STATEMENT OF JOHN E. SAVAGE

PROFESSOR OF COMPUTER SCIENCE

BROWN UNIVERSITY

BEFORE THE

COMMITTEE OF THE JUDICIARY

SUBCOMMITTEE ON

CRIME AND TERRORISM

UNITED STATES SENATE

HEARING ON CYBER SECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM

"THE TECHNOLOGY/POLICY INTERSECTION"

APRIL 12, 2011

Chairman Whitehouse, Ranking Member Kyl, and honorable Members of the Subcommittee, my name is John Savage. I am a professor of computer science at Brown University where I teach and do research in computer science. Thank you for inviting me to speak to you on cybercrime and terrorism, two very important issues.

As a nation we have chosen to computerize a very large portion of our data and infrastructure. Consequently, important and valuable personal, business and government information is now available electronically. We have also become very dependent on computer networks in our daily lives and to run governments and businesses. Unfortunately, as we know, computers and networks are not secure, putting both data and networks at risk as well as our national economy. For example, in 2009 U.S. citizens lost $560 million to computer fraud.[1]

Criminals, commercial entities, terrorist groups and nation states may compromise deployed systems and steal confidential data, such as personal identities, intellectual property, and state secrets. The global reach of the Internet, while profoundly useful also simplifies their task, thus compounding the problem. In addition, important parts of our critical infrastructure have been integrated into the Internet without sufficient concern for the myriad security hazards that are introduced. Consequently, if a major conflict is played out in cyberspace, one of the first casualties will be our economy, a daunting prospect. However, the ramifications can go well beyond just economic considerations.

How bad is the problem?

Sophisticated users today can easily penetrate our computers. In their annual 2010 report[2] PandaLabs (a private computer security company) says that 46.8% of computers worldwide were compromised. That's almost half of all computers. In early 2010 PandaLabs, Defence Intelligence (another IT security company), the FBI and the Spanish Civil Guard announced that they shut down the Mariposa botnet, a global network of 12.7 million compromised computers, an absolutely huge number of machines under the control of one group. Botnets are potentially large collections of computer based agents, all working collectively to generate spam, conduct

[1] U.S Department of Justice, Internet Crime Report.
[2] http://press.pandasecurity.com/wp-content/uploads/2010/05/PandaLabs-Annual-Report-2010.pdf

phishing expeditions, and run denial of service attacks, among other things. Phishing involves sending users messages that entice them into clicking on links, which downloads code and compromises their computers. A denial of service attack sends a flood of packets to one or a few web sites, overwhelming them and making them unavailable. This was done during the assault on Estonia in 2007 and as a precursor to the Russian invasion of Georgia in 2008.

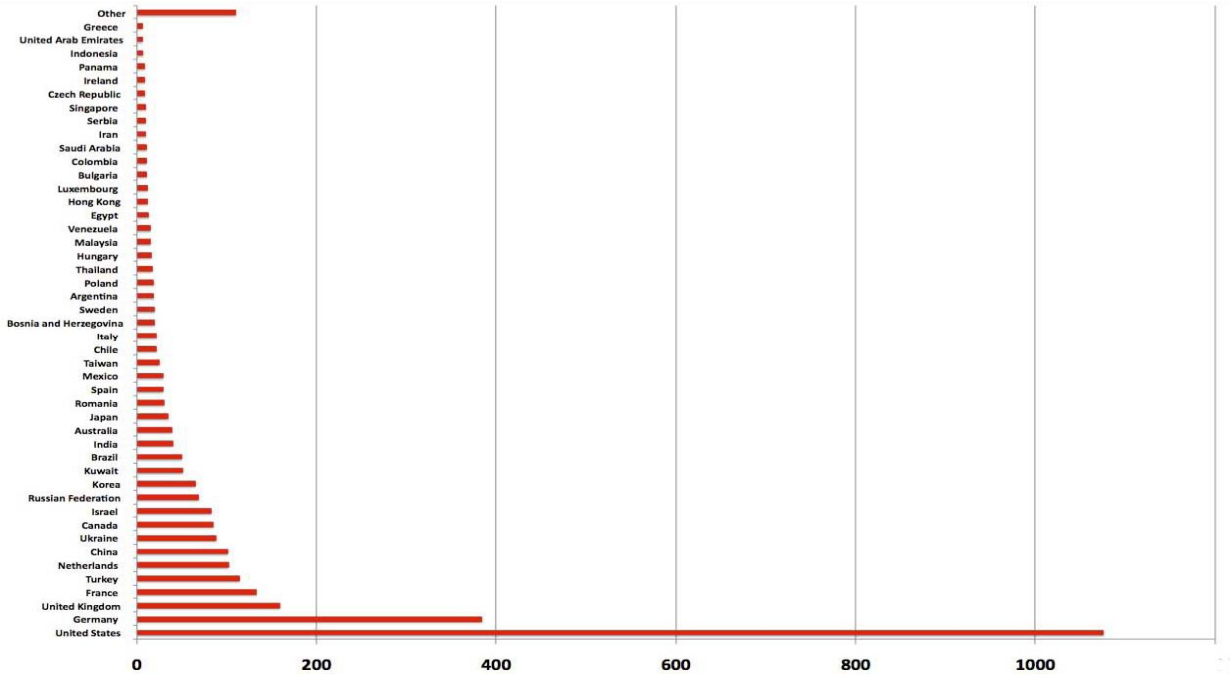
The computer industry knows that certain types of software error lead to theft, violations of privacy, and capture of the control of computers. For example, the MITRE Corporation with the assistance of the SANS Institute publishes a list[3] of the top 25 most dangerous software errors. And GFI Software reports[4] that seven of the top ten malware threats last November were Trojan horses, threats that grant complete control of a computer to an attacker.

Our networks and their support systems, such as the Domain Name System (DNS), are also vulnerable. They were designed on the assumption that individual users and network managers could be trusted to provide correct information when translating domain names, such as www.senate.gov, into IP addresses, strings of bits, and when circulating information about the available network paths. While it was reasonable to trust such information when the Internet was in its infancy, it isn't today. As a consequence, DNS attacks can not only send innocent users to malicious sites where their identities can be stolen, they can also result in traffic being routed to the wrong destinations.

An example of the latter type of attack was described in a recent paper[5] and press report[6] in which the authors claim that a 250,000-computer botnet could disrupt Internet routing globally. Imagine how much easier it would be to do this if a botnet of the size of the Mariposa botnet with almost 13 million computers were available. As shown in the graph below that was generated by Team Cymru[7] (an Internet security research firm), in January 2010 the U.S. had about three times as many botnets as any other nation.

---

[3] MITRE Corporation at http://cwe.mitre.org/top25/
[4] http://www.net-security.org/malware_news.php?id=1561
[5] **Losing Control of the Internet: Using the Data Plane to Attack the Control Plane**, Suchard et al, NDSS, 2011.
[6] **Death of the Internet, film at your local Cineplex**, I. van Beijnum, Ars Technica, March 21, 2011
[7] http://www.team-cymru.org/



What's to be done?

Computer industry insiders have solutions to many cyber security problems, but the incentives to adopt them are weak, primarily because security is expensive and there is no requirement they be adopted until disaster strikes. Nonetheless, many software companies, notably those who participate in BSIMM[8] (the Independent Software Vendors and the Financial Services Companies) have made great strides in eliminating software and system vulnerabilities that expose their products to attack. OWASP[9] plays a similar role for web-based security. Web applications offer some of the most challenging threats to identity management and theft. The fact that the cyber security problem remains a serious threat shows the need for much more research and development on the science and engineering of cyber security.

While waiting for research to bear more fruit, it makes sense for the U.S. government, together with the private sector, international partners, and independent agents, such as academics, to arrive at some reasonable software standards that all sufficiently large vendors selling software

[8] http://bsimm.com/online/
[9] https://www.owasp.org/index.php/Main_Page

in the U.S. should be required to meet. The same kind of standards could be developed and applied to the hardware vendors.

Although it is far preferable to protect systems in advance rather than patch them after vulnerabilities have been discovered, there is no alternative to requiring users to keep their software current. Because large botnets are a threat to national security, it is important to have some procedures in place to require inspection of computers to reduce the risk that they are compromised.

Protecting networks from hijackings (redirecting large volumes of traffic), man-in-the-middle attacks (intercepting traffic while en route to its destination), and routing disruptions require an entirely different set of steps. Problems of this kind are international in nature and must be handled that way. As noted in a 2009 National Academy of Sciences (NAS) study[10], it is unlikely that we can adequately secure the U.S portion of cyberspace without international engagement. Robert Knake, in a 2010 Council on Foreign Relations study[11], says that "The United States is being outmaneuvered in the international forums that will determine the future of the Internet" and warns that "nondemocratic regimes are … promoting a vision of the Internet that is tightly controlled by states." Furthermore, he says protecting our interest in "an Internet as a platform for increased efficiency and economic exchange … requires far more extensive engagement within Internet governance forums to shape the future of the network in a way that addresses security concerns without resulting in a cure that is worse than the disease."

In my opinion as a nation we should take seriously the recommendations of thoughtful observers on how best to engage the world community on this important topic while serving

[10] **Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities**, National Academies, Press, 2009.
[11] **Internet Governance in an Age of Cyber Insecurity**, Robert Knake, Report No. 56, Council on Foreign Relations, September, 2010.

our national interests. Healthy discussions on methods to develop norms of behavior and rules of the road for safe and secure operation in cyberspace should be welcomed[12].

The research and development agenda

Coming back to the research dimension, as mentioned above, the good news is that progress has been made in making software more secure by design. However, not all software vendors are applying these safeguards to their products. Furthermore, there is a lot of old software in use that has not been designed with security in mind. Finally, new software vulnerabilities are being invented all the time. Research and development to protect systems are needed to cope with these realities.

Progress has also been made in addressing serious network problems. Recently three authors published a paper[13] showing that they can defend against a multimillion-node botnet denial of service attack. For example, if the Mariposa botnet were to be used to attack government or military networks, the attack could be thwarted with their technique. This is very good news. A major threat to operations, especially in our net-centric military would be mitigated. Solutions have also been found to the network flooding attack[14] mentioned above that is designed to disrupt Internet routing globally.

The *crypto computing problem*[15], posed in 1978, is whether or not it is possible to encrypt data in such a way that computations can done without ever decrypting the data. If the problem has a solution, and if an attacker penetrates a computer equipped to behave in this way, the information obtained would be useless unless the attacker also has the keys to decrypt it. This problem remained unsolved until May 2009 when Craig Gentry provided a first proof of concept[16]. The proof is too costly to implement commercially today, but it does provide hope that an efficient solution could be found eventually to the data theft problem. This is the common path that many breakthrough discoveries take. First we must know that a solution

[12] *Cyber Security and International Agreements*, Sofaer, Clark and Diffie, **Procs. Workshop on Deterring CyberAttacks**, National Academies, Press. 2010.
[13] **Phalanx: Withstanding Multimillion-Node Botnets**, Dixon et al, Proceedings NDSI'08, 2008.
[14] **Losing Control of the Internet: Using the Data Plane to Attack the Control Plane**, Suchard et al, NDSS, 2011.
[15] **On Data Banks and Privacy Homomorphisms**, Rivest et al, Foundations of Secure Computation, 1978.
[16] https://researcher.ibm.com/researcher/view_project.php?id=1548

exists then we find an efficient one. Recently[17] both the Defense Advanced Research Projects Agency (DARPA) and the Intelligence Advanced Research Projects Agency (IARPA), recognizing the potential of this work, have funded research designed to find more efficient solutions for this technique. However, this approach is vulnerable in the sense that a secure computer is needed to encrypt the program and data in the first place and then decrypt the results.

Conclusions

The problem of making our computers, networks and applications safe from attack is unsolved and probably will remain so for several reasons. First, human innovation is relentless, and especially if there is money to be made or an enemy to defeat. Second, security has been notoriously difficult to define. This is illustrated by the fact that a single-bit error can result in a system intrusion.

Given the above, can the cyber security problem be made manageable? My answer is "Yes." I liken our computers to our homes. A determined attacker can easily break into them. So why aren't most of our homes invaded more often? Apparently because the locks are good enough, the neighbors sufficiently vigilant, uniformed police officers sufficiently visible, and the punishment, if caught and convicted, sufficiently onerous to deter attackers. We need to arrive at a similar state in cyber. However, it cannot be done without more secure hardware and software, surveillance of the abuse of computers and networks, government regulation, international engagement and, possibly, the creation of an intergovernmental organization. Since it is better to build in security rather than try to add it after the fact (such as firewalls and intrusion detection), hardware and software vendors and network providers should be required to conform to reasonable cyber security guidelines.

Recommended Governmental Actions

- Explore proposals for effective international cooperation on the development of cyberspace norms and rules of the road.

[17] http://blogs.forbes.com/andygreenberg/2011/04/06/darpa-will-spend-20-million-to-search-for-cryptos-holy-grail/

- Develop a targeted cyber security research program to address at least the following topics:
    - Find methods of conducting intrusion surveillance that protect privacy
    - Support research to discover efficient solutions to the crypto computing problem
    - Fund research to make existing systems and networks more secure
- Support programs to produce policymakers knowledgeable about computer and networking technology and technologists who can cooperate with policymakers.