Government Regulation for OS and Computer Manufacturers?

Daniel Holland
University of Colorado Interdisciplinary Telecommunications Program

Introduction

In his presentation at the February 2008 Silicon Flatirons conference, The Digital Broadband Migration: Information Policy for the Next Administration, Princeton University Professor Edward Felten discussed the threats facing cyberspace and the government's failure to develop a long-term strategy to address the security of the many users of our information technology infrastructure. In many ways, the lack of federal guidance in the computer and network space is similar to the absence of government regulation during the rise of the automobile in the US. In three parts, this paper compares the government's regulation of these two revolutionary technologies. Part 1 describes the threats facing cyberspace. Part 2 compares automobile safety regulation to the challenges faced in cyberspace. Finally, Part 3 offers some recommendations for the next administration.

Part 1: Cyberspace Under Attack

As the United States moves forward from the Information Age to the Connected Age (Zelenka, 2007), it is increasingly obvious that cyberspace has the dubious distinction of being our most important yet worst protected national resource. Although the 2003 National Strategy to Secure Cyberspace correctly describes US cyberspace as the "[…] nervous system [linking every sector of the US economy and government including] agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, […]," it does little to actually strengthen and protect this infrastructure (White House, p. 1). In fact, the Bush plan has been roundly criticized for being too vague and lacking teeth (Lemos & McCullagh, 2002). Making the situation even worse is the fact that the US is facing a new, more resilient breed of cyberspace attackers. Ken Baylor describes the evolution like this: "The cyber-criminal of today is much less likely to be the neighborhood geek recklessly unleashing malware. Instead, modern cyber criminals are often motivated by politics or greed" (2006). Unfortunately, vulnerable US infrastructure is under constant attack by organized crime, terrorist organizations, and foreign nations (SANS, 2006).

According to Professor Felten, the biggest threat to US cyberspace is, surprisingly, the average computer (2008). The average computer belongs to the average American and is most likely running popular commercial software installed on the machine at the time of purchase with dangerous and insecure default configurations (SANS, 2007). The root of the problem, according to Professor Felton, is the "software quality" of these consumer applications (2008). Because the consumer market supplies 70% of economic activity (Phillips, 2007), software manufacturers produce for this market segment first. Often, government and enterprises look to the consumer ecosystem and harvest its products (software) for their own use as "commercial off the shelf" solutions. Unfortunately, this causes a trickle down effect. If the original code included vulnerabilities, they now exist in systems across the cyberspace.

Another reason the average computer poses a threat to cyberspace is the explosion of internet protocol (IP) technology, broadband access subscription, and cloud computing. According to Professor Felten, this interdependence makes cyberspace fundamentally vulnerable: because of

internetworking, the average household computer is the weak-link in the cyberspace chain and provides attractive scaling and anonymity benefits for a determined attacker (2008). This is because vulnerable computers can quickly be turned into zombies, malware-infected machines remotely controlled by an attacker. Armies of these zombie computers are known as botnets. Vint Cerf, widely regarded as one of the inventors of the Internet, recently stated that approximately 25% of the computers on the Internet are botnet zombies (Weber, 2007). The SANS Institute's 2007 Top 10 Security Trends report noted that "The majority of bots will be bundled with rootkits," giving the attacker all-powerful root control of the infected machine (p. 2). Professor Felton noted that even if a consumer wanted to purchase a secure solution to protect himself, the market simply doesn't exist (2008). Although ominous, this paradigm is not new. A consumer in the market for an automobile in the first half of the 20th century faced similar challenges.

The Automobile: A Model For Computer Regulation?

The first automobile appeared on US roads in the 1890s and quickly revolutionized American life. "Before the automobile, people [either] lived in the city and worked in the city, or lived in the country and worked on a farm" (colorado.edu). As the automobile became commonplace, Americans were no longer limited by where they lived and worked and experienced incredible new freedoms. The effect of internetworking technology has been just as profound. Whereas the automobile gave people the ability to live and work wherever they wanted, internetworking technology has given people the ability to instantly access any information source they want.

Relatively large, stable, and slow compared to the horse, early automobiles were generally considered a safer mode of transportation. Although the first death attributed to an automobile occurred in 1899, at that time safety was not a primary concern of either the public (concerned primarily with expense, performance, and styling) or manufacturers (concerned primarily with minimizing cost). According to Professor Matthew Lee, "Both the industry and the public, with the exception of a few safety critics, agreed that auto safety was the responsibility of the driver" (1998, p. 3). As auto accidents mounted in frequency and severity (just as cyberspace attacks are escalating), the federal government responded slowly. Eventually, in 1966, the Highway Safety Act (DoT FHA) and the National Traffic and Motor Vehicle Safety Act (DoT DWI) were passed with the goal of protecting drivers, passengers, and pedestrians. Looking back, this regulation has clearly had a dramatic affect on public safety. Mandatory safety features such as seatbelts and airbags have saved countless lives. Just as importantly, automobile safety is now a major selling point and manufacturers are quick to innovate with new features including adaptive cruise control, night vision, heads-up display, and rearview cameras (CNET, 2008). The lesson here is a clear: after 1.5 million Americans died on US roads (Advocates, 2004), the government finally realized the automobile market was incapable of solving the problem and intervened. In doing so, the government planted seeds that quickly produced innovation and secondary market effects.

A frighteningly similar scenario is currently unfolding in cyberspace. According to Professor Felten, security engineering is often a secondary concern to firms focused on selling to end-users (2008). Just as automobile manufacturer's sought to minimize costs by skipping safety features, computer and operating system manufacturers try to increase margins by requiring consumers to

purchase security features (such as antivirus) separately. Security solutions that are included are often weak or misconfigured (Keizer, 2007). Critics of the Bush cybersecurity plan have pointed out that it fails to call for tough regulation and instead shifts responsibility for computer security to "[…] those least capable of doing it: individual users" (Lemos & McCullagh, 2002). Although here the term is "computer security" instead of "automobile safety," the situation is eerily reminiscent of the automobile industry's infancy: a rapidly expanding market that is both dangerous and unregulated.

Because of the "lemons problem"[1] effect described by Professor Felten, consumers are largely ignorant of the ramifications of their software purchasing decisions and are not clamoring better products (2008). Computer and software manufacturers, therefore, have no incentive to innovate and bring more secure solutions to market. Just as traffic fatalities steadily increased in the first half of the twentieth century (Advocates, 2004), the SANS Institute's 2007 Annual Update notes that computer security incidents are increasing: "We have seen significant growth in the number of client-side vulnerabilities […]. These vulnerabilities are being discovered on multiple operating systems and are being massively exploited in the wild, often to drive recruitment for botnets" (p. 1). Clearly, there are many parallels between cyberspace now and the US highway system in the first half of the twentieth century. In the 1940s, 50s, and 60s, the automobile industry purported that safety was the responsibility of the driver and recoiled at the idea of regulation (Lee, 1998). It would seem that the government and computer and software manufacturers are taking a similar position with respect to computer security.

Recommendations

The final section of this paper presents three recommendations for consideration by the next administration for addressing these problems.

Recommendation #1: Immediately require computer manufacturers to provide strong firewall and antivirus protection out-of-the-box (including default configurations certified by the government agency proposed in the next recommendation). For example, Federal Motor Vehicle Safety Standard #208 requires automobile manufacturers to provide seatbelts and airbags that meet certain minimum specifications (DoT FMVSS). Most security professionals would argue that firewall and antivirus are equally fundamental computer and network security mechanisms.

Recommendation #2: Pass legislation creating the cyberspace equivalent of the NHTSA. A logical starting point might be the US Computer Emergency Readiness Team. This new organization would have the responsibility of setting and enforcing computer and software security standards. Additionally, this new agency would also promulgate computer and software ratings similar to the NHTSA's crash safety rating for automobiles. If done correctly, this would help equalize the balance of information, in favor of the customer, when he is confronted with a purchasing decision.

Recommendation #3: Set a target date to require all operating system vendors to meet established "trusted system concepts" (Abrams and Joyce, 1995, p. 1). Fundamental principles to secure and

[1] The "lemons problem" is an economic phenomenon that describes vast differences in information available to buyer and seller.

trustworthy computing were first described by James Anderson in 1972 and included the following concepts:

- "The reference validation mechanism must be tamperproof" (p. 17).
- "The reference validation mechanism must always be invoked" (p. 17).
- "The reference validation mechanism must be small enough to be subjected to analysis and tests to ensure that it is correct" (p. 17).

An example of this in the automobile industry would be requiring manufacturers to install an odometer that is always running and cannot be rolled back. Hence, it is a trustworthy measure of a car's real age and therefore provides significant value. While the Department of Defense's Trusted Computer System Evaluation Criteria currently provides a mechanism to rate operating systems (using levels A through D), very few systems have been accredited with it (DoD, 1985). By improving the access control functions of the operating system with this type of reference monitor, exploitation of poorly coded software applications might be prevented (from returning root control of the machine to an attacker). If this can be accomplished, it would greatly diminish (and perhaps eliminate) both the value of attacking the average computer and the threats resultant from poorly coded applications.

Conclusion

Just as the automobile revolutionized the American way of life, the computer and the Internet are equally liberating and are expanding into almost all sectors of our economy and into every facet of our lives. Unfortunately, the opportunities for those who would do us harm are also exploding. According to the SANS Institute's Ten Most Important Security Trends of the Coming Year, the forecast is grim: "[…] antagonistic nations and terrorist groups, aware of the vulnerabilities, will radically expand the number of attacks" (p. 1). As Professors Lichtman and Posner point out by arguing for Internet service provider liability, holding computer users accountable for cyberspace security is not going to work (2004). In 1966, we eventually realized that American drivers needed the protection of federal safety regulation. Let's confront the similar issues playing out in cyberspace sooner rather than later.

Word count = 1866

Bibliography

Felten, E. (2008, February 11). Debugging Our Cyber-Security Policy. Lecture presented for the Silicon Flatirons' Digital Broadband Migration: Information Policy for the Next Administration lecture series, Boulder, CO.

The White House. (2003, February). The National Strategy to Secure Cyberspace.

Zelenka, A. (2007, October 6). From The Information Age To The Connected Age. Retrieved March 13, 2008, from http://gigaom.com/2007/10/06/from-the-information-age-to-the-connected-age/

Department of Defense. (1985, December 26). Trusted Computer System Evaluation Criteria. Retrieved March 12, 2008, from http://www.csrc.nist.gov/publications/history/dod85.pdf

The SANS Institute. (2006). The Ten Most Important Security Trends of the Coming Year. Retrieved March 12, 2008, from http://www.sans.org/free_resources.php

The SANS Institute. (2007). Top-20 2007 Security Risks (2007 Annual Update). Retrieved March 12, 2008, from http://www.sans.org/free_resources.php

Christian Science Monitor. Poverty Now Comes With A Color TV. Retrieved March 13, 2008, from http://articles.moneycentral.msn.com/Investing/Extra/PovertyNowComesWithAColorTV.aspx

Industry Analysis and Technology Division, Wireline Competition Bureau, Federal Communications Commission. (2007, October). High-Speed Services for Internet Access: Status as of December 31, 2006.

Weber, T. (2007, January 25). Criminals 'may overwhelm the web'. *BBC News.* 21 paragraphs. Retrieved March 14, 2003, from http://news.bbc.co.uk/1/hi/business/6298641.stm

Solove, D. (2007). "I've Got Nothing To Hide" and Other Misunderstandings of Privacy. *San Diego Law Review,* 44 (745).

Phillips, M. (2007, Jul 27). The Afternoon Report: Economy Hits Stride. *Wall Street Journal. (Eastern edition).* Retrieved March 14, 2003, from ProQuest.

Lee, M. (1998). The Ford Pinto Case and the Development of Auto Safety Regulations: 1893-1978. *Business and Economic History*, 27, 390-401.

CNET. (2008). Photos: Keep yourself alive--The latest automotive safety tech. Retrieved March 9, 2008, from http://reviews.cnet.com/4326-10895_7-6572803-1.html?tag=ss_prv

Advocates for Highway & Auto Safety. (2004). Motor Vehicle Traffic Fatalities & Fatality Rate:

1899 – 2003. Retrieved March 15, 2008, from www.saferoads.org/federal/2004/Traffic Fatalities 1899-2003.pdf

Dingfelder, S. (2003, December). Your car says: 'buckle up'. Psychologists inform regulators about the best way to remind drivers to use seat belts. *Monitor on Psychology.* 13 paragraphs. Retrieved March 14, 2003, from http://www.apa.org/monitor/dec03/seatbelt.html

Anderson, J. (1972, October). Computer Security Technology Planning Study. *ESD-TR-73-51*, I, AD-758 206, ESD/AFSC. Hanscom AFB, Bedford, MA.

Abrams, M., and Joyce, M. (1995). Trusted System Concepts. *Computers & Security*, 14 (1), 45-56. Retrieved March 16, 2008, from www.acsac.org/secshelf/papers/trusted_system_concepts.pdf

Lichtman, D., & Posner, E. A. (2004, July). Holding Internet Service Providers Accountable. *University of Chicago Journal of Law & Economics*. Retrieved March 7, 2008, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=573502

Lemos, R., & McCullagh, D. (2002, September 19). Cybersecurity plan lacks muscle. CNET News.com. Retrieved March 24, 2008, http://www.news.com/Cybersecurity-plan-lacks-muscle/2100-1023_3-958545.html

Baylor, K. (2006, September 11). Evolution of the Hacker Threat. SecurityProNews.com. Retrieved March 24, 2008, from http://www.securitypronews.com/news/Securitynews/spn-45-20060911EvolutionoftheHackerThreat.html

Author unknown. Retrieved March 24, 2008, from http://l3d.cs.colorado.edu/systems/agent sheets/New-Vista/automobile/history.html

U.S. Department of Transportation. Federal Motor Vehicle Safety Standards and Regulations (Part 571). Washington, DC. Retrieved March 24, 2008, from http://www.nhtsa.dot.gov /cars/rules/import/FMVSS/index.html

U.S. Department of Transportation. The Visual Detection of DWI Motorists. Washington, DC. Retrieved March 31, 2008, from http://www.nhtsa.dot.gov/people/injury/alcohol/dwi/dwihtml/index.htm

U.S. Department of Transportation. Federal Highway Administration Safety Overview. Washington, DC. Retrieved March 31, 2008, http://safety.fhwa.dot.gov/state_program/hsip/hsip_over.htm

Keizer, G. (2007, January 25). Anti-Spyware Rival Slams Microsoft's Windows Defender, Vista. InformationWeek.com. Retrieved April 1, 2008, from http://www.informationweek.com/news/security/showArticle.jhtml;jsessionid=1YCSM1TOC2ZBUQSNDLRSKHSCJUNN2JVN?articleID=197000593&_requestid=151063