IANA and the other five by each of the five RIRs.

The RIRs' understand that reliance on a single trust anchor operated by the IANA has the potential to radically change their relatively autonomous position, by empowering ICANN/IANA to exert more direct control over the issuance and revocation of their address resources. This could lead them inexorably into a more formal contractual relationship with ICANN, more formalized fee-paying obligations, and a more direct subordination of their policy processes to ICANN's. Moreover, there is some hope in the technical community that when the current IANA contract expires, the U.S. government will alter the IANA contract in a way that will bring an end to ICANN's sole possession of it. Thus, despite the support expressed by the NRO and the IAB for a single trust anchor for RPKI, neither explicitly proposes to make ICANN the root. This was evident from a statement they issued in 2009, which said:

> "The Regional Internet Registries (RIRs) believe that the optimal eventual RPKI configuration involves a single authoritative trust anchor. That configuration may not be achievable in the short-term and the details and timelines for its implementation will depend among other things on discussions within the RIRs' communities and dialogues with others including the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF). In the meantime, the RIRs have agreed to undertake pragmatic implementations of RPKI services based on interim trust anchor models..." (NRO, 2009)

If ICANN was the exclusive root trust anchor for the RPKI, it might be possible for it to disintermediate the RIRs, and issue certificates and address blocks directly to organizations and end users.

Aside from the IANA/ICANN issue, the RIRs have strong organizational incentives to favor implementation of RPKI. It would strengthen enormously their role in Internet operations, creating opportunities to put more "teeth" or enforcement power into their policies. It would make revocation of address resources self-enforcing; it could also be used to rigidly enforce the territorial exclusivity of each RIR's address pools.

If RPKI became so widely adopted that most ISPs refused to route packets from entities not participating in the RPKI, such a requirement would make membership in the RIRs virtually compulsory and their fees a kind of tax rather than a membership payment for a voluntarily selected set of services and organizational rights. One ISP expressed fears about the monopoly power of the RIRs during the SIDR working group:

Although there is plenty of sense in aligning the RPKI chain of trust with the resource allocation chain, ISPs may have concerns with the RIRs being the trust anchors. The incentive structure for the RIRs is fundamentally different than that of a [private market] certificate provider like Verisign/Thawte/ CyberTrust. If these root CAs time and again demonstrate that they are untrustworthy they lose customers, revenue, and potentially their trusted status. What entices an RIR toward vigilance as they validate the supposedly authorized origin of a prefix? [17]

■ Concluding observations

This paper has documented contention over the adoption of a security technology, RPKI. The contention is caused by the way the technology's implementation bases routing security on resource certificates issued by the institutions that issue IP addresses.

As the first facet of its analysis, the paper analysed the shifts in power and cost-benefit distributions that arise from RPKI's implementation. It

[17] Ryan Shea, Senior Engineer, Network and Info Security, Verizon Business in post to SIDR WG email list 22 September 2009.
http://www.ietf.org/mail-archive/web/sidr/current/msg01142.html.

demonstrated that in this area, as in so many other areas of security technology requiring coordinated action among multiple stakeholders, there is no simple progression from a less secure to a more secure state, with the improvements in security being homogenous across all actors. On the contrary, the effort to achieve collective security via RPKI alters the distribution of power and economic benefits among different types of actors. For ISPs especially, RPKI creates a major new dependency with very important economic and regulatory implications. Issuers of the certificates could literally shut off an ISP's routing operations. This would potentially give address allocation authorities (or governments issuing orders to them) direct operational effects on ISPs.

As the second facet of the analysis, the paper asked how the incentives created by these prospective redistributions of power and wealth affect the possibility that the technology will be adopted. A key fact is that the IP address allocation mechanisms to which RPKI certificates would be tied are strictly hierarchical. Predictably, given the economic and political dependencies created by a hierarchical PKI, the four key categories of stakeholders (ISPs, RIRs, ICANN and the U.S. government) have taken positions on the implementation of RPKI based on their position within the hierarchy. The two parties at the top of the address allocation hierarchy (ICANN, U.S.) are enthusiastic supporters of RPKI implementation with a single, unified trust anchor. Those in the middle of the hierarchy (the RIRs) support RPKI implementation but seek a slightly less centralized trust anchor. Such a regime would maintain their financial and policy autonomy from ICANN while allowing them to run their own certification authorities. Actors at the bottom of the hierarchy (the ISPs) are unenthusiastic about rigidly linking routing to the address allocation hierarchy and for the time being show little inclination to adopt RPKI en masse. They are deeply concerned about the potential loss of autonomy inherent in such an approach.

These varying incentives have interesting, complex impacts on adoption. The conflict over positioning within the hierarchy has given the RIRs a strong incentive to implement RPKI rapidly using multiple trust anchors rooted in their own organizations. The RIRs have implemented RPKI as a voluntary member service as a pre-emptive move. ICANN and the U.S. government are not ready to roll out a globalized RPKI implementation that they could impose upon the RIRs yet. By acting now, and achieving some usage, the RIRs make it more difficult for ICANN to later bypass them.

Note that the barriers to ISP adoption do not come from network externalities *per se*. While it is true that the security benefits are not fully realized until most other ISPs adopt compatible RPKI, pairwise combinations of ISPs can achieve small increases in routing security incrementally. The real sticking point for ISPs is the loss of autonomy vis-a-vis their address registry. Network externalities could play a major role in the story, however, if any single trust anchor achieves critical mass and begins to establish itself as the dominant hierarchy.

For the time being, the conflict over position in the hierarchy has been resolved by permitting significant scope for voluntary action by each actor. For better or worse, the Internet remains a space where authority is highly distributed and no one is in a position to tell the others what to do. But elements of hierarchy do exist, especially around critical resource allocation, and it is likely that security and other concerns will lead to continuing efforts to leverage those hierarchies into more powerful governance arrangements.

References

ANDERSON, R. & MOORE, T. (2006): "The Economics of Information Security", *Science*, 314(5799), 610-613.

BARBIR, A., MURPHY, S. & YANG, Y. (2006): *Generic Threats to Routing Protocols, RFC 4593*, Internet Engineering Task Force. http://tools.ietf.org/html/rfc4593.

BAUER, J.M. & VAN EETEN, M.J.G. (2009): "Cybersecurity: Stakeholder incentives, externalities, and policy options", *Telecommunications Policy*, 33(10-11), 706-719.

BUTLER, K., FARLEY, T., McDANIEL, P. & REXFORD, J. (2010): "A Survey of BGP Security Issues and Solutions", *Proceedings of the IEEE*, 98(1), 100-122. doi: 10.1109/JPROC.2009.2034031.

BUSH, R., AUSTEIN, R. & BELLOVIN, S. (2010): "The RPKI & Origin Validation". http://www.ripe.net/ripe/meetings/ripe.../Bush-The_RPKI_Origin_Validation.pdf.

DRAKE, W. (Ed.) (2005): "Reforming Internet Governance: Perspectives from the UN Working Group on Internet Governance", New York: United Nations Information and Communication Technologies Task Force.

ECONOMIDES, N.:

- (1996): "The economics of networks", *International Journal of Industrial Organization*, 14(6), 673-699.
- (1994): "Networks and compatibility: Implications for antitrust", *European Economic Review*, 38(3-4), 651-662.

European Network and Information Security Agency [ENISA] (2010): Report on secure routing technologies. http://www.enisa.europa.eu/act/res/technologies/tech/routing/report-on-secure-routing-technologies/at_download/fullReport.

Galexia (2005): *PKI Interoperability Models*. http://www.galexia.com/public/research/assets/pki_interoperability_models_2005/pki_interoperability_models_2005.pdf.

HU, Y., McGREW, D., PERRIG, A., WEIS, B. & WENDLANDT, D. (2006): "(R)Evolutionary Bootstrapping of a Global PKI for Secure BGP", In *Workshop on Hot Topics in Networks (HotNets'06)*, Irvine, CA. http://sparrow.ece.cmu.edu/group/pub/hu_mcgrew_perrig_weis_wendlandt_bgp.pdf.

HUSTON, G., WEILER, S., MICHAELSON, G. & KENT S. (2010): *Resource Certificate (RPKI) Trust Anchor Locator*, Internet Engineering Task Force. http://tools.ietf.org/html/draft-ietf-sidr-ta-06.

Internet Corporation for Assigned Names and Numbers [ICANN] (2010): *Plan for Enhancing Internet Security, Stability & Resiliency*. http://www.icann.org/en/topics/ssr/ssr-draft-plan-fy11-13sep10-en.pdf.

Internet Architecture Board [IAB] (2010): *IAB statement on the RPKI*. http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html.

KENT, S. (2006): "An Infrastructure Supporting Secure Internet Routing", in A.S. ATZENI & A. LIOY, *Public key infrastructure: Third European PKI Workshop: Theory and Practice*, Lecture Notes in *Computer Science* (Vol. 4043, pp. 116-129). Berlin, Heidelberg: Springer Berlin Heidelberg.

KUERBIS, B. & MUELLER, M.L. (2007): "Securing The Root: A Proposal For Distributing Signing Authority. Internet Governance Project". http://internetgovernance.org/pdf/SecuringTheRoot.pdf.

LELARGE, M. (2009): "Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives", *The Eighth Workshop on the Economics of Information Security*, University College, London.

MAYER-SCHÖNBERGER, V. & ZIEWITZ, M. (2007): "Jefferson Rebuffed - The United States and the Future of Internet Governance", *The Columbia Science and Technology Law Review* 8, no. 188.

MUELLER, M.L.:

- (2010): *Networks and States: The global politics of Internet governance*, MIT Press.
- (1997): *Universal Service: Competition, Interconnection and Monopoly in the Making of the American Telephone System*, MIT Press.

Number Resource Organization [NRO] (2009): *NRO Statement on RPKI*. http://www.nro.net/news/nro-declaration-rpki.html.

REHKTER, Y., LI, T. & HARES, S. (2006): *A Border Gateway Protocol 4 (BGP-4)*. *RFC 4271*, Internet Engineering Task Force. http://tools.ietf.org/html/rfc4271.

REKHTER, Y. & LI, T. (1995): *A Border Gateway Protocol 4 (BGP-4)*. *RFC 1771*, Internet Engineering Task Force. http://tools.ietf.org/html/rfc1771.

Interview with Keith BESGROVE,

Chairman of the Working Party on Internet Security and Privacy, OECD

Conducted by **Michel J.G. VAN EETEN**

C&S: Companies regularly name information security as one of their main concerns. How important is information security for information and knowledge-based economies?

Keith BESGROVE: It is already more important than many people realize and as the world becomes increasingly dependent upon broadband enabled internet connectivity for all its social and economic interactions, the importance of information security can only grow. Because of this, stronger systemic defences against information security challenges must continue to be developed. Equally important are is behavior changes – at the end of the day, information security is everyone's responsibility.

C&S: The private sector increasingly realizes the importance of information security but nonetheless security loopholes continue to exist. What are the direct and indirect costs of insufficient cybersecurity to high-income and developing countries?

K. B.: I'm not in a position to be able to quantify these costs – there are plenty of others around the world better placed than me to do this. But I do know from our own work here in Australia than consumers' fears about information security threats – particularly the fears about identity fraud – are having a limiting or chilling effect on people's willingness to engage in on-line commerce. This must diminish the potential for economies to take fuller advantage of the economic opportunities created by an increasingly digital economy.

C&S: All security comes at a cost, both in a monetary sense and in trade-offs against other objectives such as innovation and accessibility. How can government assess when privately-owned services and infrastructures are secure enough?

K. B.: I don't buy the trade-off argument, and I never have. For example, many people assert that you can have security or you can have privacy but you can really pursue both. Such binary arguments simply ignore the welter of developments in privacy-enhancing technologies across the globe. Good

security systems and behaviours provide big direct and indirect pay-offs and that's how we should see them.

C&S: What developments do you expect over the next five years in terms of governmental involvement in cyber security?

K. B.: I anticipate growing involvement by governments, the private sector, and civil society in developing better and more broad-ranging global collaborative mechanisms. In this area the OECD and others have provided significant intellectual leadership in facilitating the development of groups such as the Global Privacy Enforcement Network (GPEN) as well as supporting the development of groups such as the London Action Plan. In this area, I am encouraged by the growing focus by other groups such as the APEC-Tel Working Group and the International Telecommunication Union on the need for greater inter-governmental information sharing.

C&S: What are best practice examples of private sector initiatives and public-private collaboration to improve cybersecurity? Can these be replicated in other countries and regions?

K. B.: In the fight against malware, I am encouraged by the growing range of collaborative actions between governments and ISPs to develop voluntary codes of behavior where ISPs agree to work to help their clients to clean up their infected PCs and then to take better defensive measures in the future. I would highlight the work in the Netherlands, Germany, Korea, Japan and in my own country of Australia, where the new i-Code appears to be gaining some real traction with Australia's major ISPs.

C&S: Cybercrime is organized across national boundaries. Increased connectivity allows criminals to reconfigure their activities quickly in response to law enforcement. What is currently done and what should be done in the future to fight international cybercrime?

K. B.: At the moment we rely heavily on a range of, mostly informal, collaborative mechanisms between enforcement authorities in different national jurisdictions. Many of these work a lot better than the media would have us believe, but the reality is that more needs to be done to enable enforcement authorities to collaborate more effectively with each other in fighting cybercrime. In many cases this can be as simpley as modifying the domestic laws to make it legal for your police force to share information on cross-jurisdictional cases. This will remain a significant challenge for policy makers and my suspicion is that we need to think in terms of regional rather than global solutions in the short to medium term.

C&S: The security challenges are changing because of the increasing diffusion of mobile Internet services, social networks, and cloud computing. How will these changes impact the policies for cybersecurity?

K. B.: Here I am both pessimistic and optimistic. In the short term, I am pessimistic that the rapid spread of mobile devices – particularly increasingly into the hands of children – will cause a whole new range of information security challenges to arise. In the medium to longer term, I consider that the rise of cloud computing will lead to improvements in information security because, as the cloud providers increasingly struggle for supremacy, one of their key differentiators in the market place can and will be the security and reliability of their offerings.

C&S: Are there any other issues that should be on the mind of private and public sector professionals involved in cybersecurity?

K. B.: Above all else we need to be persistent. Information security challenges are constantly evolving as are the systems on which the global economy is increasingly dependent. Governments, the private sector and civil society all have important roles to play, and we cannot relax our efforts here.

Interview with Evert Jan HUMMELEN,
Head of the division Internet Security, OPTA

Conducted by **Michel J.G. VAN EETEN**

C&S: Companies regularly name information security as one of their main concerns. How important is information security for information and knowledge-based economies?

Evert Jan HUMMELEN: The importance of cyber security for modern economies shouldn't be underestimated. In these economies an important part of innovations is based on the confidence that information can be reliably stored and shared between stakeholders, regardless of whether these are companies, consumers or governmental organizations. Without this confidence, development of new ways of communicating and doing business will be hampered.

C&S: The private sector increasingly realizes the importance of information security but nonetheless security loopholes continue to exist. What are the direct and indirect costs of insufficient cyber security to high-income and developing countries?

E. J. H.: It is difficult to give a quantitative estimate of the direct and indirect costs involved. However, the Delft University of Technology has investigated the economical consequences of two specific cases that have been enforced by OPTA. In the "Thuiswerkcentrale"-case (total fine by OPTA: € 510,000) the economical damage has been estimated at € 1.61 million as a result of the fraud involved, the loss of productivity due to the removal of spam. In the case where MSN messenger was used to spread unsolicited messages (total fine by OPTA: € 82,000) the damage has been estimated at € 17.5 million based on the loss of productivity due to the removal of malware.

On a more indirect level, there are of course the costs of informing users, the costs of security measures and the costs of policy making and law enforcement.

C&S: All security comes at a cost, both in a monetary sense and in trade-offs against other objectives such as innovation and accessibility. How can government assess when privately-owned services and infrastructures are secure enough?

E. J. H.: Security of infrastructures is a shared responsibility between government and the private sector. The use of security standards and 'certificates' can support the process in which all parties involved share the same vocabulary and understanding about security of information and infrastructures.

Regarding security of information the responsibility is also shared with the end-user. The end-user, especially the consumer, has a responsibility to keep his system clean. This will prevent the system from becoming part of a botnet and it will prevent the theft of personal and financial information. Internet service providers have the (legal) obligation to take necessary technical and organizational measures and to provide proper information in order to allow consumers to protect themselves from internet insecurities. If necessary, OPTA can and will enforce this rule. Internet security is a joint responsibility for government, the private sector and consumers.

C&S: What developments do you expect over the next five years in terms of governmental involvement in cyber security?

E. J. H.: This month (February 2011) a national Cyber Security Strategy has been published in the Netherlands, Germany and France. These public-private partnerships will play an increasingly important role in increasing cyber security at a national level. I hope and expect that the international collaboration on cyber security will have a "let's get to work" approach rather than a "discussion forum". A clear strategy can also help to allocate means in the most efficient way within government and between public and private partners. Now there are so many parties involved, that all have to find their own way of reaching their goals. There should be more efficient and effective ways.

C&S: What are best practice examples of private sector initiatives and public-private collaboration to improve cyber security? Can these be replicated in other countries and regions?

E. J. H.: A very good example of a Dutch public-private partnership is the "botnet-convenant", where 14 Dutch ISP's have agreed to fight botnets. This is done by temporarily isolating computers that have been infected by malware from the Internet. This prevents further spreading of the malware and enables the ISP to assist the user in removing the malware. As soon as the infection has been removed the computer can be reconnected to the Internet. An important aspect in this approach is the idea that classical enforcement is not always the only or best approach. Working together on prevention is in my view far more effective than fining people or organizations that fail to keep their systems clean. Nevertheless strong enforcement is always necessary to get rid of vicious people on the internet.

C&S: Cybercrime is organized across national boundaries. Increased connectivity allows criminals to reconfigure their activities quickly in response to law enforcement. What is currently done and what should be done in the future to fight international cybercrime?

E. J. H.: There are a lot of international activities regarding cyber security. For example: London Action Plan (LAP), European Public-Private Partnership for Resilience (EP3R), Building a European Internet Enforcement Capability (BEIEC), the founding of national Spam Reporting Centers and the activities by ENISA.

What should be done is to start exchanging information between public and private parties across the world. Legal issues are currently sometimes preventing information sharing or are at least used as an excuse to prevent this, To be able to really improve international information sharing we must learn how to handle these legal issues. Another key element of cooperation is confidence. This is something that is built over the years by exchanging information and actually meeting each other. OPTA has always invested in its relations with key partners around the world and will continue to do so.

OPTA is working together with different international public and private parties to share information. Currently OPTA is setting up a cooperation with ACMA (Australian Communications and Media Authority).

C&S: The security challenges are changing because of the increasing diffusion of mobile Internet services, social networks, and cloud computing. How will these changes impact the policies for cybersecurity?

E. J. H.: The policies with respect to cyber security would probably not have to change much. More important is the way in which we deal with these new developments.

Mobile services require security for the mobile devices, especially since the mobile device will increasingly be used as an electronic wallet. Social networks and cloud computing require that existing legislation is interpreted according to these new developments. OPTA has already fined someone that used a social network to send unsolicited messages even though a social network is not mentioned in (or excluded from) Dutch telecommunication law.

C&S: Are there any other issues that should be on the mind of private and public sector professionals involved in cybersecurity?

E. J. H.: Less discussion, more action!

Other paper

Volunteer Computing Model Prospects in Performance Data Gathering for Broadband Policy Formulation

Volunteer Computing Model Prospects in Performance Data Gathering for Broadband Policy Formulation (*)

Chanuka WATTEGAMA & Nilusha KAPUGAMA
LIRNE*asia*, Colombo, Sri Lanka

Abstract: The recent unprecedented growth of telecom facilities has offered the Internet users in most Asian countries a flavour of broadband. Yet, despite rosy promises by telcos, the user experience has often been less than ideal. These challenges can only be overcome by right policy decisions based on evidences. Thus, monitoring the broadband Quality of Service Experience (QoSE) becomes more than an attempt to ensure quality delivery and create a basis for policy formulation.

The first approach to monitoring QoSE, is the regulator reaching deep into the innards of the telecom network to install monitoring equipment and taking remedial actions, specified under the licenses or the governing statute, when the data indicate below-standard performance. Dearth of financial and human resources can be the key challenge in such a direct approach. The second approach is based largely on user activism, where educated users voluntarily contribute their time and computing resources towards building a performance database which in turn will be used in creating the bigger picture. A comprehensive methodology to benchmark Broadband Quality of Service Experience (QoSE), based on the latter approach has been developed jointly by LIRNEasia and TeNet group of Indian Institute of Technology (IIT) Madras. This methodology uses AT-Tester, an a open source based software tool to monitor all crucial QoSE broadband metrics over a longer period, on both week days and week days covering peak as well as off peak traffic. The traffic is also monitored within segments, ISP, local and international. The methodology adapts the concept of Volunteer Computing (or Public Service Computing). The paper analyses how this approach could be used in broadband policy formulation.

Key words: Broadband, quality of service, volunteer computing.

(*) This research has been funded through a grant from the International Development Research Centre (Canada) and the Department for International Development (UK). The authors also acknowledge the contribution of Prof. Timothy Gonsalves (IIT Madras), Mr. R. Thirumurthy (Midas) and Ms. Helani Galpaya (LIRNE*asia*).

The paper was presented at the Experts Workshop; *Beyond Broadband Access: A data based information policy for a new administration*, 22-24 September 2009, Washington DC, organised by the New America Foundation

International Telecommunication Union (ITU) refers to broadband as 1.5 – 2 Mbps (ITU, 2003) while, Organisation for Economic Cooperation and Development (OECD) accepts 256kbps as the threshold (OECD, n.d.). [1] A publication by Partnership for Measuring ICT for Development (2009) defines broadband as an Internet service of at least 256 kbps in one or both directions. The US Federal Communication Commission has specified 768 kbps as the minimum speed for Broadband (KANG, 2009).

It has been noted in the available literature that provision of broadband would enable the diffusion of certain services to the public. Services such as e-gov, e-health (tele-medicine) and distance education require broadband connectivity (RAMIEREZ, 2007). Broadband has also enabled cheaper communication through Voice over Internet Protocol (VoIP). The impact of broadband is now beginning to appear on the economic statistics (KRUGER & GILROY, 2008). According to ARBORE & ORDANINI (2007, p. 83):

> "The importance of broadband in the business sector is related to the higher potential for data interchange and multimedia applications".

According to the latest OECD data, as at Q4 2008, broadband access per 100 inhabitants in OECD countries stood at 22.35 with Denmark being the highest, 37.18. According to an OECD report some countries have already reached 100% coverage, and prices have fallen since 2006. According to the same report:

> "Data on penetration, price, speed and usage of the Internet highlight how member countries have promoted competition, encouraged investment and worked together with the private sector to increase connectivity" (OECD, 2008, p. 8).

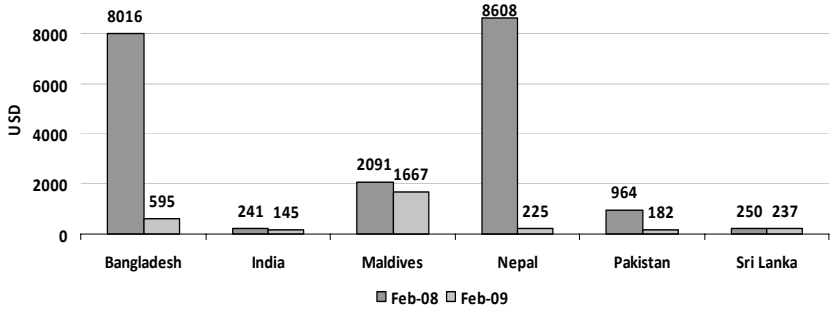
In comparison to the OECD, broadband penetration in emerging Asia is low. [2] However, two of the fastest growing markets, Philippines and Vietnam, grew at rates of 68.47% and 60.94%, respectively during the period 2007-2008 (SILVA, 2009). Overall, prices have come down making the service more affordable. A similar pattern is seen in South Asia (India, Pakistan, Bangladesh, Sri Lanka, Nepal, Bhutan, Maldives and Afghanistan). According to the ITU, the total number of fixed broadband subscribers has grown by 68.5% from 2007-2008 and the number of mobile broadband

[1] ITU definition for Broadband: Recommendation I.113 of the ITU Standardization Sector: "transmission capacity that is faster than primary rate Integrated Services Digital Network (ISDN) at 1.5 or 2.0 Megabits per second (Mbits)".

[2] This is according to the available data on ITU database, 2008.

connections grew by 218%. In between February 2008-February 2009, the price of a 256kbps fixed broadband connection has reduced in all South Asian countries (LIRNEasia, 2009, 2008). As shown in Figure 1, the biggest change in price was seen in Nepal and Bangladesh.

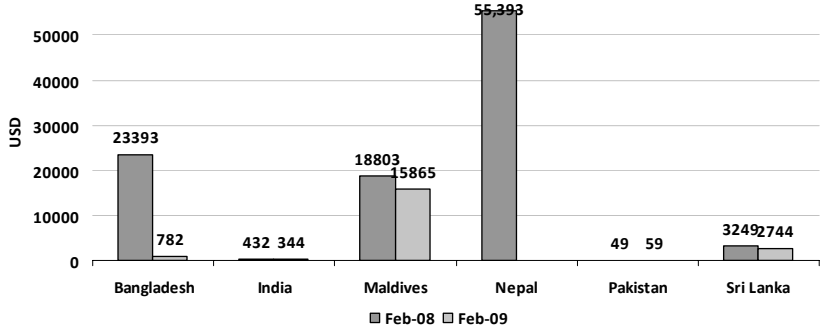
Figure 1 - Annual cost, 256kbps broadband business connection (unlimited download).



Source: LIRNEasia Broadband Benchmarks, February 2008, February 2009

The drop in retail prices in South Asia, as shown in Figure 1, has been made possible, in part, by a drop in wholesale prices though the price drops are not as large as the retail sector. The drop in wholesale prices between February 2008 and February 2009 is shown in Figure 2. Bangladesh exhibited the most significant drop.

Figure 2 - Annual cost, 2Mbps, 2km DPLC (tail cost) – Wholesale



Note: Data for Nepal for February 2009 is not available

Source: LIRNEasia broadband Benchmarks, February 2008, February 2009

The data, as shown above, depicts an increase in demand for broadband, yet increased demand and usage have posed challenges in

terms of Quality of Service Experience (QoSE) [3]. Complaints about quality have been voiced in the emerging markets for some time. User complaints are not the only thing driving interest in QoSE – there is increasing recognition that certain QoSE levels need to be maintained in order to enjoy the full economic and social benefits of broadband. As such, policy makers and regulators too have turned their attention to QoSE. Recently, the European Union commissioned a study on the quality of service provided within the region. [4]

The approaches taken by different regulators to monitor or ensure QoSE are quite different. Further in this paper, we examine these approaches and present a particular method that has been developed and tested by LIRNEasia and the Indian Institute of Technology, Madras (India). The paper also proposes a model that helps monitor QoSE with minimal regulatory action.

■ Different approaches of monitoring broadband QoSE

Even without strict regulations, broadband quality monitoring and benchmarking provides the necessary information for the users to make an intelligent choice in a competitive environment.

As noted, approaches to monitoring and regulating QoSE differ from country to country. Some countries use a mix of approaches. Table 1 classifies some of the commonly found modes of regulation.

---

[3] Quality of Service Experience (QoSE), used mainly in the field of telecommunications, is the actual measure of user's experience with an operator in terms of delivered quality with or without reference to what is being promised. This is measured technically and not subjectively. So it is different from Quality of Experience, sometimes also known as "Quality of User Experience," which is a subjective measure of a user's experiences with an operator. QoSE also differs from Quality of Service (QoS) which, in the field of computer networking and other packet-switched telecommunication networks, refers to resource reservation control mechanisms rather than the achieved service quality. Quality of service is the ability to provide different priority to different applications, users, or data flows, or to guarantee a certain level of performance to a data flow.

[4] The study has just been commissioned and the call for proposals can be found at the link: http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=5001&utm_campaign=isp&utm_medium=rss&utm_source=newsroom&utm_content=tpa-3 (accessed August 14 2009).

Table 1 - Different approaches to broadband QoSE monitoring/regulation

	Regulation/Monitoring approaches			
	Self Regulation by operators	Monitoring by regulators	User satisfaction surveys	Demand side (user) testing
Level of Intrusiveness (on the network)	None	High	None	Negligibly Low
Regulator participation	Medium to Low	High	Varies depending upon who conducts the surveys	None
Operator participation	High	High	Varies depending upon who conducts the surveys	None
User participation	None	Low	High	High
Subjectivity of results	Medium to Low	Low	High	Low

Source: Authors

Self regulation by operators

This mode is mostly used when quality is relatively better. The regulator expects self-regulation by operators instead of other stringent measures. Office of Communications of UK (Ofcom) had requested the broadband service providers to follow a voluntary code when promoting broadband speeds (Ofcom, 2008). It published a report in July 2009 on broadband, which compares advertised vs. actual speeds (PARKER, 2009).

Monitoring by regulators

Regulators are placed ideally to monitor broadband QoSE. They can play a key role in specifying the standards for operators and conducting frequent tests to make certain they are followed. Singapore is one of the few Asian countries which regulate broadband QoSE. Infocomm Development Authority (IDA), Telecommunication Regulator in Singapore, has been publishing quarterly data on the identified QoSE measures since 2006. The Telecommunication Regulation Authority of India (TRAI) and Malaysian Communication and Multimedia Commission (MCMC) have followed suit and has since published QoSE standards similar to Singapore.

All three regulators have specified the matrices:

- network availability,
- local network latency,

- international network latency,
- bandwidth utilisation.

The Indian and Malaysian regulators have included packet loss as an indicator. Non-compliance of these regulation leads to fines for the operators. Of the above matrices, network availability, latency and packet loss can be tested at the consumer end. However, bandwidth utilization information has to be provided by the operators. While the Singapore regulator allows operators to use up to 90% of the available bandwidth, the Indian and Malaysian regulators only allow up to 80%. IDA also specifies the permissible Round Trip Time (RTT) within the national segment of network and up to the first entry point in USA. [5] However, not every country has such regulatory arrangements to ensure broadband QoSE. The absence of a stringent regulatory environment in many developing countries makes it easier for telecom operators to use higher contention ratios there by lowering bandwidth than stipulated. Ordinary users, possessing neither the equipment nor the technical knowledge to ascertain this, most of the times have no alternative other than taking the word of the operator. Data for this is gathered from the supply side. Regulatory agencies are required to place necessary monitoring equipment in operators' or service providers' systems. This requires operator interaction and can be a cumbersome process. It can also be too costly in terms of equipments and personnel.

User surveys

User surveys, conducted either by the regulator (usually) or a third party (rarely) does not measure quality *per se*, but user perception. The users rank the operators based on their satisfaction/dissatisfaction of usage experience. [6]

[5] RTT *per se* is not a measure of the throughput of the link but indicates the bottlenecks in the path. For example, if the packets are pinged from Sri Lanka or India there will be a significant delay from the local exit point to the first international entry point. This is because the key issue these countries face is constraints in international bandwidth.

[6] Quality of Experience (QoE), some times also known as "Quality of User Experience," is a subjective measure of a customer's experiences with a vendor. Used typically by organisations providing services, such as hotels and hospitals.

Demand side (user) testing

Measuring the performance of the broadband service from the consumer end provides an alternative mechanism to quality monitoring by the regulator. No special equipments will be required for this except a software application that can measure the required metrics. The Web provides a gamut of applications that can be used to test the quality of a broadband link. GONSALVES & BHARADWAJ (2009) analyses some of the most popular testers including www.speedtest.net (what is popularly known as Speedtest), Speedtest2, www.speedtest2.com, and internetfrog, www.internetfrog.com. In addition, the report also does an overview of eight relatively less popular online testers.

The applications for testing QoSE of broadband were rated according to technical merit and the convenience of using the application. All three popular testers focus on download, upload and latency or ping. They are the metrics an average user is most familiar with. However, the absence of other parameters like jitter, packet loss and availability makes the testers technically incomplete as the test results give an incomplete picture. [7] Another drawback seen in all three testers is that it averages the data or results, regardless of whether or not the testing was conducted at peak or off peak times. This would undoubtedly give distorted results. In spite of its drawbacks the testers are relatively easy and quick to use and the results of the tests are displayed in graphical manner which makes it easy for a non-expert to understand.

To address some of the common drawbacks in these popular testers for measuring the broadband QoSE, a methodology to measure five metrics was designed by LIRNEasia and IIT-Madras. AT-Tester, a software application downloadable from www.broadbandasia.info is used for the testing.

■ User-centric methodology with AT-tester

The methodology developed by LIRNEasia and IIT-Madras falls into the 'user testing' category. It is an application that is available freely via web which can be downloaded and installed by users on their computers. The

[7] Commercial version of Speedtest measures jitter and packet loss.

AT-Tester software measures a total of five metrics: Throughput (download and upload speeds), Round Trip Time, jitter, packet loss and availability. Each is defined below:

Throughput (kbps)

Throughput is the "actual amount of useful data sent on a transmission" (DODD, 2005, p. 14). Defined by the ITU as "an amount of user information transferred in a period of time" (ITU, 1997, p. 15), more commonly referred to as download or upload speeds.

- Download speed is a key metric advertised in broadband services. It defines how much information a user receives.
- Upload speed defines the rate a user can send information to a server. It plays a significant role in responsiveness and real-time applications like VOIP.

Throughput varies depending on the location of the server that hosts the content. If the location is local, such as an ISP server, the throughput may be higher than it would be for an international server. Therefore the testing has included throughput for both local (ISP) and international servers.

Latency or RTT (ms)

"Latency refers to delays when voice packets transverse the network" (DODD, 2005, p. 60). This is significant in systems that require two-way interactive communication, such as voice telephony, or ACK/NAK [acknowledge/not acknowledge] data systems where the round-trip time directly affects the throughput rate, such as the Transmission Control Protocol (TCP). The ITU definition states that "Latency means transmission delay for FEC (Forwarding Equivalence Class) encoding, decoding, interleaving and de-interleaving" (ITU, 2004a, p. 9).

Jitter (ms)

"Jitter is uneven latency and packet loss" (DODD, 2005, p. 60). It is the variation of end-to-end delay from one packet to the next within the same packet stream/connection/flow. Jitter is more relevant for real-time traffic like VOIP. Ideally, the figure should be low.

Also defined by ITU as "Short-term non-cumulative variations of the significant instants of a digital signal from their ideal positions in time" (ITU, 1993, p. 6).

Packet Loss (%)

The ratio of packets that does not reach the destination to the sent. Degradation can result in noticeable performance loss with streaming technologies, VOIP and video conferencing. ITU states that:

> "In general, IP-based networks do not guarantee delivery of packets. Packets will be dropped under peak loads and during periods of congestion. In case of multimedia services, when a late packet finally arrives, it will be considered lost" (ITU, 2004b, p. 6).

Availability

The number of times the user is able to access the Broadband services. Availability = (1–F/T) x 100

Depending on the application, different combinations of the above metrics become important. Table 2 below gives the degree of importance of each metric with regards to different applications.

Table 2 - Importance of the matrices across applications

	Throughput		*Delay*		
Service	Download	Upload	RTT	Jitter	Loss
Browse (Text)	++	-	+	-	-
Browse (Media)	+++	-	+	-	-
Download file	+++	-	+	+	+
Upload file	-	+++	-	-	-
Transactions	+	+	++	+	+
Streaming Media	+++	-	+	++	++
VoIP	+	+	+++	+++	+++
Games	++	+	+++	++	++

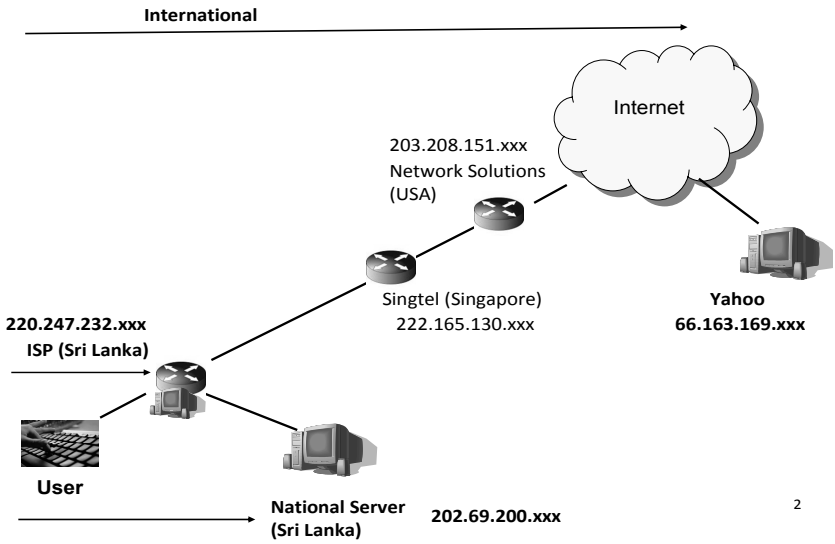
Note: +++ Highly Relevant ++ very relevant + relevant - not relevant

Source: GONSALVES & THIRUMURTHY, 2008

The above metrics are measured separately for three domains; ISP, national, and international. From the user to the Internet Service Provider (ISP) is the ISP Domain. (aka 'last mile' or 'first mile'). From the user to a website hosted within the geographical boundaries of the user's country is the National Domain. This is an important metric in countries such as Japan where most of the local content is hosted on local servers (i.e. within servers located within the country). Most of the content that a typical Japanese user accesses resides on servers within Japan, and language constraints prevent

most Japanese users looking for content elsewhere. For users from India or Bangladesh, this might not be the case given the lack of local content and higher percentage of persons speaking English. The final domain is the International Domain, defined as being from the user to a server or website hosted outside the country of testing. Figure 3 presents this information.

Figure 3 - Three domains of testing



Note: In the above example, the user is situated in Sri Lanka. The two ISPs shown (SLT and Dialog) are shown in Sri Lanka (the user's own ISP is SLT, while Dialog is a competing ISP). International content may be accessed from Singapore or USA (as shown) or any other location outside of Sri Lanka.

Source: LIRNEasia

■ Volunteer computing as a means of data gathering

The LIRNEasia/IIT Madras broadband QoSE monitoring project was largely based on the concept of Volunteer Computing for data gathering purposes.

Volunteer computing is defined as "a form of distributed computing in which the general public volunteers processing and storage resources to computing projects" (ANDERSON, 2009, p. 1). It becomes necessary as computationally intensive research activities require outside resources. It

allows researchers to use the resources (such as processing speeds and storage capacity) of computers connected via the internet, that would be otherwise unavailable to them (TOTH & FINKLE, 2007). One of the first projects to benefit from the volunteer computing is 'Great Internet Mersenne Prime Search', (GIMPS) [8], a mathematics project on finding the prime numbers. The project began in 1997. According to ANDERSON & REED (2009) volunteer computing is now used in a wide variety of fields; physics, molecular biology, medicine, chemistry, astronomy, climate dynamics, mathematics, and the study of games. Most typically, volunteer computing is used either in academic or popular public interest projects like climate change and cancer research. CHRISTENSEN *et al*. (2005) details how volunteer computing has aided in the research into climate change. In one of the most popular 'volunteer computing' modes, volunteers are required to download a software application from a project website and install it. From there on the processes are largely automated where the software does the required tasks of computations, communicating with the main server and uploading the results. In the initial stages that involved some human interaction. Now most of the tasks are automated.

Volunteer computing requires a trust between the volunteers and the project managers. Anonymous volunteers will not and cannot be held accountable for incorrect data. In turn, the volunteers trust the project to be within legal standards such as security, privacy and intellectual property laws. In spite of the advances in the relative ease of taking part in a volunteer computing, it has been estimated that only about 1% of world's computers participate in it. As the literature suggests, obtaining volunteers is easier when the project holds public appeal Volunteer computing Projects should be designed to ensure minimum inconvenience to the volunteers. (CHRISTENSEN *et al*., 2005).

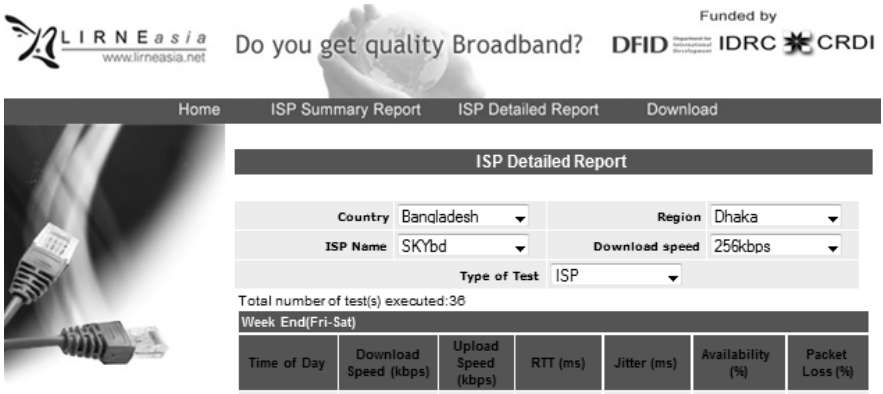
■ Volunteer computing in broadband QoSE measurements

Inherent interest of users to know the quality of their broadband links was the foundation for the LIRNEasia/IIT Madras research project. The AT-Tester assumed therefore that the general public would be interested in

[8] More details about the project can be found in their website; http://www.mersenne.org/. Accessed on 2 September 2009.

downloading, installing and running a software that enables them to measure broadband quality. Provided that the process was user-friendly and the application (and provider) was trustworthy.

Figure 4 - Sample test report from broadbandasia.info



ISP Detailed Report

Country: Bangladesh | Region: Dhaka
ISP Name: SKYbd | Download speed: 256kbps
Type of Test: ISP

Total number of test(s) executed:36

Week End(Fri-Sat)

Time of Day	Download Speed (kbps)	Upload Speed (kbps)	RTT (ms)	Jitter (ms)	Availability (%)	Packet Loss (%)
8:00 AM	253.15	110.91	34	0.43	100	0
11:00 AM	219.17	117.69	39.33	0.6	100	0
3:00 PM	230.85	110.56	35	0.17	100	0
6:00 PM	232.53	149.39	32.67	0.63	100	0
8:00 PM	229.76	120.45	40	0.7	100	0
11:00 PM	246.59	123.95	25.67	0.27	100	0

Week Day(Sun-Thu)

Time of Day	Download Speed (kbps)	Upload Speed (kbps)	RTT (ms)	Jitter (ms)	Availability (%)	Packet Loss (%)
8:00 AM	252.19	118.88	36.33	0.5	100	0
11:00 AM	230.99	96.19	36.33	0.53	100	0
3:00 PM	219.2	94.67	46.33	0.5	96.67	0
6:00 PM	211.39	95.04	24.33	0.43	100	0
8:00 PM	222.35	93.63	27	0.27	100	0
11:00 PM	242.77	89.65	29.67	0.6	100	0

* We have given here all possible speeds. Please note some of them might not be offered by your ISP.

Source: www.broadbandasia.info

The value of the tester lies not just in getting a user to test his or her connection quality. Rather to enable the user to compare his/her metrics with a group of other users (or an average).This is facilitated by having the measurement data automatically uploaded to the website (www.broadbandasia.info, the same website from where the user downloads the application from). The user of the software (or anyone else, for that matter) is then able to view the data reported by all other users. Results are available on country and city basis, where applicable. The averaged results of all tests conducted are reported. Figure 4 shows a sample of data from Bangladesh. The key to success of course is in having as many users reporting data as possible.

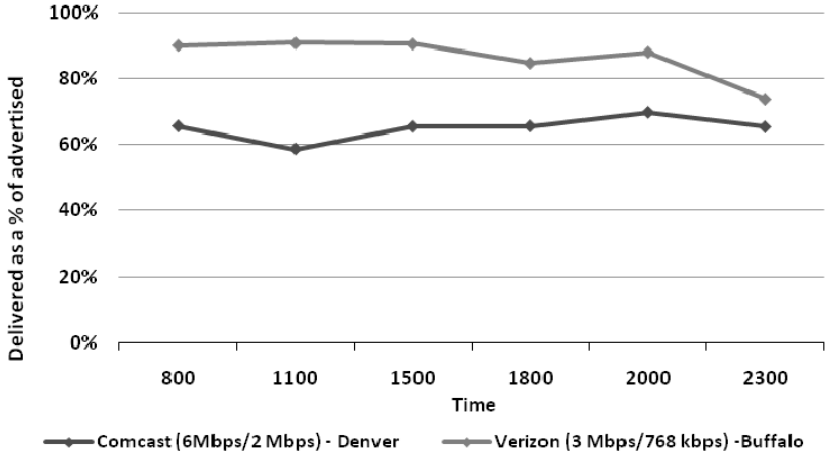
■ Examples of data analysis

The project was initiated in 2008 when the AT-Tester software was first developed and used. The project has been continuing since. QoSE information on broadband packages of several countries has been recorded since then. Given that the project is still in early stages, not all data comes from volunteers. At times the research team from LIRNEasia had to employ testers in order to ensure that data from multiple locations were collected at the same time, in order to facilitate benchmarking. The following are examples of the type of information that can be extracted by analyzing the data gathered and the policy interventions it could lead to.

Results for the USA

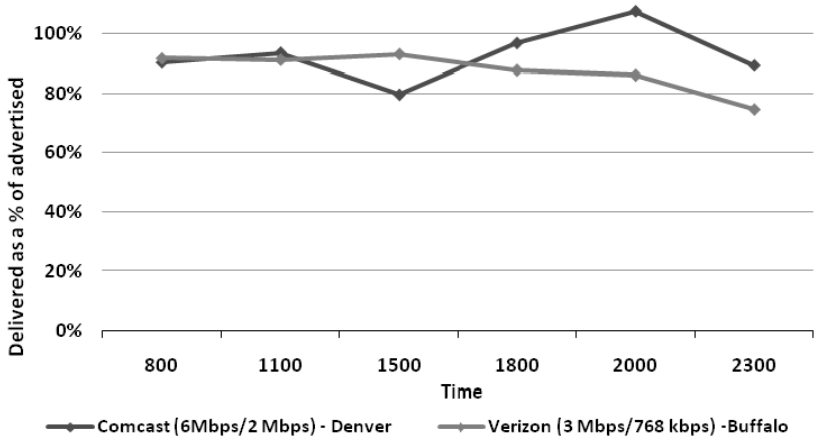
In USA, QoSE results for two unlimited broadband packages, in two cities are available, Verizon and Comcast. Comcast, tested in Denver, has an advertised download speed of 6 Mbps and upload of 2 Mbps and it is priced at USD 59.95 per month. Verizon, tested in Buffalo, New York has an advertised download and upload speeds of 2Mbps and 768 kbps respectively and a monthly cost of the connection is USD 29.99. The tests were conducted in August 2009, 6 times a day in order to capture the peak and off peak times. The download test results (as percentages of advertised speeds) are given in Figures 5, 6 and 7

Figure 5 - Download from ISP domain – US operators, August 2009



Source: LIRNEasia test results, August, 2009

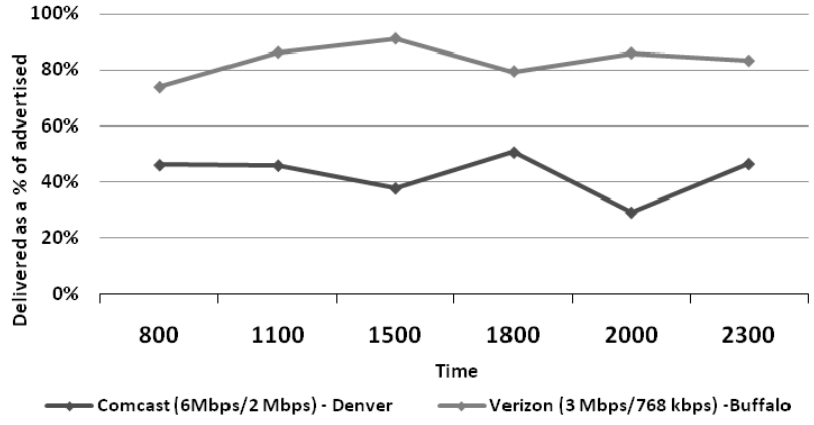
Figure 6 - Download from national domain – US operators, August 2009



Source: LIRNEasia test results, August, 2009

In all three graphs, Figures 5, 6 and 7, the download speed data shows Verizon performs better than Comcast. This is more significant in the international segment. Ideally, the speeds should have been close to 100%, but no serious performance drops are observed.

Figure 7 - Download from international domain – US operators, August 2009

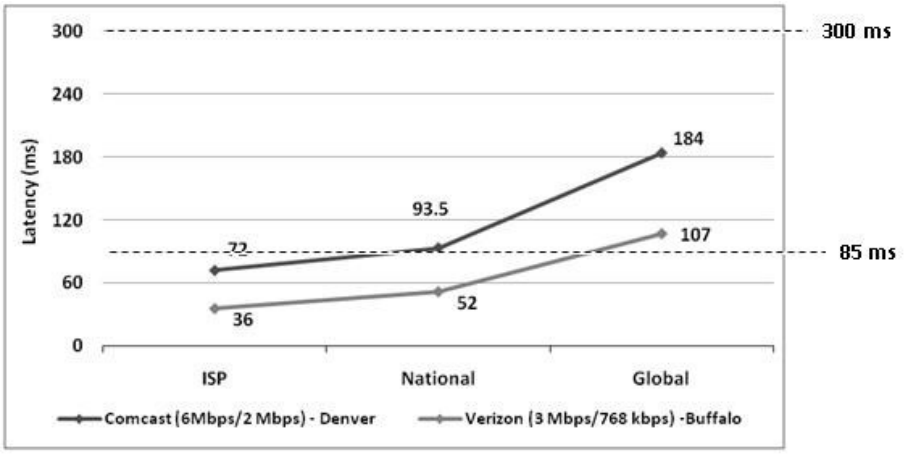


Source: LIRNEasia test results, August, 2009

Performance is seen falling below 75% for Comcast in Figure 7. Its users might experience this drop in quality when accessing an international server.

This indicates possible bottlenecks in the trans-Atlantic link used by Comcast.

Figure 8 - Round trip time to ISP, national and international domains (in ms) US operators, August 2009



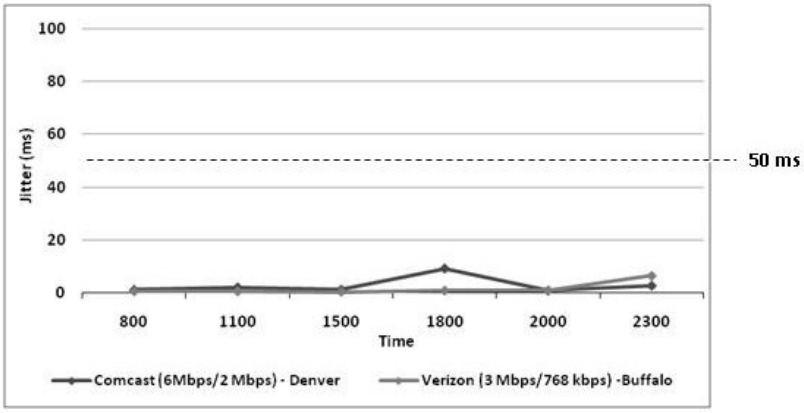
Source: LIRNEasia test results, August, 2009

A typical download speed graph for a package not prone to congestion, shows drops during 'peak' periods, usually around 11 am (business peak) and anytime between 6 pm to 11 pm (residential peak). Absence of such an inverted hump characteristics mean the networks are not overly congested, or right contention ratios are applied. Latency (RTT) plays a major role in the real time or interactive applications. The specified limit for the Singaporean operators by the Infocomm Development Authority (IDA) is 85 ms for local network segment and 300 ms for international segment (until the first entry point to USA from Singapore.) Out of the two US operators, while Broadband Verizon complies with both, Comcast meets the national standard only in certain cases (NB. USA is taken as the 'international' destination for users from most of the countries. For USA and Canada, Germany is taken as the 'international' destination, representing a server in Europe). Neither universal acceptance levels nor national standards exist for jitter and packet loss. The limits depend upon the applications too. Ideal will be 0 ms jitter and 0% packet loss. For practical purposes LIRNEasia has adopted 50ms and 3% as standards. Performances of both operators are within these overall limits.

Based on the above results (which are all within reasonable or acceptable range), there is little need to call for policy interventions. The only

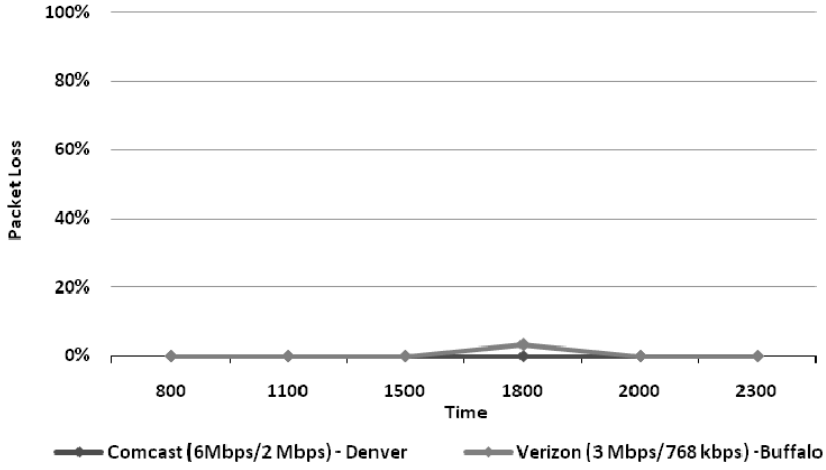
improvement might be to expand the international link capacity for Comcast in order to obtain better download speeds when accessing content overseas. [9]

Figure 9 - Jitter when pinged to the international domain (in ms)
US operators, August 2009



Source: LIRNEasia test results, August, 2009

Figure 10 - Packet loss when pinged to international domain – US operators, August 2009



Source: LIRNEasia test results, August, 2009

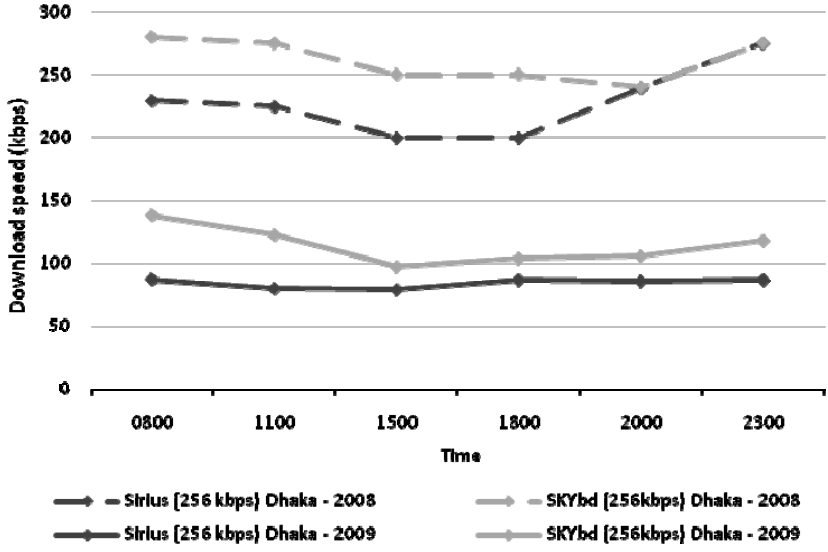
[9] However, given the propensity for even international data to be hosted in the US, it is likely that the International Domain is the least accessed by US-based broadband users.

Results from South Asia

The results of testing from South Asia, in contrast, show that there is much to be desired, and therefore point at opportunities for regulatory intervention. Under its Rapid Response program LIRNEasia makes quick responses to specific requests for training/advice by governments/entities in the region on telecom policy and regulatory issues. One form of response is a written submission (e.g., to a public consultation or to media). On several occasions data from broadband QoSE database has been used as the basis of these rapid responses.

Bangladesh: Comparing the tests done in September/2008 to the ones done in February 2009 in Dhaka, Bangladesh showed a marked deterioration in download speed within these 6 months (Figure 11). These results were used in the policy recommendations made by LIRNEasia to Bangladesh Telecommunication Regulatory Commission (BTRC) in August 2009.

Figure 11 - Download speed in international domain, Bangladesh

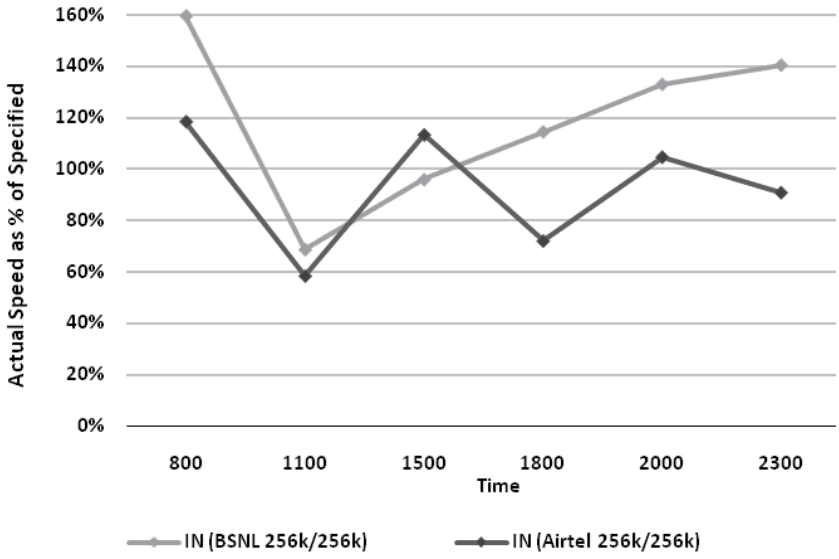


Source: LIRNEasia Broadband Test Results, Sept 2008 and Feb 2009

The possible reasoning was the immediate expansion of the broadband user base in Bangladesh, following the rapid drop in prices (Please refer Figure 1), perhaps without allowing the operators to expand their infrastructure. LIRNEasia recommended the approach regulators should

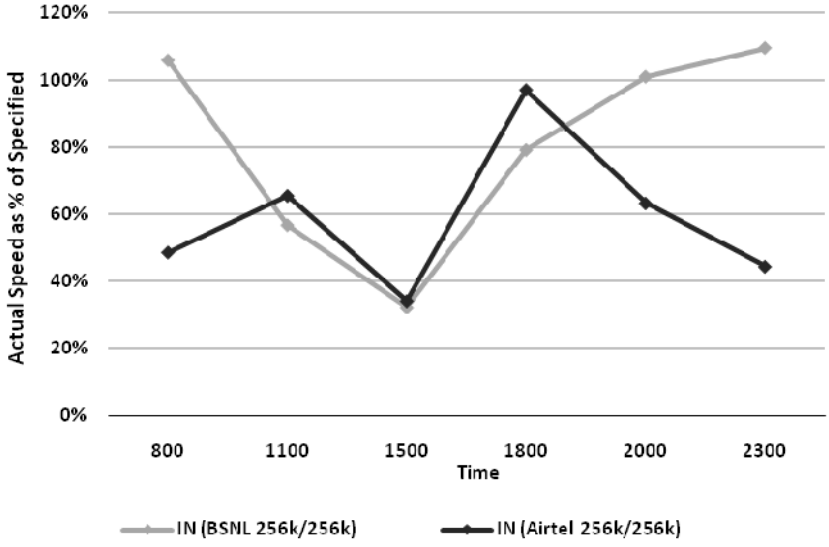
take in adopting broadband regulatory measures based on its experiences in QoSE research in South Asia.

Figure 12 - Download speed in ISP domain for Chennai



Source: LIRNEasia test results, Sept 2008

Figure 13 - Download speed from international domain for Chennai



Source: LIRNEasia test results, Sept 2008

India: Recommendations were made to Telecommunication Regulatory Authority in India (TRAI) also based on the erratic patterns observed in download speeds offered by the Indian operators.

Prima facie, this appears a case of over-delivery but only because TRAI has specified the local operators to advertise based on the minimum speeds rather than a range. In spite of the higher percentages, in actual terms the speeds are low and behave in an erratic pattern. This normally happens when there are significant variations in the number of users sharing the same link. LIRNEasia's key recommendation here was to specify the contention ratios, 1:20 for business and 1:50 for residential, for the operators. They have adopted 1:30 (business) and 1:50 (residential).

■ Observations on the use of volunteer computing model

The following are the observations for a period of nearly a year of operation:

- The response rate was not as high as expected. The anticipated level of traffic, based on the presumed broadband user activism in South Asian countries was not seen. The data received now largely appears to be from one-time users. [10]
- The model seems to work better for certain countries than the rest. Response rate is best for Sri Lanka and India.
- The number of requests to register for testing is higher than the number of tests completed [11], as indicated by the site statistics, than the number that completes the process.
- More test results are observed being fed immediately after the awareness creation workshops by LIRNEasia and IIT Madras.

It is too early to deduce the success/failure of the model. The low rate of response can be due to multiple reasons. Perhaps activism *per se* was not adequate to entice users to contribute the anticipated time and effort. It also may be due to less awareness. Some users have commented on the

[10] Since it is not mandatory for a user to input results to the database, the number of records in the database is not a reflection of the number of tests conducted, which has to be higher.

[11] The application needs pre-registration. The user has to provide the ISP, country and package information.

aspects of user-friendliness of the software application. The need for first time registration discourages many users but it is essential as the ISP information needs to be fed to the system. It cannot be the user's responsibility for two reasons. An ordinary user might not be aware of the technical details of the ISP. Then it is too risky to entirely depend on the data fed by a volunteer with no guarantee about the accuracy.

■ Conclusion

LIRNEasia has used the data gathered through the AT-Tester software application for four rapid responses it made to South Asian regulators for policy intervention purposes. Two of these are shown above. Though not all data gathered was through volunteer computing, this illustrates the potential.

The volunteer model as it is might not be the best for an exercise of this nature. The additional time and effort, compared to other examples that use the same model makes a big difference. Users cannot be expected to make this contribution without any return. They need to be compensated, not necessarily in financial terms, but at least in kind.

The other improvement can be awareness creation. It will not be practical to expect users to spend time doing a test on a site they find on a casual search. A casual user does not fit into the ideal profile of a 'volunteer'. Rather the volunteers need to be carefully nurtured. Awareness creation plays a major role there. Increase in the response rate following awareness creation workshops indicates that would be a good exercise, but other modes too can be tried.

Overall, these trends suggest the need to slightly deviate from the volunteer computing model. Participation requires the broadband users to contribute both his/her time and computer resources to the project.

References

ARBORE, A. & ORDANINI, A. (2006): "Broadband Divide Among SMEs The Role of Size, Location and Outsourcing Strategies", *International Small Business Journal*, 24(1), 83-99.

ANDERSON D.P. & REED, K. (2009): Proceedings of the 42nd Hawaii International Conference on System Sciences: *Celebrating Diversity in Volunteer Computing*, Hawaii, USA, 5-8 January 2009.
http://boinc.berkeley.edu/boinc_papers/hicss_08/hicss_08.pdf (accessed August 20 2009).

CHRISTENSEN, C., AINA, T. & STAINFORTH, D. (2005): Proceedings of the 1st IEEE Conference on e-Science and Grid Computing, *The Challenge of Volunteer Computing With Lengthy Climate Modelling Simulations*, Melbourne, Australia, 5-8 Dec 2005. http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1572203
(accessed Sept. 1 2009).

DODD, A. (2005): "The Essential Guide to Telecommunication" Fourth Edition, Pearson Education.

GONSALVES, T.A. & THIRUMURTHY, R. (2008): "Broadband Quality of Service", Presented at the Expert Forum on ICT Sector Indicators and Benchmarks Regulation, 15 June 2008, Singapore. http://lirneasia.net/wp-content/uploads/2008/06/broadbandqosv30.pdf (accessed August 18 2009).

GONSALVES, T.A. & BHARADWAJ, A. (2009): *Comparison of AT-Tester with Other Popular Testers for Quality of Service Experience (QoSE) of an Internet Connection*. http://lirneasia.net/wp-content/uploads/2009/09/AT-TesterComparison.pdf (accessed September 2 2009)

ITU:

- (1993): "ITU-T Rec. G.701 (03/93) General Aspects of Digital Transmission Systems". http://www.itu.int/rec/T-REC-G.701-199303-I/e (accessed August 15 2009).
- (1997): "ITU-T Rec. X641 (12/97) Information technology – Quality of Service: Framework". http://www.laas.fr/~eexposit/pmwiki/pmwiki.php/Refs/Main?action=download&upname=X.641.pdf (accessed August 15 2009).
- (2003): "Birth of Broadband, Frequently Asked Questions". http://www.itu.int/osg/spu/publications/birthofbroadband/faq.html (accessed August 15 2009).
- (2004a): "ITU-T Rec. G.972 (06/2004) Definition of terms relevant to optical fibre submarine cable systems". http://veri.library.ncnu.edu.tw/itu-t/ORIGINAL/G/T-REC-G.972-200406-I!!PDF-E.pdf (accessed August 15 2009).
- (2004b): "ITU-T Rec. H.360 (03/04) An architecture for end-to-end QoS control and signalling". http://www.itu.int/rec/T-REC-H.360-200403-I/en (accessed Aug. 15 2009)

KANG, C. (2009): "FCC Broadband Proposal May Miss Out on Stimulus: Networks May Be Built Ahead of Policies", *The Washington Post*, April 8.
http://www.washingtonpost.com/wp-dyn/content/article/2009/04/07/AR2009040703996.html
(accessed September 2 2009).

KRUGER, L.G. & GILROY, A.A. (2008): "Congressional research service report for Congress, order code RL30719 Broadband internet access and the digital divide: federal Assistance program".
http://www.nationalaglawcenter.org/assets/crs/RL30719.pdf (accessed Aug. 18 2009)

LIRNEasia:

- (2009): *Broadband Benchmarks*.
http://www.lirneasia.net/wp-content/uploads/2007/08/lirneasia-broadband-prices-emergingasia-feb-2009.pdf (accessed August 15 2009).

- (2008): *Broadband Benchmarks*. http://lirneasia.net/wp-content/uploads/2008/07/broadband-benchmarks-dimuthu1.pdf (accessed August 15 2009).

OECD:

- (n.d.) "OECD Broadband Subscriber Criteria".
http://www.oecd.org/document/46/0,3343,en_2649_34225_39575598_1_1_1_1,00.html (accessed August 15 2009).

- (2008): "Broadband Growth and Policies in OECD countries".
http://www.oecd.org/dataoecd/32/57/40629067.pdf (accessed August 29 2009).

Ofcom (2008): "Voluntary Code of Practice: Broadband Speeds". http://www.ofcom.org.uk/telecoms/ioi/copbb/copbb/copbb.pdf (accessed September 4 2009)

PARKER, A. (2009): "Ofcom reveals lagging broadband speeds", *Financial Times*, July 28. http://www.ft.com/cms/s/0/57142ecc-7aee-11de-8c34-00144feabdc0.html?nclick_check=1 (accessed September 2 2009).

Partnership for Measuring ICT for Development (2009): "Revisions and additions to the Core list of ICT Indicators". http://www.itu.int/ITU-D/ict/partnership/material/CoreICTIndicators_e_rev2.pdf (accessed August 18 2009).

RAMIEREZ, R. (2007): "Appreciating the Contribution of Broadband ICT with Rural and Remote Communities: Stepping Stones Toward an Alternative Paradigm", *The Information Society*, 23: 85-94.

SILVA, V. (2009): "Asia Leads in Broadband Growth", *The Industry Standard*, June 20. http://pcworld.about.com/od/networkin1/Asia-Leads-in-Broadband-Growth.htm (accessed September 2 2009).

TOTH, D. & FINKEL, D. (2007): Proceedings of the 6th WSEAS Int. Conf. on Software Engineering, Parallel and Distributed Systems, *Characterizing Resource Availability for Volunteer Computing and its Impact on Task Distribution Methods*, Corfu Island, Greece, February 16-19 2007.
http://portal.acm.org/citation.cfm?id=1353821 (accessed August 25 2009).

Websites

www.broadbandasia.info
www.speedtest.net
www.speedtest2.com
www.internetfrog.com.
http://www.mersenne.org

Features

- ☐ Regulation and Competition
- ☐ Firms and Markets
- ☐ Technical Innovations
- ☐ Public Policies
- ■ **Use Logics**
- ■ **Book Review**

Use Logics

Digital Confidence: Bases of Trust and Impact on Usages (*)

Sophie LUBRANO
IDATE, Montpellier, France

Use of Internet has intensified, especially, in the field of commerce, social networks, but also in administration or banking, which implies numerous transmissions of personal information online.

These new practices generate new risks which the consumer may or may not perceive, but that could hinder development of the digital economy. What are online consumer fears? How could the consumer be reassured? And what is the real impact of confidence on uses? Would they trust a centralized identity-management service?

We investigate these questions, and try to address them using the results of a survey conducted in France in 2009 on behalf of CDC.

Having their bank accounts hacked is the main fear, even for non-internet users

Different types of risks are identified by the customers regarding online activities:

(*) This article is based on a study conducted by IDATE on behalf of CDC in 2010 about the digital confidence of French people. During this study, IDATE held a survey among French people, Internet users as well as non-internet users. The aim was to identify the main criteria on which digital confidence is based, and their impact on uses.

- The main risk identified is to have their bank account hacked and money stolen. Nearly one internet user in two (45%) estimates that online shopping increases the risk of being hacked. According to another survey [1], in 2010 in France more than 50 000 people have had their computers hacked, for an average loss of 2000 EUR.

- The second risk is more related to privacy: the danger that other people could access one's bank account, personal information related to administration (tax return, social welfare), or personal tastes and hobbies in the social networks. For instance, about ¼ of people (22%) fear that someone else could access their bank account online.

- Overall, technical risks are not high on the list of user fears: about 4% of people estimate that the website could malfunction.

Table 1 - Risks identified by online customers

	Internet users	*Non internets users*	*Total*
E-Commerce			
Hacking of bank data	45%	38%	43%
Someone else having access to personal data	26%	21%	25%
Website malfunction	5%	6%	5%
E-Banking			
Hacking of bank account	20%	33%	24%
Someone else having access to my bank account	24%	18%	22%
Website malfunction	4%	2%	4%
E-Administration			
Personal information used without permission by someone else	9%	16%	11%
Personal information accessed without permission by someone else	9%	15%	11%
Risk of identity error	5%	10%	7%
Website malfunction	4%	5%	4%
Social Network			
Private life is not sufficiently protected on social networks (% saying "yes") (*)	32%		21%

(*) IFOP Survey 2010

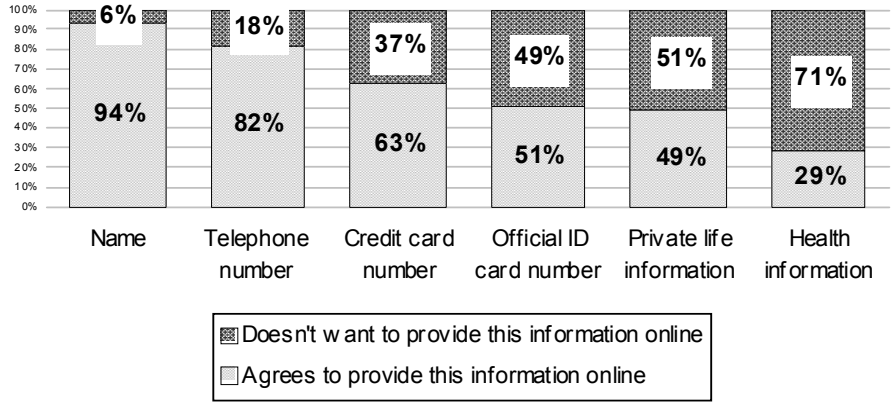
Source: IDATE/CDC survey on digital confidence 2009

1 Credoc Survey, 2010.

Security needs depend on the type of personal data involved

People do not have the same security expectation, depending on the type of personal details: they usually agree on giving their name or telephone number online, but are more reluctant to provide official credit card or ID card number, or private life information. And they are unwilling to provide information regarding their health. Security needs varies depending on the "intimacy" level of the data.

Figure 1 - Type of attributes internet users would be ready to provide online



Source: CDC/IDATE survey 2009, base: internet users

What are the foundations of internet user trust?

Experience is a good yardstick, and the service provider is an another pillar of trust

There are several ways to create a climate of trust:

- Trust is primarily based on service provider reputation, especially for e-commerce: in France, 71% of internet users declare that they place their confidence in well-known merchant sites; regarding e-banking or e-administration, users trust banks and administration in general.
- The second trust builder derives from good experience on the web sites: regarding e-administration, 47% of internet users say they put their trust in websites offering a positive experience.

- Technical guarantees are also important: regarding e-commerce, 55% of internet users say they base their confidence on technical guarantees.

- Lastly, recommendations made by other users are not really crucial as people prefer to trust their own experience.

Table 2 - Reasons of having confidence in online services

	E-Commerce	*E-Banking*	*E-Administration*
Well-known e-commerce websites Confidence in banks or administrations in general	71%	51%	43%
Good experience with the website / Trusted relationship with the website	30%	28%	47%
Technical warranty	53%	55%	44%
Recommendation of other users	15%	5%	7%

Base: internet users, CDC/IDATE survey 2009

The Public sector is more reassuring than the private sector

People place greater trust in public institutions such as government or local authorities than in private sector players: in France, more than half of internet users would provide their phone number to the government or banks, but only 1/3 to a merchant website. Social networks benefit from a relatively low level of trust: only 9% of internet users would provide their phone number on a social network.

What impact of confidence on uses?

Even though people have identified risks on the web, they still use online services, which implies personal detail transmission on the net:

- In developed countries, between 60% and 90% of internet users have already bought online

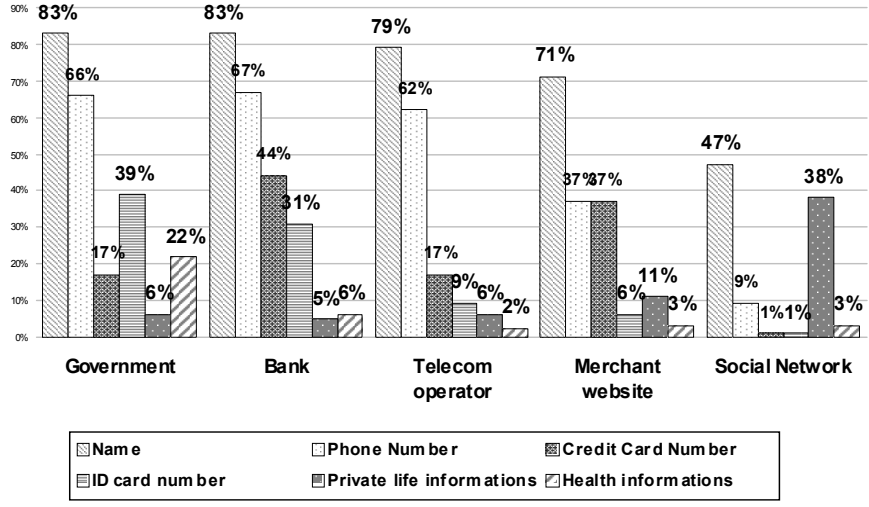
- In developed countries, between 50% and 60% of internet users manage a profile on an existing social network

- In France, 80% of internet users access their bank account online, and 60% have made tax returns online

The level of trust does not directly impact uses; for instance in France, 51% of internet users estimate there is a risk inherent in shopping online, but

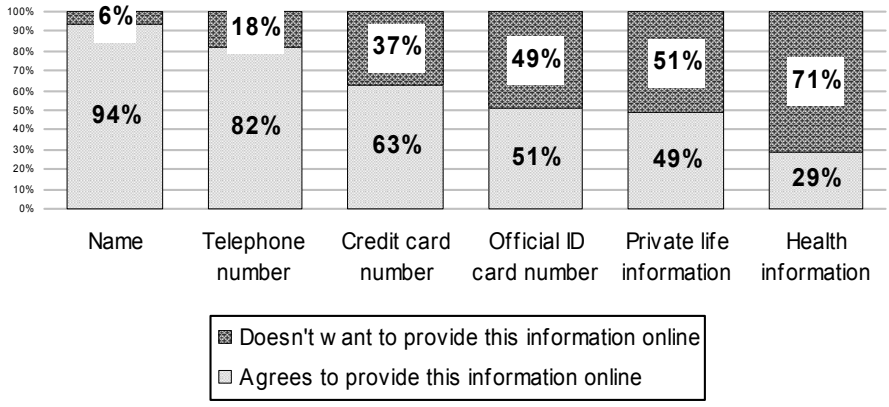
85% still do so: the benefit obtained outweighs the risk. As we have seen before, Internet users have deployed strategies to manage risks.

Figure 2 - Legitimacy of actors by attribute type



CDC/IDATE survey 2009, base: internet users

Figure 3 - Comparison between confidence rate and use rate



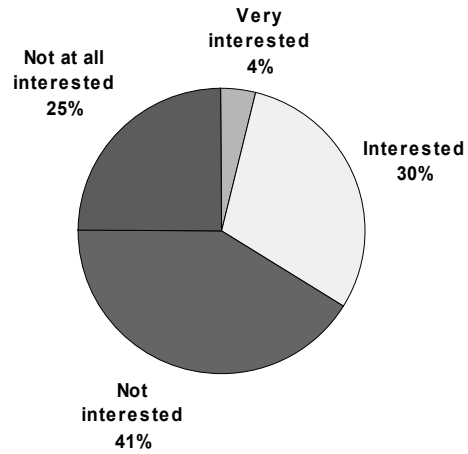
Source: CDC/IDATE survey 2009, base: internet users

What about centralized identity management services?

Regarding a centralized service used for identity management, more than one internet user out of four is interested, but only 4% are very interested. Even though people perceived the practical advantages, especially not having to fill out data forms time and time again, they do not trust centralized services: 60% would not trust the security provided, and 34% fear losing everything.

As seen before, people do not really trust private players to provide such a secure service: 84% trust government and only 10% trust social networks.

Figure 4 - Interest in a centralized identities management services (*)



(*) Defined as a service which allows access to personal datas in multiple services with only one identification and authentication.

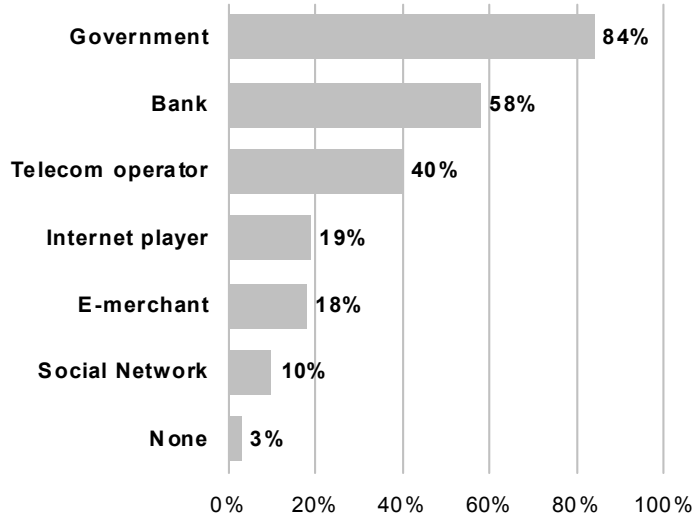
Source: CDC/IDATE survey 2009, base: internet users

Table 3 - Perceived advantage/disadvantage of centralized service

Service triggers	*Brakes for users*
Reduces refilling information forms (62%) Avoids inputting many passwords (54%) Provides access to multiple services (27%) Limits data completion tasks (25%) Secures personal informations (21%) Provides more security (13%)	User prefers to keep multiple identities (63%) Lack of trust in security (60%) Wary of centralized service (57%) No real usefulness (46%) Fear to losing everything (34%) Lack of trust in technology (28%) Prefer to manage it themselves (5%)

Source: CDC/IDATE survey 2009, base: internet users

Figure 5 - Player estimated legitimated to provide centralized service



Source: CDC/IDATE survey 2009, base: internet users

In conclusion

Even though they have identified many risks while using online services, the benefit of online services is estimated to outweigh the threats. Internet users have strategies to lower risks, such as using well-known websites or public institutions. Governments have a role to play, insofar as they could reassure internet users and thereby foster digital economy development.

Methodology of the survey

- Sample: 1000 interviews (700 internet users online, 300 non-internet users by phone)
- Samples structured by quotas
- Target: More than 15 year-old people
- Date: October 2009

Book Review

By Richard HAWKINS and Isabelle POTTIER

■ **Philip M. NAPOLI**
Audience Evolution
New Technologies and the Transformation of Media Audiences
New York: Columbia University Press, 2010
by Richard HAWKINS

We live in an era when almost daily some new challenge emerges to what, for a couple of generations now, communications scholars have referred to as the media industries. In this very concise, tightly argued and very timely volume, Philip Napoli makes an important contribution to understanding these industry dynamics in the current milieu and, indeed, raises many pertinent questions as to whether the "new media" have much connection to "media" as they have been understood in the past. In pursuing this point, and in contrast to a prevailing emphasis upon technology as the driving force for these changes, the author focuses instead upon audiences and how their relationships with technology evolve. The focus on the social construction of audiences, rather than of technology or organizations, offers a refreshingly different perspective and the author explores it a provocative and scholarly way.

Napoli is careful to ground his analysis in a long tradition of critical media studies concerning the media-audience relationship, and does not make the all too common error of assuming that just because the technological environment evolves, previous observations and theories about the forces engaged in that environment somehow become irrelevant. Instead, he reintroduces and re-interprets the ideas of several leading media scholars of the 1970s and 1980s in this new context. In particular he draws attention back to the "audience commodity" debate, instigated by the ideas of Dallas Smythe, and taken up by Jhally, Liess, Murdock, Livant and many others. It is striking how these ideas, conceived at a time when television was the most advanced technology available to most consumers, and which sounded overly radical and polemical to many scholars of the day, appear in many ways to fit current developments like a glove. After all, what are You Tube and Facebook users doing if not directly producing the commodities that sustain these enterprises? And producing them "in substance"! This is

emblematic of Napoli's central hypothesis that in order to understand how the media are evolving, you have to look first at how the audience is evolving as a factor of production.

For this reviewer at least, the key stand-out message in this book concerns not so much the relationship between audiences and evolving technology, but the role of measurement, not only in exploring audience characteristics and dynamics, but in defining and redefining what an audience is to the complex cluster of business enterprises that constitute "the media" as conventionally understood. Napoli's basic proposition here is that the goal of media as a business has changed from, as he puts it, "reaching as many eyeballs as possible", to understanding and exploiting the *qualities* of a multitude of relationships between audiences and media. He then tracks the practice of audience measurement since early in its inception, noting that early decisions to focus on measuring audience size were predicated more on how analysts had come to define "audience" than on the lack of ability to measure other aspects. When considering the implications of the marriage between rapidly advancing data techniques and the availability of massive amounts of virtually nano-level data about everyone and everything, Napoli's observations and arguments are salutary. Many have commented upon the now ingrained data fetishism of contemporary practice in management and policy, and on the problem of over-interpreting the accuracy of any measurement, especially where hideously complex social relationships and patterns are concerned. Napoli opens the door to an intriguing possibility that, at some point, the contemporary media could be strangled by its own data much as its predecessors appear to have been. Thus, he offers a challenge to scholars not to become too enamored of the exploding range of technical possibilities to explore audience behavior, and not to let them inject the same kinds of data-driven biases into their analysis that bedeviled much earlier scholarship on media audiences.

Perhaps the one point that this reviewer found somewhat odd, is that throughout the book, the author anchors discussion of the media-audience relationship almost exclusively in or around "content". This is effective insofar as certainly the nature and scope of "content" has changed dramatically. Arguably, however, the individuals who make up the audience for content also use the core digital technologies and devices for many purposes that are not associated necessarily with content consumption in either the old or the emerging new meanings. A tendency can be seen, explicitly or by implication, to tag every form of IT usage as content consumption, which in the end may be too broad to be useful analytically. We might also consider, for example, that the business models surrounding most electronic devices involves instigating a level of engagement between users (audiences?) and the device (e.g. through perpetual learning curves and cycles of updates and obsolescence) that establishes a powerful, interactive and lasting relationship over and above the apps or services as

such. The part of Napoli's argument that was missing for me, or not as well advanced, concerns the relationship between the content industries and the equipment, infrastructure and device industries, and specifically where the borders might lie, or not, between the use of technology and the consumption of content.

To conclude, this is a book that will appeal not only to scholars in audience research, media marketing and communication, but also to professionals in various industry sectors and in the public services. There is a significant "public interest" dimension to this book in that it illuminates evolving practices in contemporary media that have implications for the privacy, security and property rights of individuals. Although the policy issues are discussed only in a US context, readers in other countries surely will recognize the essence of the arguments as they pertain in other jurisdictions. The volume would be an ideal candidate in my view for selection as a text for senior undergraduate and graduate courses in media analysis and management. The extraordinarily comprehensive and well balanced bibliography alone is worth the price of the book. As a whole package, the book provides an invaluable roadmap to further scholarship in this important and dynamic field.

■ Daniel LE METAYER (Ed.)

Les technologies de l'information au service des droits : opportunités, défis, limites (Putting Information Technology at the Service of Rights: Opportunities, Challenges, Limitations)

Publisher: Bruylant (Bruxelles), December 2010, ISBN 978-2-8027-2960-0
Collection *Cahiers du Centre de recherche informatique et droit* (CRID) no. 25, Namur (Belgium)

by Isabelle POTTIER

This book, result of a symposium on the PRIAM (*) project, focuses on how to use information technology in the service of law. Can we develop tools that can enhance people's rights? Is the use of information technology raising many questions for lawyers and IT professionals? It also addresses general questions about law and technology: how can tools actually strengthen law/rights? How far can they be used? What technical and legal constraints must be imposed to avoid jeopardizing the safety or legal rights of individuals? These questions are followed by specific questions on digital goods, digital rights management and protection of copyright, protection of

(*) PRIAM : PRivacy Issues in AMbient intelligence. Collaborative project funded by INRIA and involving teams from INRIA (ACES, AMAZONES and LICIT), Faculty of Law, Saint Etienne and the University of Twente.

privacy and protection of the security of medical data. The book addresses them all by analyzing the (actual or potential) contribution of information technology both in sensitive areas such as data protection or the protection of digital goods, and in the activities of legal practitioners (legal drafting, helps to resolve disputes, etc.).

Les technologies de l'information au service des droits : opportunités, défis, limites is published by Bruylant in the collection des *Cahiers du Centre de recherches informatique et droit* (CRID). CRID is a research centre dedicated to the legal and economic aspects of information technologies. In Belgium, CRID is one of the key actors in software law and open-source culture.

Author biographies

The Editors

■ **Loretta ANANIA**: After receiving her Ph.D. from the Massachussetts Institute of Technology in 1990 with a thesis on Network Planning in the Information Society, Loretta Anania joined the European Commission. She was active in the RACE programme, in the Future & Emergent Technologies unit, and is currently responsible for search engine R&D in the Networked Media unit. She was twice elected as Chair of the International Telecommunications Society Board.

■ **Johannes M. BAUER** is a Professor in the Department of Telecommunication, Information Studies and Media at Michigan State University where he is also the Director of Special Programs of the Quello Center for Telecommunication Management and Law at Michigan State University. Dr. Bauer joined Michigan State University in 1990 after receiving his doctorate in economics from the Vienna University of Economics and Business Administration, Vienna, Austria. He taught and researched as a visiting professor at the Delft University of Technology, the Netherlands (academic year 2000-2001), the University of International Business and Economics in Beijing, China (May 2002), and the University of Konstanz, Germany (summer 2010).
bauerj@msu.edu

■ **Michel J.G. VAN EETEN** is Professor of Public Administration at the Faculty of Technology, Policy and Management, Delft University of Technology, the Netherlands. He also teaches in several programs for executive education at the Netherlands School of Public Administration in The Hague.
His recent research has been focused on the governance of infrastructures, most notably on the issue of internet security. He has also published on the reliability of electricity, telecommunication and transportation networks. In addition to his work on infrastructures, he has an enduring interest in the role of symbolic language in politics and policy. Recent work as a policy analyst includes advice on the economics of cybersecurity for the Dutch Ministry of Economic Affairs, the United Nations International Telecommunications Union and the OECD.

The interviewees

■ **Keith BESGROVE** works at OECD. He is the First Assistant Secretary, Consumer Policy and Post division of the Australian Department of Broadband, Communications and the Digital Economy. Keith is responsible for programs which provide access to broadband communications in rural and remote regions, consumer

policy, and cyber security issues relating to small business and home users. He is also the current chair of the OECD's Working Party on Information Security and Privacy, a position which he has held for the past three years. Keith has an extensive background in communications and cybersecurity policy issues and played a leading role in the establishment of the OECD Anti-Spam Taskforce.

■ **Evert Jan HUMMELEN** is deputy head of the department Consumers, Numbers and Chair's Office at OPTA (Independent Post and Telecommunications Authority). He has been working for OPTA since 2003. He is currently responsible for the Internet Security Team at OPTA after being a member of that team since 2009. Before that he has been enforcing market parties' compliance with obligations OPTA poses in case they hold a significant market power.

The authors

■ **Fabio BISOGNI** is Member of the Board at FORMIT Foundation and Head of Research and Innovation area. Responsible for the management of international projects on different topics: Critical Infrastructures and Crisis Management, Policy support, Innovation and International academic cooperation. He is a certified Tax accountant and auditor and an Economist with an Executive Master in ICT Engineering. In the past he worked for the Fraunhofer Institute IPK in Berlin, for Ernst & Young management consultants in Rome, and for CNH in Italy and UK in the field of Business development and Management Systems.

■ **Marjory S. BLUMENTHAL** joined Georgetown University in August 2003 as Associate Provost, Academic. Her responsibilities are broad, notably including leadership in strengthening the sciences and science and technology policy at Georgetown. She teaches, advises students, and consults on Internet and cybersecurity policy, areas where she continues to pursue personal research. Between July 1987 and August 2003, Marjory built and served as Executive Director of the National Academies' Computer Science and Telecommunications Board (CSTB; http://cstb.org). She designed, directed, and oversaw collaborative study projects and symposia on technical and policy issues in computing and telecommunications. Marjory is the principal author and/or substantive editor of numerous books and articles. She is a member of the Advisory Board of the Pew Internet & American Life Project and the Center for Strategic and International Studies Commission on Cybersecurity; she chairs the External Advisory Board of the Center for Embedded Networked Sensing at UCLA; and she is a RAND adjunct and an Office of Naval Research grantee. She did her undergraduate work at Brown University and her graduate work at Harvard University.

■ **Simona CAVALLINI** is researcher in economics and Project Coordinator in the Research and Innovation Area at FORMIT Foundation. She obtained a degree in economics on financial markets and institutions in 2002, a Master degree in

Economics in 2003 and she attended the first two years course of a Ph.D. in Economics working on topics related to innovation. During the past years, she has coordinated research activities in different EU projects on socio-economic impacts related to disruption of critical infrastructures. She is interested in economics of security including optimal investment analysis, market failures in a security context and policy definition.

■ **Richard CLAYTON** worked in the UK ISP industry until 2000 when he returned to the University of Cambridge to study for a Ph.D. He has remained as an academic, doing security economics research in the Computer Laboratory. He is currently engaged in a three year collaboration with the National Physical Laboratory (NPL) to develop robust measures of Internet security mechanisms.

■ **Sara DI TROCCHIO** is Ph.D. Candidate of the Law and Economics doctoral Programme of the University of Siena. After her undergraduate studies in Economics at University La Sapienza in Rome, she collaborated on national and international research projects mainly focused on the analysis of economic incentives aimed at encouraging information sharing in competitive environments. Among the others, she contributed as FORMIT Foundation consultant to the research activities on economics of security and resilience in critical communications and information infrastructures. Her research interests are mainly focused on law and economics, antitrust and industrial organization, economics of Information security and energy market.

■ **Richard HAWKINS** is a political economist specializing in innovation and research policy issues. Currently he is Professor and Tier 1 Canada Research Chair in the Social Context of Technology in the Faculty of Communication & Culture at the University of Calgary, and Senior Fellow at The Centre for Innovation Studies (THECIS). He holds BA and MA degrees from Simon Fraser University (Canada), and a DPhil from the University of Sussex (UK).

■ **Nilusha KAPUGAMA** is Research Manager at LIRNEasia. Nilusha is currently working on the LIRNEasia project Knowledge Based Economies (KBE), conducting research on two identified agriculture value chains in Sri Lanka on the potential to increase its efficiency, inclusiveness and the use of ICTs. She is also involved in assisting with the evaluation of LIRNEasia projects through the use of outcome mapping and Utilisation Focused Evaluation (UFE). She has worked on the LIRNEasia project, Broadband Quality of Service Experience (QoSE) while managing LIRNEasia's capacity building programme, CPRsouth. Prior to joining LIRNEasia, She worked as project intern at the Institute of Policy Studies, Sri Lanka, on projects relating to the telecom industry. She has also worked as an intern at the Standard Chartered Bank, Sri Lanka. Nilusha obtained her Masters in Development Economics and Policy from the University of Manchester in September 2007.
nilusha@lirneasia.net

■ **Brenden KUERBIS** is a doctoral candidate at Syracuse University's School of Information Studies, where he researches Internet governance, particularly with regard to the standardization and policy concerning Internet infrastructure security. He is a regular contributor to the Internet Governance Project Blog, a widely read source for coverage and analysis of the management of critical Internet resources and political economy of global Internet policy.

■ **Sophie LUBRANO** is Senior Consultant at IDATE. She is specialised in demand analysis, particularly in the area of consumer applications. Sophie also contributes her expertise in supply analysis, notably companies' Internet service strategies. Her assignments focus on various aspects of the telecom industry: Internet, media, landline and mobile telephony. Prior to joining IDATE, Sophie was an economic consultant for B.I.P.E., where she was in charge of telecom market monitoring. She is an economist, with a post-graduate degree from ESLSCA (Ecole Supérieure Libre des Sciences Commerciales Appliquées).
s.pernet@idate.org

■ **Nicole van der MEULEN** completed her studies in Political Science in 2006 before embarking on a Ph.D. in law at Tilburg University. She recently finished her dissertation to obtain her doctoral degree, and is currently working as a consultant for the Centre of Expertise in The Hague, an independent foundation concerned with issues relating to ICT and management in the public sector. Her research interests remain in the area of cybercrime and cybersecurity, which is illustrated through her current assignment as member of the knowledge centre of GOVCERT.NL, the Dutch Government Computer Emergency Response Team.
n.van.der.meulen@hec.nl

■ **Tyler MOORE** is a postdoctoral fellow at Harvard University's Center for Research on Computation and Society. His research interests include the economics of information security, the study of electronic crime, and the development of policy for strengthening security. Moore completed his Ph.D. in Computer Science at the University of Cambridge, supervised by Professor Ross Anderson. His Ph.D. thesis investigated cooperative attack and defense in the design of decentralized wireless networks and through empirical analysis of phishing attacks on the Internet. Moore has also written reports for ENISA and the US National Academy of Sciences detailing policy recommendations for improving cyber security. He is a 2004 Marshall Scholar.

■ **Milton L. MUELLER** teaches and does research on the political economy of communication and information at Syracuse University's School of Information Studies. He has a longstanding interest in the history of communication technologies and global governance institutions. His new book *Networks and States: The global politics of Internet governance* (MIT Press, 2010) provides a comprehensive overview of the political and economic drivers of a new global politics. Mueller received the Ph.D. from the University of Pennsylvania in 1989.

■ **Isabelle POTTIER** is attorney-at-law and head of the research and publications department of the law firm Alain Bensoussan; she has particular expertise in drafting studies on the assessment and legal protection of new technologies as well as on electronic evidence and archival.

■ **Chanuka WATTEGAMA** is an Independent Policy Reseacher and Consultant. His expertise is in telecom policy and regulations, ICT for Development, Development Economics, Disaster Risk Reduction and Development Evaluation. Chanuka previously worked as the Senior Research Manager at LIRNEasia (http://www.lirneasia.net), an Asian think tank on policy and regulation. An Electronics Engineer by profession, he has completed his Master of Business Administration (MBA) degree from University of Colombo. At LIRNEasia, Chanuka led two projects. The first one was an attempt to test a new user centric broadband Quality of Services Experience (QoSE) in South Asia. Mobile 2.0 explored the emergence of more than voice mobile applications in Asia and conditions that facilitate. His work also involved studying cell broadcasting for disaster management and Telecom Regulatory Environment analysis of Indonesia. Chanuka has also worked as Program Specialist ICT4D at United Nations Development Program (UNDP) Asia-Pacific Development Information Program (APDIP) out-posted to Colombo Regional Center's Millennium Development Goals (MDG) Initiative. His focus was to use Information and Communication Technology (ICTs) for poverty reduction and achievement of the MDGs.
chanuka@lirneasia.net

Events

2nd PhD Seminar of the International Telecommunications Society
Budapest, Hungary - September 21-22, 2011

TPRC - 39th Research Conference
Arlington, Virginia - September 23-25, 2011

Conference in Honor of Professor Emeritus Lester D. Taylor
Jackson Hole, Wyoming - October 10, 2011

Digiworld Summit 2011
Will the device be king?
Montpellier, France - November 16-17, 2011

Creation of CEPS Digital Forum

Announcement and Call for papers

2nd PhD Seminar of the International Telecommunications Society

21-22nd September 2011

Budapest, Hungary

Meet the experts!

The International Telecommunications Society (ITS) is an association of academics and other professionals in the information, communications, and technology sectors Its network of researchers comprises outstanding scholars in the field of telecommunications research that are well known from the literature (see www.itsworld.org).

In order to share the valuable expertise represented by highly specialised academics and renowned industry experts with younger researchers, the ITS organises a PhD seminar.

About 15 students will be selected from the responses to this call. In accordance with the topics presented by the winning candidates, experts from the ITS network will be chosen to discuss new ideas brought forward by PhD students. The focus will be on the discussion of ideas presented by the participants, and less on the mere presentation of papers. A selection of papers presented at the seminar will be published in Telecommunications Policy.

The seminar will be linked with the European Regional Conference of the ITS to be held at the same location before the Ph.D seminar. Access to this conference will be free of charge for the participants of the PhD seminar.

The seminar will be organised by ITS and Chalmers University of Technology. It will be held in Budapest and hosted by the Scientific Association for Infocommunications Hungary (hte).

Call for papers

Papers can be submitted for presentation and discussion related to the following topics:

Regulation of telecommunication markets

- Regulatory regimes and institutions
- Regulatory response to market dynamics (changing technologies, new services, new platforms, new players, new value chains)
- Updating theoretical insights for better regulation
- Current regulatory problems at the European, international and national levels
- Regulating mobile services: justification, necessity, solutions

Challenges of convergence of telecommunication systems and content supply

- Definition and delimitation of markets
- Supply chain configurations
- Regulatory problems of converging markets
- Internet Governance

Development of telecommunication markets

- Internationalisation of markets: the expansion of markets through mergers and FDI
- Technology driven markets vs. regulation driven markets
- User driven market developments
- Emerging markets

Telecommunications and Society

- Internet governance
- Privacy issues
- Digital divide
- Access to content

This list is not exclusive. Other topics in the field of telecommunications are also welcome. Please send your paper together with a CV to:
Erik BOHLIN: erik.bohlin@chalmers.se
and to Brigitte PREISSL: b.preissl@zbw.eu

Important dates

Deadline for the submission of papers: 15 May 2011
Response by: 15 June 2011
Final paper to be submitted by: 1 August 2011

CALL FOR PAPERS

TPRC Presents

The 39th Research Conference on Communication, Information, and Internet Policy

Hosted by George Mason University Law School, Arlington, Virginia

Friday, September 23 through Sunday, September 25, 2011

www.tprc.org

TPRC is an annual conference on communication, information and internet policy that convenes international and interdisciplinary researchers and policymakers from academia, industry, government, and nonprofit organizations. Its purpose is to present original research relevant to policy making, share the knowledge requirements of practitioners, and engage in discussion on current policy issues. The conference program consists of presentations selected from submitted paper abstracts, student papers and panel submissions.

TPRC is now soliciting abstracts of papers, panel proposals, and student papers for presentation at the 2011 conference, to be held September 23-25, 2011 at the George Mason University Law School, in Arlington, Virginia. These presentations should report current theoretical or empirical research relevant to communication and information policy, and may be from any disciplinary perspective – the sole criterion is research quality. Themes of particular interest include, but are not limited to:

- Network Competition
- Broadband Deployment and Adoption
- Wireless Communications
- Innovation and Entrepreneurship
- Media, New and Old
- Intellectual Property
- Privacy, Security, Identity and Trust
- Internet Ecosystem Governance
- Affordability and Access
- International and Comparative Studies
- Societal Challenges, Endangered Rights and Social Justice
- Emerging Topics

Full category descriptions can be found via our web site: http://www.tprc.org

Submissions are due by March 31, 2011. Abstracts and panel proposals must be submitted electronically at http://www.tprc.org by following the submit button at the end of each topic description. Standards for abstracts are provided below. The review process is single blind, and a short biographical sketch for each author is required.

Acceptances/rejections will be provided by May 15, 2011. Complete papers for accepted abstracts will be due to TPRC on August15, 2011. Papers not submitted in final form by the due date will be removed from the program. At least one author of the paper is expected to attend the conference to present the accepted submission.

Students are encouraged to submit papers for the student paper competition. Visit our web site, www.tprc.org for the Student Papers CFP. Full student papers must be submitted by April 30, 2011.

We also welcome proposals for panel discussions of broad interest. These should include a description of the panel topic, a proposed panel moderator and a list of possible panelists. Panel proposals should be submitted by March 31, 2011 at http://www.tprc.org.

The journals *Telecommunications Policy* and *Journal on Information Policy* will both invite papers for special issues from this year's conference. Guest editors drawn from the TPRC Program Committee will invite selected authors to submit their papers for review.

Please address inquiries to:
info@tprc.org

Call for Papers

Conference in Honor of Professor Emeritus Lester D. Taylor

Monday, 10 October 2011

Jackson Hole, Wyoming

Rigorous demand study for information and communications technology (ICT) began with Lester D. Taylor's *Telecommunications Demand: Survey and Critique* (1980) which set a yardstick for subsequent research. Taylor followed up with *Telecommunications Demand: In Theory and Practice* (1994) which expanded and refined the approach, at a critical time when competition was being accelerated through the divestiture of AT&T. He authored numerous other papers in this area. His earlier book, *Consumer Demand in the United States: Prices, Income, and Consumption Behavior* (1966/1970) (coauthored with Hendrik S. Houthakker) became required reading for anyone serious about consumer demand studies. More recently it has been updated (2010) to account for much of the theory and applications since the first publication.

Demand and telecommunications analyses are not Professor Taylor's only contributions; he has published: *Mathematics and Probabilities Statistics* (1975); *Capital Accumulation and Money* (2000); and even *Hospital Costs in Massachusetts: An Econometric Study* (1968). Professor Taylor's writing in these areas has been innovative and insightful.

This call for papers is set around the themes of Professor Taylor's work. Papers will be peer reviewed. Those selected will be published in a Festschrift in honor of Professor Taylor edited by James Alleman and Paul Rappoport.

Topics include (but not limited to):

Information and Communications Technologies

- Residential telecommunication demand
- Wireless demand
- IP-based voice
- Broadband services
- Consumer choice

- Broadband deployment and infrastructure
- Business demand for data and communication services
- Case studies - Consumer demand; by region, country
- Wireless services; cellular, satellite, WiFi, WiMax, etc.
- Fixed line services: traditional telephony, cable, DSL, fiber-optic, etc.

Consumer Demand

Capital Investment

The events venue is:

Spring Creek Ranch (http://www.springcreekranch.com/)
1800 Spirit Dance Road • Jackson WY 83001
307-732-8133 • 800-443-6139

Abstract submissions are due: 16 May 2011

Abstract acceptance notification: 21 June 2011

Paper submissions are due: 30 August 2011

Please send abstracts to James Alleman at James.Alleman@Colorado.edu with subject title: Taylor event abstract.

We plan to publish the accepted papers in the Springer Economic Series: Economics of Science, Technology and Innovation and anticipate that the Festschrift will be completed in less than a year after the conference.

Limited travel funds, scholarships and honoria will be available.

Sponsors: Centris
Columbia Institute of Tele-Information (CITI)
International Telecommunications Society

Organizers: James Alleman
Jason Buckweitz
Bruce Egan
Eli Noam
Paul Rappoport

For additional information and updates see CITI website:
http://www4.gsb.columbia.edu/citi/events/Taylor2011

Will the device be king?

16-17 november 2011, Montpellier (France)

Smartphones, tablets, connected televisions… for consumers, adopting innovative services and applications usually starts with a new device, especially now that more and more objects are being designed to network. And even though applications are bound to eventually operate in the cloud, it does not mean that the devices are just dumb machines with nowhere to go, as some might think.

The economic weight of hardware markets, the battle for supremacy between smartphone OS, and the emergence of app stores operated by the leading device manufacturers have all revealed the various platform strategies that only a few heavyweights are able to engage in. These more or less open strategies embody the features of two-sided markets, targeting not only consumers but also developers and content providers. They also have to go head to head with other ecosystems created by the Internet giants (search engines, social networks, e-commerce and e-payment) and the leading telcos.

Addressing the device issue ultimately means addressing questions of how users habits and expectations will evolve, the strategic assets of the central players of tomorrow's Internet, and what changes we are likely to see in electronic communications markets' structure.

- Devices tailored to new consumption habits

- What device combinations will be the most common a few years from now? What will be the key determining factors?
- Will users' choice be influenced mainly by the appeal of a certain ecosystem (ensuring interoperability and a good selection of content)? Or will that not matter, as most content can be accessed by all devices?
- Will the dividing lines between personal/home devices and work devices be erased further still?
- How will users who own several devices divide their time between fixed, mobile and roaming access?

- Adapting the value chain to tomorrow's Internet

- What are the commonalities and differences in the device strategies employed by Apple, Amazon, Orange, Samsung, Microsoft, Cisco… and Google? Can we expect to see a Facebook device?
- Will there still be companies that supply devices with no services and applications attached? Will manufacturing be handed over more and more to specialized firms?
- What is the future outlook for IPTV set-top boxes when competing with connected TV solutions?
- From a more general perspective, what role for devices associated with managed services (vs. those available on the open Internet?)
- What might change to make smartphones the biggest selling devices? How many OS will there be in the smartphone and tablet market?
- What will become of carriers' subsidy schemes with smartphones and tablets? Are we likely to see mobile carriers cut out of the loop by soft SIM strategies? What revenue might NFC apps generate?
- What ties are there between the various protagonists and the various visions of cloud computing (Net-centric vs. device-centric vs. cloud-centric)?

- Changes in the competition landscape and regulation that adapts

- How to address the issues of standardisation and exclusivity between platforms, and between platforms and developers and content providers?
- To what extent does the Net neutrality debate need to extend to the dangers of certain device manufacturers abusing their newfound dominant positions?

The DigiWorld Summit, in brief

- The benchmark conference **on the core issues of convergence**: telecoms, Internet, media
- Over **1,300 participants**, including more than **150 speakers**, from over **30 countries**
- A series of special **Executive seminars** hosted by IDATE experts and our partners: Next Gen Networks: the latest issues; Digital Content: new economics; Smart Living; Developments in Net neutrality; Video Games markets; E-health; Smart Grid…
- **Satellite events**: FIA business meeting, MIG (international conference on Motion in Games)
- **Product demo area** for innovative applications, the DigiWorld Economic Journal prize
- A host of invaluable **networking opportunities**: Breaking the ice party on the 15th, Gala dinner on the 16th …

CEPS DIGITAL FORUM

UNLOCKING EUROPE'S POTENTIAL TO ENTER THE INFORMATION SOCIETY

The European Commission recently launched its Digital Agenda, which sets very ambitious targets for the years to come and confirms the Digital Internal Market as the single most important reform of the past few years. As observed also by the recent report by Mario Monti on the future of the Single Market, "the EU could gain 4% of GDP by stimulating the fast development of the digital single market by 2020. This corresponds to a gain of almost € 500 billion and means that the digital single market alone could have an impact similar to the 1992 internal market programme".

Against this background, and in light of the crucial importance of the digital revolution in the EU27, CEPS has decided to take action. After 5 years and three successful editions of Task Forces on electronic communications, we have decided to create a more permanent platform for debating the policy challenges posed by the information society era. Such a forum for discussion is missing in Brussels, at a time in which the European Commission is engaged in shaping the digital agenda for the years to come, under the guidance of Commissioner Neelie Kroes.

The new forum – termed CEPS Digital Forum – will group academics, telecommunications operators, broadcasters, equipment manufacturers, application producers, Internet champions, national regulators and European institutions, to enable a constructive dialogue on how to achieve a successful transition towards the information society for all.

Planned activities of the CEPS Digital Forum include the following:

- Four plenary meetings per year: a full-day event dedicated to one key issue, plus a discussion of current developments and update of corporate members of development in markets, research and legislation around the world;

- The creation of working parties on ad hoc issues, such as the economics of cloud computing, spectrum policy, net neutrality, emerging business models, content and copyright issues, etc.
- The creation of a Digital Forum website and intranet, where participants will have access to resources, news and comments (www.digitalforum.eu);
- A Digital Forum blog that will host contributions from the participants and external experts, and will call for contributions also from other regions (e.g., the US and Asia);
- A Digital Forum newsletter that will keep participants updated on recent developments in information society policies worldwide;
- The possibility of organising ad hoc events called by Digital Forum participants in Brussels or in other locations.

In order to achieve these goals, the CEPS Digital Forum will count on partnerships and collaboration with a number of existing platforms and academic groups around the world. A Scientific Board will be appointed in order to ensure the quality of scientific output and constant contact with academia, industry and institutions. The Digital Forum will be chaired by Staffan Jerneck, Director and Director of Corporate relations of CEPS, and will be managed by CEPS Senior Research Fellow Andrea Renda.

How to become a member

Being member of CEPS is a pre-requisite for participation to the CEPS Digital Forum.

Corporate membership of CEPS is open to corporations and national federations. Institutional membership is available for Brussels-based European trade associations and research institutes. Representatives of the European Commission and Council, Members of the European Parliament, academics, practitioners and national regulators will be invited to participate.

No other participation fee is foreseen except for cases in which ad hoc task forces or conference are organised.

For more information, please contact:
Staffan JERNECK
Director & Director of Corporate Relations, CEPS
+32 2 229 39 10 (direct line); +32 475 903 924 (mobile)
Email: Staffan.Jerneck@ceps.eu

COMMUNICATIONS & STRATEGIES

DigiWorld Economic Journal

Guide for authors

COMMUNICATIONS & STRATEGIES is an international journal that aims to publish peer-reviewed papers focusing on the industry's key issues and offering a forum for the finest socio-economic analysis of the telecoms, IT and audiovisual sectors.

It proposes thematic **Dossiers** including several papers and interviews with academic or institutional personalities. In addition to the Dossier, we usually publish a **selection of papers** that typically cover innovative issues in the sector. The **Features** rubric contains short papers offering factual analyses of recent developments in the fields of regulation and competition, firms and markets, technical innovations, public policies and use logics, as well as book reviews.

Submission of papers

All papers submitted for publication will be reviewed using the "double blind" system by at least two referees, selected based on the subject matter of the paper, from the journal's panel of referees. Shorter articles appearing in the "Features" section are refereed at the discretion of the Editor.

Proposals must be submitted in Word format (.doc) and should not exceed 6,500 words, including the footnotes and references. Please ensure that all illustrations (graphics, figures, etc.) are in black and white - excluding any color - and are of printing quality. Bibliographical references should be included at the end of the article. Should these references appear in the text, please indicate the author's name and the year of publication in brackets.

Coordination and information
Sophie NIGON
s.nigon@idate.org
+33 (0)4 67 14 44 16
www.comstrat.org