Statement for Hearing on Cyber Crime: Modernizing our Legal Framework for the Information Age

Before the Subcommittee on Crime and Terrorism
United States Senate Committee on the Judiciary
July 8th, 2015

Mr. Chairman, Ranking Member Whitehouse, members of the Committee, thank you for the opportunity to contribute to this hearing. I am the senior director of community and public affairs at Rapid7, a security data and analytics company trusted by more than 3,900 organizations. We are participating in this hearing to represent the perspective of security researchers. I work extensively with researchers, both within Rapid7, and through the Metasploit Framework, which is an open source penetration testing platform driven by contributions from researchers. Metasploit gives organizations the ability to safely test their defenses against the tools and techniques used by cybercriminals in the wild, so defenders can understand whether attacks will be successful, what the impact of an attack will be, and what steps they need to take to protect their organization.

Given the complexity of technology, the pace of innovation, and the potential for human error, we can never expect to build or deploy completely invulnerable systems. Researchers act as independent auditors or antibodies in the digital immune system, mimicking the behavior of cybercriminals in order to test whether computing systems and networks are vulnerable to attack. Once flaws are identified, researchers alert the vendors and technology users, either directly or through a third party, providing the information needed to fix weaknesses and better protect customers and technical systems. Some work for the companies who build and deploy the systems, but many more operate separately. As independent testers, validators, and problem solvers, they are the antibodies of the digital immune system.

According to the Open Source Vulnerability Database, more than 13,500 technology vulnerabilities were disclosed in 2014[1]. This included the Heartbleed vulnerability, which impacted 17% of the secure servers powering the internet, undermining the security of hundreds of thousands of websites, including banking and healthcare sites that deal extensively with confidential personal information.[2] We also saw research revealing a bug in around 5,300 gas station tank gauges across the United States, exposing them to remote attack.[3]
It's clear that research is essential to our safety, yet it is at risk from both current and future legislation. The Computer Fraud and Abuse Act (CFAA) and similar state laws make no distinction between the well-intentioned work of researchers and the nefarious efforts of bad actors. Though they are primarily used to address cybercrime, these laws also deter security research.

Essentially an online anti-trespass law[4], the CFAA is intentionally broad; however, in the 30 years since the law

---

[1] The Open Source Vulnerability Database: http://blog.osvdb.org/
[2] "Half a million widely trusted websites vulnerable to Heartbleed bug," Netcraft, April 2014: http://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html
[3] "The Internet of Gas Station Tank Gauges," Rapid7, January 2015: https://community.rapid7.com/community/infosec/blog/2015/01/22/the-internet-of-gas-station-tank-gauges
[4] "Obama's proposed changes to the computer hacking statute: A deep dive," Washington Post, January 2015: http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/

was first enacted, technology has changed a great deal and the vagueness of the statutory language has become an increasingly big problem for the security research community. Today we see the statute being applied inconsistently by the courts, and unpredictably by prosecutors. The lack of clear definitions and boundary lines creates uncertainty over whether well-meaning research efforts will violate the law. This murkiness deters researchers from engaging in independent research projects, or disclosing accidental discoveries to those who can fix them.

This unfortunate effect is exacerbated by the law containing both criminal penalties and a private cause of action. Technology providers that fear the reputational fallout from a vulnerability disclosure use the threat of a lawsuit as a stick to scare researchers away. This is a worryingly common occurrence as many technology providers focus on the short-term impact to their business, and view independent researchers as trouble makers.

For example, a researcher found a flaw in an interactive toy designed to enable people to communicate with young children. Users were only supposed to be able to communicate with the child once approved by the child's parents, but the bug meant anyone could start talking to the child without their parents' knowledge. In addition, the system would send out information on the child including their name, age and location. When the researcher disclosed his findings to the toy's manufacturer, they threatened legal action. The researcher persevered and eventually the issues were addressed; however, the stress of the experience left the researcher wary of conducting further research.

While the majority of legal threats to researchers come from technology providers, they are not the most frightening concern. A researcher that worked on an internet scanning project that revealed vulnerabilities affecting tens of millions of routers in homes and offices around the U.S. faced the possibility of criminal prosecution. The project involved scanning publicly accessible assets on the internet and revealed important issues such as a bug that could be used to blow up buildings. This was disclosed to the technology vendors and infrastructure operators through the CERT Coordination Center[5] so they could be addressed. Despite the FBI determining that the research project was bona fide and valuable, the prosecutor thought it might be a violation of a state law that is similar to the CFAA. Eventually the prosecutor did drop the investigation; however, facing jail time understandably shook the researcher's confidence, and he ended the project and took a break from research altogether – not an outcome that makes any of us safer.

One of the problems this example highlights is the inconsistency with which these cases are brought, and the challenges presented by the complexity of them. Few prosecutors are actually experts in computer crimes, particularly at the state level, yet cybercrime convictions have become an appealing way to move ahead. This may encourage some to pursue prosecutions that penalize the people who are actually trying to make us more secure.

These are just two example; there are many more. When researchers suffer legal threats, it is not just them or security companies that lose; we all do. I assure you that criminals are looking for these bugs and will take advantage of them, so we need the expertise of researchers to help us protect ourselves. Ignorance is not bliss, it is insecurity. Chilling security research means we won't know what we don't know, and we cannot address issues until we become aware of them.

Yet for all the discussion around cybersecurity legislation, this is not a problem being addressed yet. Most discussions around updating the CFAA focus on extending its application and making penalties more stringent. Penalties are certainly an important part of deterring crime, particularly domestically within the U.S., but they

[5] CERT Coordination Center: https://www.cert.org/about/

are less likely to be impactful internationally when you consider how hard it is to prosecute foreign actors. Studies suggest that people determine whether to commit a crime based primarily on the likelihood of being caught, not the severity of the penalty[6]. This is probably even more the case with large organized crime groups such as the Russian Business Network[7], or state-sponsored hacking groups, such as Deep Panda[8].

This brings me to the Committee's proposed legislation, the International Cybercrime Prevention Act of 2015 (ICPA), which, among other things, would update the CFAA. I'd like to thank the Committee for giving us the chance to comment on the draft proposal. We applaud your emphasis on the prevention of cybercrime. There are a number of things the Bill does well and we were encouraged to see some updates to the proposal we saw from the Department of Justice at the start of the year.

In particular, we are very supportive of the provision intended to shut down botnets and agree this is best undertaken by law enforcement within the checks and balances of a legal framework. We also commend the Bill's focus on protecting critical infrastructure. It makes sense to include the requirement that "the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Our concern with the Bill is that it does not address the issues affecting security researchers. In fact, it could make the situation worse for them. We understand that creating a carve-out is a challenge as often researchers' efforts mirror those of cybercriminals, despite radically-different intentions. We strongly urge the Committee to consider this problem and whether there is a way to create an exemption for research, perhaps based around intent or outcomes.

In addition, clarifying and updating some of the language of the Bill will at least enable researchers to act with more confidence over what is or is not permissible. For example, the statute revolves around the concept of "authorization," but this term is not well defined. Likewise, notions of protected computers and obtaining information are drastically out of date and do not consider the role technology providers and owners may play in exposing data.

Without clarifying the CFAA and creating greater consistency in the way it is prosecuted and litigated, we diminish the value of security research and make it far harder for U.S. organizations and consumers to protect themselves. The reality is that technical systems are complex by nature and will always have bugs that provide opportunities for attackers. The only way to mitigate this is to support a culture where these issues can be proactively identified, disclosed, and addressed. It's not the imperfection of systems that should define us, it's how we respond to the knowledge that they will not be perfect.

Once again, I'd like to thank you for the opportunity of testifying today. I welcome your questions and comments.

---

[6] "Deterrence in Criminal Justice," The Sentencing Project, 2010: http://www.sentencingproject.org/doc/Deterrence%20Briefing%20.pdf

[7] "Shadowy Russian Firm Seen as Conduit for Cybercrime," Washington Post, 2007: http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html

[8] Deep Panda implicated in Athem attack: http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack