Daniel Taylor

Information Technology 103, Section 003

Due: October 5th, 2010

The Never-ending Struggle for Online Security

"By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on http://academicintegrity.gmu.edu/honorcode/ . I am fully aware of the following sections of the Honor Code: Extent of the Honor Code, Responsibility of the Student and Penalty. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://universitypolicy.gmu.edu/1301gen.html web site."

10/4/2010

X Daniel Taylor

Introduction

Unfortunately, there is no such thing as absolute security on the Internet. It's literally impossible to eliminate the risks of fraud, identity theft, espionage, or malicious attack. But if you think about, that's no different than the real world. We make security tradeoffs all the time, finding acceptable levels for risks like privacy loss or theft. The dangers on the Internet are really no different than those in the real world. However, according to Schneier's *The Invisible Battleground* (2009), there are differences, and they trip us up again and again. We understand how the real world works, so we try to apply that understanding to the Internet. In the real world, we want to prevent copyright infringement, so we try to make bits so they can't be copied. We want to know where data comes from, so we try to enforce attribution. Schneier says our problem is that "we think we can design computer voting machines because we know how mechanical voting machines work. We build electronic banking systems that mimic the brick-and- mortar bank branches they've replaced, and social networking sites that try to capture all the richness of human interaction. But these things don't work as we envision, because the world of bits is unlike the world of atoms - and the same rules don't apply. This isn't to say that Internet security is impossible, only that we tend to go about it all wrong. But as more and more of our critical infrastructure moves to the Internet, we need to start getting it right" (Schneier, 2009, p.14). And even though these risks aren't completely unavoidable, it makes sense that many companies are dedicated to fighting these online threats. People want to be able to browse the internet, free from fear of losing all of their documents because of one wrong click on a fake advertisement.

Background

One thing laymen will often overlook when questioning the prevalence and persistence of malicious programs is that the Internet is global, there are no borders or boundaries. This needs to be taken into consideration by any entity wishing to enhance online security. “One of the reasons anti-spam legislation has so little effect is that most spam comes from overseas. Laws attempting to regulate anonymity will fail for similar reasons” (Schneier, 2009). New York Institute of Technology’s President Edward Guiliano, Ph.D. agreed with the fact that internet security enhancement needs to focus on the global aspect. At the first Cyber Security Conference on Sept. 15, 2010, he “explained the need for leaders in academia, security, and government agencies to collaboratively combat cyber security attacks on a global scale. ‘Logic has enabled the wonders of computer networks and the Internet, and is now a threatening explosive able to bring down the electrical grid, shut down ATMs, paralyze Wall Street, steal identities, and hamstring military forces,’ he said. ‘Developed nations are more vulnerable to these attacks than less developed nations. Now, for the first time in history, low-tech is a battlefield advantage’" (Computers, Networks & Communications, 2010). And there are even newer and sneakier kinds of malicious programs being introduced into the cyber world. “Cascading pop-ups. Web page re-directs. Crawling computer speeds. Anyone who’s been online has surely experienced the effects of spyware. A few years ago, organizations were mainly concerned with things like adware and cookies that track a user’s surfing habits. But spyware is becoming increasingly pernicious and sophisticated. Monitoring software, which is sometimes placed directly on computers and at other times is installed via Trojan horse or by automatic Web site download, can log keystrokes or send periodic screen shots back to attackers. Such applications, sometimes combined with ‘common word’ technology, are increasingly stealing users’ financial and other personal information. According to a Kaspersky Lab report, key loggers surged 500 percent in a recent three-and-a-half-year period. To fight this ongoing threat, the major antispyware vendors have rolled out products that use heuristics and signatures to identify, then either block or disable spyware, essentially taking a 'blacklisting' approach. However, as some IT security professionals discovered, there are other solutions. In recent years, some software companies have started bucking this blacklisting approach, opting instead for a solution that 'whitelists' the applications and executables that can run on workstations. In other cases, medium-sized businesses, which have typically relied on desktop security software and single-point network products, are finding they can afford more comprehensive perimeter solutions" (Wagley, 2008).

Potential Benefits

Cloud computing has enabled some programmers to create simple programs that protect one's computer without having to install more software. iSheriff Security as a Service (SaaS) is a cloud-based email and Web protection service. It offers anti-spam filtering, anti-virus and malware protection for web and email, real-time web 2.0 security, data leakage prevention for web and email, website filtering and category access management, website malware protection, acceptable user policy enforcement, email archiving and secure email encryption services, and reporting services for email and web security. "Cloud-based security, or Security as a Service, is an increasingly popular and effective means of gaining enterprise-class Internet security but without the need for additional hardware, tedious administration or IT expertise" (Computer Networks, 2010). People don't like having to buy all kinds of packs of virus software and hardware. This sort of convenient all-in-one type of internet security service is very popular in today's world. But users will see just how efficient such all-in-one services are.

Further Required Research

Many people have suggestions as to what to focus on to make the internet more secure. Schneier suggests that “the government needs to secure its own networks. This will take money, and it will take coordination. We need a cybersecurity coordinator, and he needs to have budgetary authority. This should be done openly, with commercial products, and not behind classified doors. Despite what the NSA might say, we should not weaken security by building systems to facilitate eavesdropping. We're all safer if information technology is more secure, even though the bad guys can use it, too. And the NSA should not be in charge of this in any case these are common problems with common solutions, and secrecy doesn't help.

Secondly, the government should use its immense buying power to improve the security of commercial products and services. Most of the cost of these products is in development rather than production. Think software: the first copy costs millions to develop, but subsequent copies are essentially free. Additionally, the government has to buy computers for all its employees, and secure all its networks. It should consolidate those contracts, and include explicit security requirements. This will motivate vendors to make serious security improvements in the products and services they sell to the government, and everyone else will benefit because vendors will include those improvements in the same products and services they sell commercially.

Also, we need smart legislation to improve security in places where critical infrastructure is in private hands. We shouldn't make the mistake of thinking the market will magically solve Internet security. There are lots of areas in security where externalities cause security failures. For example, software companies that sell insecure products are exploiting an externality just as much as chemical plants that dump waste into the river. Good laws regulate results, not methodologies. A law requiring companies to secure personal data is good; a law specifying what technologies they should use to do so is not. Mandating liabilities for software vulnerabilities is good; detailing how to avoid them is not. The government should legislate for the results it wants and implement the appropriate penalties, then step back and let the market figure out how to achieve those results. That's what markets are good at.

Basically, we need to invest broadly in security research. Basic research is risky; it doesn't always pay off. That's why companies have stopped funding it. Bell Labs is gone because nobody could afford it after the AT&T breakup. But the root cause of its demise was a desire for higher efficiency and short-term profitability - not unreasonable in an unregulated business. Government research can be used to balance that desire by funding long- term research. We should let the NSF and other funding agencies decide how to spend the money with minimal micromanagement from Congress; the same with the national laboratories. Yes, some research will sound silly to a layman. But no one can predict what will be useful for what. And compared to corporate tax breaks and other subsidies, this is chump change" (Schneier, 2009).

Conclusion

Just because something is impossible doesn't mean we shouldn't at least attempt to tackle it the best we can. There are many different ways to go about fighting spyware and other malicious programs. The key is that there needs to be continuous efforts to keep enhancing online security there are worldwide, continuous countering efforts to do the opposite.

References

Computer Networks; iSheriff: Channel Partners Hungry for SaaS. (2010, October). Internet Weekly News,839. Retrieved October 4, 2010, from Sciences Module. (Document ID: 2149693051).

Annotation: This article explained the benefits of cloud computing and iSheriff.

New York Institute of Technology; NYIT Combats Worldwide Security Issues at Cyber Security Conference. (2010, October). Computers, Networks & Communications,120. Retrieved October 4, 2010, from Sciences Module. (Document ID: 2149820331).

Annotation: This article shared what was discussed at the first Cyber Security Conference on Sept. 15, 2010 regarding worldwide cyber security issues.

Schneier, B. (2009). The Invisible Battleground. Ripon Forum, 43(4), 12-13. Retrieved September 30, 2010, from ProQuest Social Science Journals. (Document ID: 1907834621).

Annotation: This article delved into why malicious programs are so prevalent and what we can do to fight them.

Wagley, J. (2008, February). Winners in the Spyware Wars. Security Management, 52(2), 68. Retrieved October 4, 2010, from ABI/INFORM Global. (Document ID: 1462453261).

Annotation: This article explained what the current status is regarding fighting spyware.