The Computer Fraud and Abuse Act Hampers Security Research

The Computer Fraud and Abuse Act is a vague law that chills important white-hat security testing of computers we use for critical tasks every day.

Sadly, computer manufacturers and system operators often do not want to hear about security flaws in their machines—learning about these problems means they’ll have to spend time and resources fixing them. But it’s better for all if these if these flaws come to light. The bad guys will find them, even if we do not talk about them and public awareness of security vulnerabilities creates pressure for manufacturers to address the problems and to build safer technologies for everyone in the future.

Why would we want to let security researchers test others’ computers without their permission?

- **To protect public health.** Several academic and independent security researchers, including computer science professor Tadayoshi Kohno at the University of Washington, have revealed security flaws in medical devices like insulin pumps and pacemakers. These vulnerabilities put the privacy and physical safety of patients at risk. As a result of this important computer science research, the Government Accountability Office has recommended that the FDA figure out a plan to keep tabs on the security risks of implantable medical devices.

- **To secure elections.** A number of computer scientists, including Princeton professor and former FTC chief technologist Ed Felten, have tested the security of electronic voting systems that use computers to record and tally votes in elections. This work has been critical in exposing flaws that would make it possible for wrongdoers to rig elections. Without this research, we wouldn’t know the problems exist, and there would be no pressure to fix them so that the election system isn’t vulnerable to attack. Now, the public can have an informed open debate about whether using electronic voting machines with no audit trail is a good idea.

---


• **To make driving more safe.** Computer scientists, including professor Stefan Savage at the University of California San Diego, are documenting security vulnerabilities in computer systems in cars. These flaws could make it possible for malicious hackers to interfere with car systems in a way that would make the vehicle less safe to drive, like tampering with the cars’ brakes. Without the work of these researchers, the public wouldn’t know about these flaws, and car manufacturers wouldn’t know that it is important to build these systems in a better way.

• **To protect consumer privacy on the Internet.** Computer scientists are studying how advertisers and other companies track consumers’ activities online and report web browsing details back to entities interested in knowing such information. By understanding precisely how this technology works, the researchers have also developed a tool called ShareMeNot that lets users block this tracking to protect their privacy.

Security research is important to keep all computer users safe. If we do not know about security vulnerabilities, we cannot fix them, and we cannot make better computer systems in the future. The CFAA should protect white-hat hackers and give them incentives to continue their important work.

---
