Editors: Matt Bishop, bishop@cs.ucdavis.edu
Deborah A. Frincke, deborah.frincke@pnl.gov

Computer Security Education and Research

Handle with Care

Bradley S. Rubin
University of St. Thomas

Donald Cheung
Minnesota Bureau of Criminal Apprehension

Many computer security researchers are actively seeking ways to detect attackers and their malicious code and tools to protect computing systems from hackers' activities. Sharing these research findings with practitioners and students magnifies the impact. In pursuing these goals, however, researchers, educators, and their students must ensure that their own computing activities remain legal and ethical. Computer security professionals should be equally cautious in assisting corporate or government computer resource owners with investigations.

Advances in technology often outstrip the legal system's ability to create statutes and experience case law to test them—a process that can take many years. In this column, we outline specific areas where those in academic security roles should tread carefully, particularly with regard to US laws.

Network sniffing

Network traces can be invaluable learning tools for understanding network protocols, malware, and attacker origins and behaviors. Yet, given that sniffing implies monitoring or intercepting data, researchers must be aware of possible legal ramifications. They should consult legal counsel regarding federal and state laws before conducting sniffing because legality in this area depends on the totality of circumstances. Federal and most state laws prohibit nearly anyone from intercepting communications between others, and violators can face harsh criminal or civil penalties.

The federal Wiretap Act was originally designed to prevent the interception of audio communications via common carriers (such as phone companies).[1] As technology advanced, the wiretap statutes extended the protection to include nonaudible digital communication, so they now apply to virtually any type of data transmitted via any network.

The wiretap statutes include several exceptions that let law enforcement or network owners legally intercept or monitor communication:

- *Provider protection.* Under this exception, network owners can monitor network traffic (intercept communication) to protect their rights and property from damage and theft of service. However, this exception is primarily for protection, and operators can face civil or criminal consequences if they deviate from that purpose.
- *Consent.* User consent—whether verbal, written, or implied—gives a network owner permission to monitor all activities that the user's computer generates. Many employers require employees to sign some type of electronic usage agreement, through which they relinquish privacy expectations while using company computers and networks. Companies and publicly accessible terminals increasingly use banners to obtain implied consent by forcing users to click on "agree" buttons before they can access system resources.
- *Computer trespass.* The USA Patriot Act's passage in October 2001 gave the US government the authority to monitor computer hackers' activities under specific circumstances.[2] Acting under the government's direction, network and system owners or operators can intercept computer trespassers' wire or electronic communications transmitted to, through, or from protected computers. Those acting under the government's direction must be lawfully engaged in investigations for which they have reasonable grounds to believe that the intercepted communications' contents will be relevant.

Network traces are such powerful teaching tools that we encourage their use, although we suggest that classroom exercises use only traces properly precaptured by instructors or captured by students sniffing their own traffic. Network switches reduce the risk of capturing sensitive bystander wired-network traffic because they have better privacy characteristics than network hubs. However, the increasing use of unse-

Program in depth

The University of St. Thomas, located in St. Paul, is Minnesota's largest private university, and has had more than 2,000 alumni in its 20-year history, which makes the university's graduate program in software one of the largest of its kind. The program draws on a large international student population, and night and weekend courses make it particularly attractive to working professionals.

The computer security concentration for the master's degrees consists of courses such as computer security, advanced computer security, computer forensics, and legal issues in technology. Both an instructional and a research laboratory are available for hands-on exercises and experiments. Philosophically, the computer security program emphasizes theoretical and applied engineering issues, such as the mathematical foundations of the Advanced Encryption Standard, as well as the human issues that are so often the weakest link in protecting information and systems.

More details about the graduate programs in software are available at www.stthomas.edu/gradsoftware.

University of St. Thomas at a glance

Location	St. Paul, Minnesota
Category	Private
Students	10,641
Percent undergraduate	52 percent
Baccalaureate programs	96
Graduate programs	46
Graduate programs in software founded	1985
Graduate programs in software students	689
Graduate programs in software faculty	26
Graduate programs in software alumni	2,000+
Graduate programs in software lab size	5,000 sq. ft.
Information assurance courses	4
Information assurance faculty	3

cured wireless networks reopens this privacy exposure risk.

Vulnerability testing

Port scanning for locating open ports on systems, fingerprinting for identifying the specific software behind open ports, and more detailed scans for identifying vulnerabilities can be valuable techniques for assessing systems' security postures. On the flip side, attackers can also use these tools to identify victims. At a minimum, running such tools without warning can waste the target network or system owners' time with responding to intrusion detection alarms. Worse yet, the scanner could be accused of preparing to initiate a computer crime. As with network sniffing, you must get the owners' explicit permission before running any vulnerability identification tools against their systems.

Once again, the safest classroom practice is to have the instructor precapture vulnerability scans for exercises. In some cases, students can perform vulnerability scans on their own systems using one of two approaches. Scanning in *loopback mode*—targeting the same system that runs the vulnerability scanning software—avoids many of the dangers we outlined, but it often obscures the true external view of the system's security posture across networks and firewalls. Using external computers to perform vulnerability assessments of their own computers can minimize dangers and present a truer picture for students. Assessing your own equipment can be powerfully instructive and motivating.

Honeypots

Honeypots are designed to look like production systems, but researchers use them to attract attackers and learn from their tools and techniques, or to provide indicators of possible compromise in related production systems. Honeypots are another powerful way to give students a real-world view of actual threats, but they raise interesting questions, from entrapment and wiretapping issues to potential liability. The Honeynet Project provides a great resource that describes the many legal issues in honeypot technology.[3]

Researchers must be aware of several issues when operating honeypots, including:

- *Intercepting communications and packets.* As mentioned, federal and state laws prohibit the interception of communications. Interestingly, honeypot owners might be able to obtain implied consent by using banner notification of communications intercept upon system connection. If such banners became common enough, attackers might ignore them and continue to engage the honeypots rather than being deterred.
- *Liabilities.* A honeypot owner could be held liable if a cracker utilized the honeypot's resources, such as bandwidth or storage space, to commit illegal acts—launching denial-of-service (DoS) attacks from the honeypot against other companies or government agencies or using the honeypot's storage space to distribute pirated music, movies, or child pornography, for example. Some recent implementations, such as the Honeywall (www.honeynet.org/tools/cdrom), are designed to use signature scanning and network packet-counting techniques to limit or halt outbound traffic, thereby reducing damage and liability.

- *Entrapment*. If caught, an attacker might try to use entrapment as a defense. To be successful, however, the defendant would have to prove that the honeypot owner went above and beyond normal system administration practices to entice the attacker to commit a crime that he or she was not predisposed to.

These issues also make great classroom discussion topics—satisfying the ethical and legal component that is sometimes difficult to achieve in technical programs.

Although these cautionary areas address honeypot operation, they provide no guidance for what a researcher should do once a honeypot is attacked. If a honeypot is used exclusively for research and has nothing of value in it, researchers aren't required to report attackers to law enforcement. Yet, tempting as it might be to turn the tables on computer attackers and bombard them with DoS attacks or break into their systems to further identify them, doing so isn't a good idea. An innocent third party might own the system originating the attacks—or perhaps it was made to look as if that were the case. Worse, the attacker might then have legitimate grounds for bringing legal action against the researcher for breaking into the attacker's system! Unfortunately, it's often best to report system misuse to the suspected originating network address owner's abuse email address, although that usually yields little action.

Viruses and worms

To understand how to protect systems from viruses and worms, it's essential to be able to dissect malware. More debatably, some researchers believe that writing new types of malware is important in developing defenses against future attacks. At the very least, such researchers must take extreme steps to ensure that the malware doesn't escape their research facilities and damage external systems. In fact, the risk of costly accidents is why writing viruses or worms is one of the few topics we discourage in student proposals for class projects.

Breaking encryption

One of the best ways to understand a technology is to take it apart, and many engineering students first gained both their interest and skills in computer technology through hands-on, exploratory hacking. Perhaps the ultimate challenge in computing is to break encryption algorithms and encryption-based hardware and software. Indeed, many best practices and important human issues in computer security have come from lessons learned through vulnerabilities that hackers brought to light.

Yet, the previously unlimited freedom to hack is increasingly falling under legislative control. In the US, the Digital Millennium Copyright Act (DMCA) allows circumvention, for good faith research purposes, of the encryption used for digital rights management (DRM) with copyrighted media.[4] The DMCA's numerous prerequisites include the following:

- researchers must lawfully obtain the media,
- circumvention must be necessary for the research,
- researchers must be trained in cryptography, and
- they must make good-faith efforts to obtain authorization in advance and notify the copyright owner of the research results.

Interestingly, DMCA doesn't allow research exceptions for non-encryption-based technologies, such as watermarking, used to protect copyrights.

Some researchers have decided that the effort of obtaining consent and the risk of broad legal interpretations branding their efforts illegal aren't worth the energy. The unfortunate upshot of the DMCA's requirements could be to inhibit research in this area even as a better-informed and skilled underground develops because those with malicious intent are unlikely to be deterred by the legal constraints.

Vulnerability disclosure

When researchers come across security vulnerabilities in software products, it's customary to give a company some time to react before making them public. Publicizing the vulnerability too early can allow attackers to use the information to prepare attacks before a patch is ready, but doing so too late can let others find the flaw as well and prepare attacks. Moreover, delaying too long lessens the pressure on vendors to fix problems. CERT, for example, has a policy of allowing 45 days to pass before making vulnerabilities public.

Child pornography

In the areas we mentioned earlier, it's possible to do academic research while proceeding with caution. Child pornography, however, is strictly off limits for all purposes. In the US, possessing child pornography is a crime for anyone other than a sworn law enforcement agent. In addition to federal statues, virtually all 50 states have similar laws to prohibit individuals from possessing, distributing, or manufacturing child pornography.

According to federal statutes (US criminal code), child pornography is defined as (excerpted)[5]:

> Any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where— …
>
> (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. …

Federal and state statutes are very similar in their definitions. The penalty for possessing child pornography is very harsh; each image is considered one count. In Minnesota, each count can carry up to five years' imprisonment and fines.

Computer security researchers employ various techniques and technologies to conduct their activities in an effort to protect existing systems and develop designs for future secure systems. Although the intent serves the overall societal good, the methods must remain both legal and ethical. The specific areas we discussed here require attention and care. These issues also make great classroom discussion topics in any information security curriculum—satisfying the ethical and legal component that is sometimes difficult to achieve in technical programs. □

References

1. *Wire and Electronic Communications Interception and Interception of Oral Communications*, *US Code*, title 18, chapter 119, 2004; www.access.gpo.gov/uscode/title18/parti_chapter119_.html.
2. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act*, 2001; www.fincen.gov/pa_main.html.
3. The Honeynet Project, *Know Your Enemy: Learning about Security Threats*, 2nd ed., Addison-Wesley Professional, 2004.
4. *Digital Millennium Copyright Act*, US House Rule 2281, US Copyright Office summary, 1998; www.copyright.gov/legislation/dmca.pdf.
5. *Sexual Exploitation and Other Abuse of Children*, *US Code*, Title 18, Chapter 110, www.access.gpo.gov/uscode/title18/parti_chapter110_.html.

Bradley S. Rubin *is an assistant professor at the University of St. Thomas, in St. Paul, Minnesota. His research interests include computer security and information retrieval. Rubin has a PhD in computer science from the University of Wisconsin, Madison. He recently published a book chapter "Public Key Algorithms" in the* Handbook of Information Security *(Wiley, 2005). Contact him at bsrubin@stthomas.edu.*

Donald Cheung *is a special agent at the Minnesota Bureau of Criminal Apprehension. His research interest is in computer forensics. Cheung has an MS in software engineering from the University of St. Thomas, where he now teaches a computer forensics course as an adjunct instructor. Contact him at donald.cheung@state.mn.us.*