The Role of Internet Service Providers in Cyber Security

Project Leads

Brent Rowe, MA, RTI International
Dallas Wood, MA, RTI International
Douglas Reeves, PhD, North Carolina State University
Fern Braun, BA, RTI International

Statement of Problem

Internet insecurity is a worldwide problem that has generated a multitude of costs for businesses, governments, and individuals. Past research (e.g., Frith, 2005; Gallaher, Rowe, Rogozhin, & Link, 2006) suggests that one significant factor in these cyber security problems is the inadequate level of security maintained by home users and small businesses. Attackers compromise the computers of such users, developing networks of “zombies” or “bots” (called “botnets”) through which they send large amounts of spam and conduct other malicious activity (Markoff, 2007). Unfortunately, home users and small businesses are often unaffected by such activities and thus lack the incentives to invest in a security plan that approaches the socially optimal level of security, thus making all users less secure (Schneier, 2007b). Economists refer to such an issue as a “free rider” or “public goods” problem (Anderson & Moore, 2006).

A handful of research studies and security experts have suggested that Internet Service Providers (ISPs) may be in a good position to cost-effectively prevent certain types of malicious cyber behavior, such as the operation of botnets on home users’ and small businesses’ computers (e.g., Evers, 2005; Huang, Xianjun, and Whinston, 2007; Richards,
2007; and Schneier, 2007a). Similar to a neighborhood entrance security checkpoint that provides a measure of security to all houses branching off the private roads therein, individual Internet users would be much better protected if their ISP played a larger security role. One study found that just 10 ISPs accounted for 30 percent of IP addresses sending out spam worldwide, meaning that an ISP’s actions to protect their network may already be an important factor in cyber security (Van Eeten 2010). The economic literature suggests that ISPs could take advantage of both information asymmetry and economies of scale to provide more security at a lower cost, particularly for individual Internet users and small businesses.

The purpose of this brief is to review the existing literature and popular press on actions that ISPs are taking or could take to better secure their customers, economic barriers to such solutions, and incentives needed to increase ISP involvement.

Cyber security has become a monumental problem. Franklin and colleagues (2007) and McDaniel (2006) suggest that sophisticated hackers are stealing hundreds of millions of dollars each year, in addition to the inefficiency costs incurred by businesses and individuals. Further, these authors suggest that one well-designed attack could easily destroy a business’ operations or cripple an industry or the electricity grid for several days or weeks.¹

In many cases today, the “vehicles” that hackers use to conduct illicit activities are “compromised” computers (sometimes called bots or botnets), usually owned by home Internet users and small businesses who are unaware that their computers have been “recruited.” In 2007, Dave DeWalt, CEO of McAfee, stated that he believes bots are the biggest cyber security threat today: “the engines that drive everything” (Swartz, 2007). And the 2007 National Academies report Toward a Safer and More Secure Cyberspace points to bots as a significant and growing threat to consumers and national security (Goodman & Lin, 2007).

According to some estimates, bots could account for as many as 11% of the 650 million computers attached to the Internet, or 71.5 million computers (Markoff, 2007). Bots are used to send large amounts of spam, host “phishing” websites, and wage distributed denial of service (DDoS) attacks. Recent estimates suggest that between 80% and 95% of spam comes from botnets, and between 80% and 90% of e-mail is spam (Hodapp, 2007; Zhuge, Holz, Han, Guo, & Zou, 2007). This spam wastes time, costs money (e.g., through fraud), crashes servers, and serves as a mechanism both to distribute viruses, worms, and adware and to “recruit” new bots. To solve this problem, many security experts and researchers have suggested that ISPs are ideally suited to mitigate a variety of cyber security issues, including bot activities (Evers, 2005; Huang, Xianjun, & Whinston, 2007; Richards, 2007; Schneier, 2007a).

¹ Of note, in early April 2009, it was announced that spies had penetrated the U.S. electricity grid (Gorman, 2009).
ISP-Based Security Solutions: Alternatives and Trends

ISPs observe traffic flowing into and out of their networks. They are in a position to observe traffic spikes that could be associated with excessive malicious traffic (e.g., caused by worms or spam bots) and “filter” suspicious traffic. For example, ISPs could stop suspicious traffic from entering their network, and if traffic originating from their network looked malicious, they could suspend the network access of customers suspected of being bots or knowingly sending malicious traffic. Alternately, ISPs can force their users to adopt more security on their host computers.

Today, many ISPs are offering some security services, but many are not (Schneier, 2007a). In general, ISP-based security solutions can be grouped into three main categories of implementation scenarios aimed at improving their customers’ security:

1. **Fully External**: Provide users with security advice (e.g., how to setup a firewall) or free products (e.g., antivirus software).

2. **Fully Internal**: Implement increased filtering at the ISP level so that suspicious activity is addressed (e.g., a user or group of users is investigated and possibly lose sending privileges temporarily).\(^2\)

3. **Partially Internal/Partially External**: Impose policies on users that cause them to play a role in preventing unwanted traffic (e.g., an ISP forces customers to approve e-mail received from unknown senders before e-mail is accepted).

Several ISPs today offer their customers “fully external” products and services. Many ISPs provide antivirus, firewall, or antimalware software to customers either free (i.e., included in the purchase of their Internet plan) or for an additional fee, which is often a lower price than that faced by individuals purchasing directly from companies such as McAfee or Norton. This promotes the use of security programs among customers who might not otherwise purchase the software. However, users are still usually left to install and operate such mechanisms on their own.

In other cases, ISPs in the United States and abroad are offering “fully internal” services to business users. In October 2006, BT began to offer a service that involved robust e-mail scanning (Mellor, 2006). ISPs such as Comcast have also tried imposing penalties on their customers who allow zombies to operate on their network; however, users have responded very negatively to perceived filtering of their Internet communications (e.g., Roberts, 2004; Cassavoy, 2007; Mitchell, 2007). Additionally, business users have been wary of outsourcing their network security (Gallaher et al., 2006; Rowe, 2007). In economic terms, they seem to be responding to the principal agent problem (Jensen & Meckling, 1976)— firms are concerned with

\(^2\) It is very unlikely that ISPs will be able to provide fully secure Internet communications. In their argument for more ISP security liability, Lichtman and Posner (2004) acknowledge a negative effect of more ISP-based security: users might decide to spend less on host-level security. The authors suggest that robust ISP-level and host-level security would be ideal.
that the incentives motivating an ISP or managed security service provider (MSSP)\(^3\) to provide the best security at the lowest cost are not fully aligned with their security desires.

Further, the U.S. government has solicited secure Internet connections from ISPs through the Trusted Internet Connections Initiative (Nagest, 2009); this would provide fully internal security services to U.S. government agencies. AT&T was the first provider of such services.

Several ISPs also offer “partially internal and partially external” services to home users and small business users. Earthlink forces customers to “approve” all new incoming message senders before messages can be accessed. This is not error-proof, however; a spammer could send e-mail from a known address, and it would get through.

In the U.S., the Federal Communications Commission (FCC) and the legal system have recently begun to play a large role in the debate over what ISPs can and should be able to do in terms of treating customers differently and managing their network, including security-related activities. In 2008, Comcast began slowing user access to a file-sharing site. The FCC attempted to enforce net neutrality—generally defined to mean not discriminating against Internet traffic based on the content—by ordering that Comcast cease such activities. Comcast appealed the sanction, and in 2010 the U.S. Court of Appeals ruled unanimously in favor of Comcast, stating that the FCC does not have the power to halt this practice (NY Times, 2010).

The Comcast case demonstrated that the legal restrictions on ISPs are not currently well defined. It is unclear how the FCC will be able to regulate the Internet in the future. Broadband may become a highly regulated utility like the telephone service industry or, if the current state of policy stands, the FCC may be unable to enforce its net neutrality policy.

In terms of ISPs’ role in providing security to home Internet users, the FCC has so far only provided guidance to ISPs. A working group in FCC’s Communications Security, Reliability and Interoperability Council released a network protection best practices document for ISPs in December 2010 (CSRIC 2010). The paper includes 24 best practices, divided into the categories of prevention, detection, notification, mitigation, and privacy considerations, and emphasizes the importance of timely detection and notification, security software provision, and improved end-user education. The group recommends that ISPs quarantine infected customers only after multiple contact attempts, except in extreme cases.

In other countries, including Australia, the Netherlands, Germany, and Japan, governments are taking steps toward developing public-private partnerships to improve cyber security through ISPs. In 2010, Australia created a voluntary code of practice for ISPs, asking that they maintain a system for notifying infected computers, keep up-to-date threat information, provide resources for end users, and use a reporting mechanism to inform the government about severe threats (Internet Industry Association 2010). Japan has already

---

\(^3\) MSSPs are service companies that provide outsourced security services to businesses.
seen positive impacts from their “Cyber Clean Center,” a collection of over 70 ISPs dedicated to improving cyber security (OECD 2010).

Overall, the market trend appears to be moving toward ISPs providing more security to their customers; a variety of barriers exist, however, and more information is needed (e.g., on customers’ willingness to pay for security) to motivate faster and more widespread ISP security provisioning.

**Economic Barriers to ISP-Provided Security**

Currently, the information necessary (e.g., costs, pricing models) to develop a convincing business model for ISPs to provide security to their customers does not exist in the public domain. Huang, Xianjun, and Whinston (2007) analyzed the issue and concluded that ISPs will continue to have trouble finding a return on their investment because of the significant costs involved in providing additional security filtering.

ISPs’ concerns are varied, but they focus on the many costs of providing security services. Two such costs are described by an editorial response to the Australian government’s ISP security mandate (Winterford & Hill, 2008):

- **Technical costs:** The primary technical costs are two fold—identifying bots and stopping them; both are very complex tasks. Any solutions will require a variety of fixed and variable costs, including capital and labor required to identify potential botnets and to remediate the infection. Further, hackers continue to adapt their techniques to evade detection, making future service costs more uncertain.

- **Customer service costs:** One of the biggest costs to ISPs are the costs associated with successful notification of customers. Email might be perceived as spam, letters sent by mail may look like marketing material, and phone calls are costly. Further, identifying the person / computer that has been infected may be difficult if more than one computer exists at a given address. The costs for this activity can be significant.

- **Legal issues:** Customer contracts often specifically prevent an ISP from filtering traffic, and international connections multiply the potential legal complexities. ISPs also worry that providing more security would implicitly increase their liability (i.e., if an ISP states that they provide security and a customer is negatively affected by a security breach, the ISP could be held fully or partially liable).

In a recent study by the authors of this research brief, the average cost of security for consumers purchasing security services from the top 23 ISPs, either as part of the price of the Internet plan or as a separate fee, was approximately $5 per month (Rowe et al, 2011). However, the cost for ISPs to providing these services is unknown.

A study by Clayton (2010) analyzed the cost of a government-subsidized PC infection remediation scheme; the author estimated the cost of cleaning up an infected PC at $70. The
author’s scenario assumed that an ISP would report a security problem to a customer, who would then choose to either pay some fee for the clean-up service, with the remainder of the cost covered by the government, or solve the problem themselves.

Despite the insufficient information, ISP security provisioning could benefit from network effects. Economic theory suggests that ISP costs per unit of security provided should decrease as the number of ISPs implementing security measures increases because “learning curve lessons” are internalized by the market and a higher level of security results more quickly.

**User Demand for Security**

Proper incentive mechanisms are essential to gaining the participation of ISPs in providing security services. ISP-based security could offer a new source of revenue (as well as build customer loyalty and reduce customer turnover); however, the commercial success of ISP security offerings will depend largely on customers’ demand (i.e., willingness to pay) for additional security.

Individuals’ and small businesses’ investments in cyber security are often neither socially nor privately optimal. Anecdotally, users’ interest in security products and services seems inconsistent, and their decision processes often differ greatly. However, the overall lack of optimal investments can be explained in terms of two common economic concepts:

1. **Incomplete information**: Users inaccurately calculate the total private cost of security products and associated labor, as well as the impact of breaches (Gallaher et al., 2006).

2. **Negative externalities**: Users are apathetic regarding external costs that are imposed on other organizations and individual Internet users as a result of inadequate security at the investing organization.

Several studies have tried to estimated demand for cyber security services. A 2004 study of consumers in the United Kingdom found that 58% would be willing to pay $3 or more per month for more protection. In the same study, 66% of consumers said they would switch ISPs to one that offered “clean” Internet service (StreamShield Networks, 2004). Gallaher and colleagues (2006) also interviewed a small sample of home Internet users and found that more than 50% spend more than $20 per year on security products or subscription services. More than half also indicated a willingness to pay their ISP 10% more for additional security.

Most recently, in 2011 study by Rowe et al, stated preference analysis was used to assess users’ willingness to pay for security services. The results showed that the average respondent was willing to pay up to $7.24 per month (in addition to the current Internet access bill) if no time was required and his or her Internet could not be limited in any way. In particular,
survey data suggested that such a plan would need to offer a greatly reduced risk of identity theft, less computer slow down or crashing, and greatly reduced risk to others (in order of the value placed by survey respondents) in order to increase willingness to pay.

**New Incentives for ISPs**

If sufficient user demand exists in excess of the costs involved, ISPs should be providing more security. Assuming most ISPs would investigate such options where additional revenue could be generated, it is likely that offering security services has never been an easily justified investment determination. As such, alternate strategies may be needed to motivate ISPs to become more involved in providing security, particularly to home users and small businesses, who have the least resources and information available with which to make security decisions and who, as a group, have the potential to aid attackers who abuse their insecurity.

After concluding that ISPs should provide more security, Huang, Xianjun, & Whinston (2007) suggest that new incentive frameworks will be required. In particular, the authors suggest a new price-sharing scheme in which various Internet stakeholders share the costs by setting service prices inclusive of the positive and negative externalities inherent in decisions being made. Chen, Longstaff, and Carley (2004) developed a model to empirically analyze the incentive framework that would allow ISPs to provide additional security in the form of new DDoS filtering services to business customers. This paper is based on a more robust analysis than the Huang, Xianjun, and Whinston paper (2007), but the model discussed therein relies on relatively weak assumptions (e.g., a small number of ISP solutions should be considered, users’ willingness to pay should be averaged, and network effects should not be considered in ISPs’ cost functions). In general, both of these papers, which represent the best known papers on this topic, fail to provide empirical data with which to estimate the costs and benefits to ISPs and various Internet users.

Absent identifiable market-based incentives for ISPs to be more diligent providers of security, government could take action. McCullagh (2005) and others have suggested that the government pass regulation to force ISPs to provide some level of security to customers, and Lichtman and Posner (2004) propose that courts encourage ISPs to offer more security by holding them accountable for failing to act. Alternately, a 2007 paper by Parameswaran and colleagues advocates for a certifying authority to “approve” ISPs that provide higher security, thereby encouraging ISPs to prevent outbound malicious traffic.

Government subsidies or other public support could also be considered if the private benefit-cost trade-off cannot motivate cost-effective private sector action and if neither government regulations nor liability are tenable solutions.

---

5 In 2006 a Belgian court ordered an ISP to block all peer-to-peer network traffic sent and received by its customers (Thomson, 2007).

6 Of note, several U.S. government initiatives have aimed to combat botnets. Through “Operation Bot Roast,” the Federal
Conclusion

Research described in this brief suggests that ISPs are providing some security services to their customers today; however, many experts believe they should provide more. Barriers preventing ISPs from becoming more involved include a variety of technical costs and legal issues, as well as uncertainty regarding who would pay these costs. To overcome such barriers, several papers have suggested that government regulations or liability would provide the appropriate motivation to ISPs. Others suggest that users would pay enough to cover these ISP costs.

Research by Rowe et al provides the first economic data to support the development of new product offerings and marketing tactics by ISPs as well as providing data to estimate the potential benefits that citizens if the government helped to subsidize ISP-based security. Looking forward, additional research is needed to assess the specific ways in which ISPs would bear costs to provide security. Identification, notification, and remediation costs need to be assessed separately to determine whether some of these costs (e.g., notification and/or remediation) could be shared through, for example, and public private partnership.

Although ISPs do not view security as a central role, they are in an optimal position to provide security to home internet users. As such, more research and policy work should be conducted to test how ISPs could be incentivized—e.g., through developing improved marketing messages to customers or by receiving government subsidies—to provide increased security for their networks, potentially reducing cyber attacks and increasing the reliability of the entire Internet infrastructure. By shifting some of the burden of security from end users to ISPs, who have more information and are more technically capable, everyone could benefit—ISPs, individual users, and businesses responsible for providing and operating (and profiting from) secure networks.

Contact Information

Brent Rowe
114 Sansome St., Suite 500, San Francisco, CA 94104
(415) 848-1317
browe@rti.org

Bureau of Investigation (FBI) contacted over a million PC owners whose computers were turned into bots (FBI, 2007). The Federal Trade Commission (FTC) also organized a campaign called “Operation Spam Zombies,” involving more than a dozen government agencies that aimed to identify and remove botnets by working with ISPs and consumers (FTC, 2005). No information was available on the success of either program.
This research brief was prepared by Mr. Brent Rowe, Mr. Dallas Wood, Dr. Douglas Reeves, and Ms. Fern Braun.

**Brent Rowe, MA**, is a Senior Economist at RTI International. He has significant experience in studying security related issues and recently co-authored a book entitled *Cyber Security: Economic Strategies and Public Policy Alternatives*.

**Dallas Wood, MA** is an Economist at RTI International. He has extensive research experience collected new data and conducting robust analyses for economic studies of new technologies as well as studies of environmental issues.

**Douglas Reeves, PhD**, is a Professor of Computer Science and Electrical and Computer Engineering at N.C. State University. His research focuses on network security and peer-to-peer computing, with current funding from the National Science Foundation (NSF).

**Fern Braun, BA**, is an Associate Economist at RTI International. Her research has included providing data collection and analysis support for studies on new technologies and environmental policies.

---

**References**


