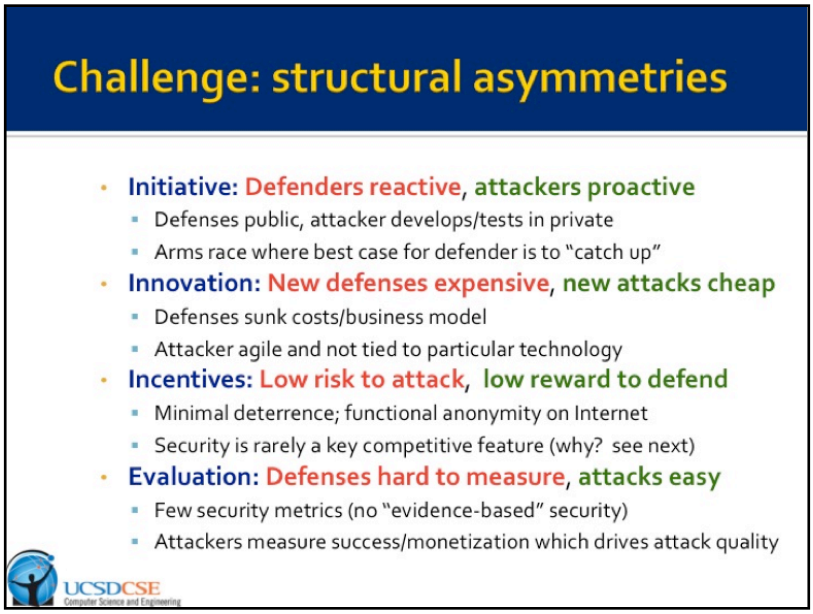
# Successes and Challenges of Computer Security Research

**Stefan Savage**
**University of California, San Diego**




Security – computer and otherwise – is part reality and part perception. Webster's dictionary captures this dichotomy in its definition: "freedom from danger; freedom from fear or anxiety." Telling one from the other can be difficult at any time, but it is even harder during times of technological change.

The benefits and risks of technology evolve hand in hand. Just as the internal combustion engine begat highway accidents and auto theft, many of the most visible and transformative successes of computing technology – e-mail, databases, e-commerce, the Web and so on – have ushered in new classes of abuse. Indeed, the global connectivity provided by the Internet has transformed the threats we face, just as it has transformed the rest of our lives.

However, countering our online threats is not merely a technological undertaking: economic and social forces are integrally involved. Fundamental to security is the notion of an adversary; persons or organizations with complex motivations and capabilities that must be understood and addressed in an integrated way. We must consider these issues because security in the real world is neither a binary property ("you have it or you don't") nor one that allows perfection. Security is ultimately about innovating faster than the adversary; ideally enough to stay ahead of the threats we will face.

Over the last two decades, the Federal Networking and Information Technology Research and Development (NITRD) Program has invested in a wide range of novel approaches to counter the ever-evolving classes of abuse. And, while we will never be "done," the progress has been significant.

For example, much of the recent evolution of computer abuse is driven by commerce. When the first Web browsers were developed and the notion of buying goods online emerged, people were concerned about divulging their credit card numbers. The solution was a protocol – Hypertext Transfer Protocol with Secure Socket Layer, or HTTPS – built directly upon research funded by the NITRD Program. (While HTTPS was engineered by Netscape, innovations in public-key cryptography, efficient private-key cryptography, key-exchange protocols, and certificate authorities and trust hierarchies – all supported by the NITRD Program – were necessary for its development.) HTTPS has been a tremendous success. It is not perfect, but it has enabled countless billion-dollar businesses for which fraud rates are relatively low.

HTTPS is by no means unique. Most of the mechanisms that today's computers use to protect users have their seeds in NITRD investments – mechanisms such as virtual private networks, network defenses (such as firewalls, intrusion detection, and data leakage protection), two-factor authentication, anti-malware, exploit mitigation (e.g., address space layout randomization, data execution prevention, stack cookies), vulnerability detection tools, and virtual machine isolation.

However, we will always have new challenges ahead of us in this constantly evolving landscape.

Today, botnets, spam, phishing, banking trojans, identity theft and so on are increasingly commercially motivated enterprises engaged in a constant arms race with computer security researchers. Once it became possible to make money from computer infection, whether through advertising (like spam) or theft (like stealing bank account credentials), this economic engine fed a bloom in online crime that we are still experiencing.

Looking forward, as we leave ever-more detailed online footprints – via purchasing, browsing and social relationships – we give rise to an emerging "big data" ecosystem that collects, processes and resells this information. Concerns about this issue are typically framed in terms of privacy, but security and privacy are intimately related: it is not simply about extracting information about people's desires and social relationships, but using that understanding to affect their behavior.

Finally, there is growing potential for the abuse of computers as instruments of organized conflict. These range from loosely organized "hacktivists" who see computing infrastructure as a natural target for their attentions to extremist groups and nation states with more strategic aims. While the obvious threats posed by these adversaries involve information theft or espionage, far more transformative is the potential for them to impact the physical world. The Stuxnet worm, designed to sabotage gas centrifuges in Iran, made it clear that computer attacks can in fact have physical, real-world consequences – a particularly troubling precedent because computing capabilities are now embedded in virtually every aspect of our lives – our civilian and military infrastructure, of course, but also our homes, our cars, even our bodies.

Hampering our ability to address all of these concerns is the asymmetric nature of the existing conflict:

- initiative – defenders are reactive, but attackers are proactive;
- innovation – new defenses are expensive, but new attacks are cheap;
- incentives – there is a low risk to attack, but a lower reward to defend; and
- evaluation – defenses are hard to measure, but attacks are easy.

Thus, it is not merely enough to create new defenses, but we must think structurally about which new types of activities can alter this playing field structurally. This is ultimately a research endeavor; one of high individual risk and high aggregate reward.

The Federal government has made a significant commitment to cybersecurity research through the NITRD Program over the last 20 years as described above, but the challenges of the future are every bit as great.