U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON SCIENCE AND TECHNOLOGY
SUBCOMMITTEE ON TECHNOLOGY AND INNOVATION

HEARING CHARTER

Planning for the Future of Cyber Attack Attribution

Thursday, July 15, 2010
10:00 a.m. – 12:00 p.m.
2318 Rayburn House Office Building

I. Purpose

On Thursday, July 15, 2010, the Subcommittee on Technology and Innovation will hold a hearing to discuss attribution in cyber attacks, and how attribution technologies have the potential to affect the anonymity and privacy of internet users.

II. Witnesses

Dr. David Wheeler is a Research Staff Member of the Information Technology and Systems Division at the Institute for Defense Analyses.

Mr. Robert Knake is an International Affairs Fellow at the Council on Foreign Relations.

Mr. Ed Giorgio is the President and Co-Founder of Ponte Technologies.

Mr. Marc Rotenberg is the President of the Electronic Privacy Information Center.

III. Background

Cyber Attacks
Statistics clearly show that cyber attacks are common and costly. Following a recent survey of more than 2000 companies worldwide, Symantec reported that 42 percent rated cyber risk as their top concern, beating out other risks such as natural disasters, terrorism, and traditional crime. Symantec also reported that 75 percent of companies reported cyber attacks in the past twelve months and that 92 percent had seen significant monetary costs, averaging $2 million per year per company, as a result of those attacks.[1]

A 2004 Congressional Research Service report stated that "the stock price impact of cyber-attacks show that identified target firms suffer losses of 1%-5% in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate

[1] Symantec. (2010). *2010 State of Enterprise Security Global Results.* Retrieved from http://www.slideshare.net/symantec/2010-state-of-enterprise-security

into shareholder losses of between $50 million and $200 million".[2] According to a Market Wire article published in 2007, the economic impact from one comprehensive cyber attack on critical infrastructure could exceed $700 billion.[3]

Role of Attribution Technology

Being able to identify an attacker can be a strong deterrent against attack. During the Cold War, the Soviet Union and the United States remained in a nuclear standoff because either country would have been able to identify its attacker and stage a counter attack. In contrast, if a person, company, or government is attacked in cyberspace, it is often arduous – if not impossible – to determine the perpetrator of the attack.

Attribution technologies can be a useful tool in identifying and locating the assailant in a cyber attack. In terms of cyber attacks, attribution can be defined as "determining the identity or location of an attacker or an attacker's intermediary".[4] The attacker's identity can include a person's name, account information, or an alias. The location may include a geographical location or a virtual location, such as an IP address or Ethernet address.

In some cases, attribution technology may simply trace an attack back to an intermediary through which the attacker worked. For example, an attack can be transmitted via a fleet of 'zombies', or computers that can both delay and increase the severity of the attack. A sophisticated attacker may even be able to hide his or her identity so well that those looking for the attacker might falsely attribute the attack to an unrelated party. This can be done by an attacker who intentionally creates a false trail by sending incorrect data through any attribution process. To be effective and useful, new attribution technologies will need to have the ability to counter these, and future, methods of contravention.

The December 2009 attack on Google email accounts belonging to Chinese human rights activists in the United States, Europe, and China demonstrates the need for improvements in attribution technologies. Because the attacks showed a new level of sophistication, attributing their source has been a particularly difficult process. While the U.S. has been successful in tracing the attacks to two technical schools, it is still not known who was specifically behind these attacks.

In addition to helping to gain information about an isolated attack on a specific machine or network, successful attribution technologies can also be used to increase the security of the internet for people accessing personal information online – logging into a personal bank account, for example. If an online account required a recognizable IP range in addition to a pin code to retrieve account information, the ability of a hacker to access the account would be limited.

---

[2] Congressional Research Service. (2004, April 1). *The Economic Impact of Cyber-Attacks*. (Order Code RL32331). Washington, D.C.: Congressional Research Service. Retrieved from http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

[3] "New Research Shows Cyber Attack Could Cost U.S. 50 Times More Than Katrina". Market Wire. FindArticles.com. 09 Jul, 2010. http://findarticles.com/p/articles/mi_pwwi/is_200707/ai_n19429846/

[4] David A. Wheeler and Gregory N. Larsen, *Techniques for Cyber Attack Attribution* (Institute for Defense Analysis, IDA Paper P-3792. October 2003), p.1

Anonymity and Privacy

Complete attribution may have negative ramifications for internet anonymity and privacy. For example, dissidents in countries where the government censures websites with firewalls may bypass or attack those firewalls to access prohibited information. If the government had attribution technology that allowed it to completely attribute the attack to its firewall, the government might use the information gained through attribution to punish dissidents for accessing the information. There is also the potential for attribution technologies to be used by a government, a company, or individual to identify the source of a posting or comment on the internet that is intended to be anonymous.

IV. Issues and Concerns

As more and more of the Nation's infrastructure becomes dependent on the internet, the potential impact of a successful cyber attack against the United States increases. Many of the tools we rely upon in our daily lives (traffic lights, restocking food supplies, millions of office jobs, etc.) have the potential to be rendered non-functional through a cyber attack. While attribution technologies may play an important role in limiting the effects of such crippling attacks, there may need to be clearly defined limits on when such technologies should be used. For example, proactively tracing interactions within a system may help determine where an attack originated after one occurs, but tracing every interaction is impractical and quite likely unconstitutional. It may be appropriate, therefore, to limit the use of attribution technology in most cases to post-attack.

A second area of interest is who is, or should be, responsible for the development, coordination, and implementation of attribution technologies. Even if some critical infrastructure is privately owned, the government arguably has a responsibility to its citizens to ensure that the infrastructure is protected. Given the interest in ensuring that government resources are utilized efficiently, there may be a need to strengthen coordination and collaboration between government and industry on the development of new attribution technologies in order to avoid redundancy and leverage resources.

There may also be a need to determine the appropriate role of the government in responding to cyber attacks on private companies and individuals. In general, if a company or individual is physically attacked by an outside government, a company, or an individual, it is quite likely that the government would step in and defend the attacked company or individual. If a company or individual is the victim of a cyber attack, it is currently unclear what the government's role is, or should be, in responding to the attack.

Finally, the implications of attribution technologies for the anonymity and privacy of internet users should be considered. It may be necessary to consider ways to limit the use of attribution technologies to identifying the source of cyber attacks and in ways that do not suppress the freedom of speech or otherwise implicate the anonymity and privacy of people using the internet for legitimate purposes. There may also be a need to determine who (government or industry or both) should maintain responsibility for ensuring that attribution technologies are used consistent with any identified limits.

V. Overarching Questions

The following questions were asked of each witness:

- As has been stated by many experts, deterrence is a productive way to prevent physical attacks. How can attack attribution play a role in deterring cyber attacks?

- What are the proper roles of both the government and private industry in developing and improving attack attribution capabilities? What R&D is needed to address capability gaps in attack attribution and who should be responsible for completing that R&D?

- What are the distinguishing factors between anonymity and privacy? How should we account for both in the development and use of attribution technologies?

- Is there a need for standards in the development and implementation of attack attribution technologies? Is there a specific need for privacy standards and if so, what should be the government's role in the development of these standards?