Editors: Michael Lesk, lesk@acm.org
Martin R. Stytz, mstytz@att.net
Roland L. Trope, roland.trope@verizon.net

Strengthening the Weakest Link in Digital Protection

William Suchan and Edward Sobiesk
US Military Academy

Although much has been written about digital protection technologies, the greatest vulnerability in any system is invariably the person behind the keyboard. In our one-semester course at the US Military Academy in New York, we educate roughly 800 undergraduates from nontechnical fields each year on intermediate-level IT skills. We place our students in an isolated virtual-computing environment, give them hands-on experience with a variety of attack vectors that hackers use to exploit vulnerabilities, and provide them with a multidimensional framework for understanding and mitigating risks. As a result of this educational experience, our students are better able to internalize the concepts we teach and end up with an increased realization of the actions required to protect crucial resources.

A hybrid approach

The Digital Protection department's goal is to keep readers informed of the latest technological advances relevant to protecting digital property, whether it be intellectual property, valuable information, or financial assets stored and transmitted digitally. Advances in this arena usually come from security professionals who received an in-depth education in the technical aspects of security while enrolled in computer or engineering programs, such as those our colleagues describe.[1] Unfortunately, this highly educated population is very small.

Public and private sector organizations have used various approaches to reach those who will have the biggest impact on digital protection: end users. User-education programs, often referred to as *awareness campaigns*, often fail to enhance digital protection because they neglect to take into account the fact that the typical user's mental model[2] doesn't value intellectual property. Even some of the best awareness efforts—such as West Point's Carronade exercise, which sends emails to users to test whether they'll fall prey to spear phishing attacks[3]—do little more than teach users about self-preservation or how to prevent themselves from becoming cybervictims.

With both ends of the awareness-education continuum well covered—and neither end adequately addressing digital protection—we attempt to establish a suitable middle ground. The result is a unique hybrid approach that encompasses both education and awareness. Because we teach technical concepts and skills to students in nontechnical majors, we had to choose our pedagogical approach very carefully. Rather than using just one of the two most common security education philosophies[4]—focusing on either attack or defense operations—we chose both. By juxtaposing both operations, students see firsthand the need for multilayered defense techniques.

Even when users have the motivation to secure their own systems and understand the importance of protecting valuable personal information, they don't necessarily have any incentive to value others' intellectual property. We blame the slanted development of their mental model: students today believe that anything they find on the Internet is fair game, and ownership is merely a matter of downloading. To counter this attitude, we seek to develop in our students a sense of the importance of intellectual property. We feel that unless students respect the property of others, they won't have a strong motivation to protect it.

To achieve our goal of reducing the potential vulnerabilities nontechnical users introduce, we've integrated three major components into our course:

- a broad overview of key IT topics;
- lessons directly targeting information assurance (IA); and
- a recurring thread of ethical and security considerations that's explicitly injected into lessons throughout the semester.

We combine these components into a mandatory intermediate-level IT course for juniors majoring in nontechnical majors such as the humanities or social sciences. The only formal computer education these students possess is from a freshmen introductory IT course.

A broad IT foundation

A general overview of key IT topics increases our students' technical knowledge and facilitates their ability to be safer users. Our course ma-

terials include advanced and dynamic Web design and implementation, the digitization process, networking, databases, information systems, and a specific block of lessons devoted to IA. Students also study several aspects of military and commercial IT infrastructures such as packet switching and bandwidth utilization, as well as learn IT concepts and techniques that will facilitate their professional success and inspire life-long learning in the IT domain. We intend for the course material to complement the immersive IT environment in which our students function; all students own laptops, and all classrooms and dorm rooms have wireless or wired Internet and network connectivity.

Our course explores the underlying technologies in greater depth and breadth than most general education IT courses. From detailed coverage of the TCP/IP protocol to understanding run-length encoding to sophisticated relational database development, we always try to take students a few degrees deeper than they ever have to go as typical users. Besides the direct educational benefits, going deeper into a few areas creates a mindset that depth exists in all areas, and such a mindset improves security. Anecdotal evidence shows that students are internalizing course concepts—after the course ends, they sometimes forward technical articles and news releases to us and are proud of the fact that they understand the technical content. We also receive several reports each year from students who are using what they learned in the course while engaged in summer internships.

Specific IA content

Several lessons in our course directly target the topic of IA. We teach students to apply the IA model[5] shown in Figure 1, which focuses on the intersection of information states, security services, and security countermeasures. We follow this up with multiple hands-on security experiences using both isolated physical networks and virtual networks constructed with VMware.[6]

Learning to apply the IA model increases the user's ability to mitigate risk in several ways. The reference framework brings to light the multidimensional aspects of information security and teaches students to focus on one intersection of components at a time (see Figure 1). The IA model also stresses that security countermeasures involve more than just technological solutions. Finally, and perhaps most importantly, users fully understand their specific role in security; students are often surprised to learn that in many situations, the user is the most important, and possibly the only, line of defense.

Additionally, we teach our students to look at cyberattacks from both the attacker's and the defender's viewpoints. We cover an attacker's actions in terms of the reconnaissance, exploitation, and consolidation phases, and discuss the defender's actions in terms of the prevention, detection, response, and recover and restore phases. We then evaluate these phases in terms of the IA model.

Hands-on experiences using VMware strongly reinforce IA concepts and demonstrate to students the powerful capabilities that attackers possess. VMware is a virtualization environment that lets you set up a network consisting of multiple operating systems that all run on a single machine. During these lessons, students use lab computers loaded with a virtual network that includes a Windows XP attacker system and a Windows 2000 victim system. Throughout a three-lesson sequence, we teach students how to use sites such as the American Registry for Internet Numbers (ARIN; www.arin.net) and software such as SuperScan (www.foundstone.com) to passively and actively perform reconnaissance on potential victims; properly employ a firewall to counteract active reconnaissance; conduct a security assessment to identify vulnerabilities using Nessus (www.nessus.org); and attack a system using both a buffer-overflow attack and Trojans with the SubSeven and NetBus tools. It's important to note that we don't teach students how to conduct actual attacks; rather, we make them aware of common vulnerabilities that attackers use to compromise systems. As a result, once the students start to explore attackers' tools, they're usually shocked at how easy it is for an attacker to exploit vulnerable systems and gain control of remote computers.

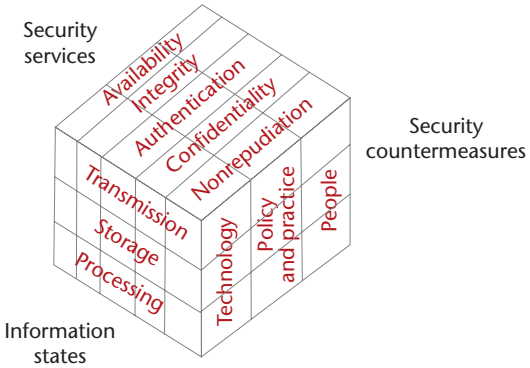

Figure 1. Information assurance (IA) model. We teach students to apply the IA model to a wide variety of situations, such as the use of encryption as a countermeasure to provide confidentiality during data transmission.

The course's final exercise requires students to set up an actual client-server network, which includes the use of front-end Web forms to submit information to a back-end database on a server. Students then use laptops to eavesdrop on the network and intercept traffic using Ethereal's (www.ethereal.com) packet-sniffing capability. As a countermeasure, students encrypt their transmissions using Secure Sockets Layer (SSL) to ensure information confidentiality. We then evaluate the students' actions within the context of the IA model, and the students finish the course's IA section far more knowledgeable and with a far better security mindset than they had a few lessons earlier.

Recurring threads

A final component of educating users involves an ever-present awareness of security throughout the course's other lessons. During a lesson on biometrics, for example, students explore the advantages and disadvantages of biometric security using fingerprint, iris, and facial recognition technologies, including demonstrations of false accepts and rejects. For the course's network-design project, students often use security as one of the criteria against which to evaluate their designs' suitability. Throughout the semester, we discuss common security vulnerabilities as well as countermeasures that students can apply directly to their own computers.

The last piece of the puzzle, and the lynchpin of the course's digital protection aspect, is the IT ethics thread that runs throughout the semester. Although it's not a novel idea to include ethics in an IT course, we apply ethical lessons specifically to attack the mental model that our students initially have regarding intellectual property in cyberspace. Students clearly understand the concept that merchandise in a store is the store owner's property. Likewise, we must force them to realize that intellectual property belongs to its owner, and that their concept of physical property and cyberproperty should be exactly the same.

We've found that the best way to inculcate this ethical lesson into our students' minds is to force them to use it. Students have lectures, assigned readings, and exercises about intellectual property, but by requiring them to apply these concepts in their projects, they learn the habits they'll need later in their professional lives. For the course Web design project, for example, we encourage students to "shop" for Web designs, but they must get permission to use the design before it shows up in their work. This might include contacting copyright holders directly to seek permission or using Web sites such as Open Source Web Design (www.oswd.org), in which authors provide usage instructions. This lets students feel that they're not only doing the right thing, but that the right thing is relatively easy to do—which goes a long way toward changing their concept of cyberproperty.

We seek their realization that it's hypocritical to use technology to keep attackers out if [users] simultaneously violate copyright law through illegal downloading.

When the semester ends, we've succeeded only if our students realize that all the technology they can apply toward cyberdefense is worthless if they don't respect intellectual property. We seek their realization that it's hypocritical to use technology to keep attackers out if they simultaneously violate copyright law through illegal downloading. Digital protection can only be truly successful when users realize that their personal integrity is the only thing that prevents them from becoming the cybercriminals they're trying so hard to thwart. ▢

References

1. R. Dodge and D. Ragsdale, "Technology Education at the US Military Academy," *IEEE Security & Privacy*, vol. 3, no. 2, 2005, pp. 49–53.
2. D. Norman, *The Design of Everyday Things*, Doubleday, 1988, p. 17.
3. A. Ferguson, "Fostering Email Security Awareness: The West Point Carronade," *Educause Quarterly*, vol. 28, no. 1, 2005, pp. 54–57.
4. D. Frincke, "Who Watches the Security Educators?," *IEEE Security & Privacy*, vol. 1, no. 3, 2003, pp. 56–58.
5. W. Maconachy et al., "A Model for Information Assurance: An Integrated Approach," *Proc. 2nd Ann. IEEE Information Assurance Workshop* (IAW 2001), IEEE CS Press, 2001, pp. 306–310.
6. D. Ragsdale, S. Lathrop, and R. Dodge, "A Virtual Environment for IA Education," *Proc. 4th Ann. IEEE Information Assurance Workshop* (IAW 2003), IEEE CS Press, 2003, pp. 17–23.

William Suchan *is an assistant professor and the IT Core Program Director in the Department of Electrical Engineering and Computer Science at the US Military Academy in New York. He has a PhD in computer science from Arizona State University. Contact him at william.suchan@usma.edu.*

Edward Sobiesk *is an assistant professor and course director for the IT305-Theory and Practice of Military IT Systems course in the Department of Electrical Engineering and Computer Science at the US Military Academy in New York. He has a PhD in computer and information sciences from the University of Minnesota. Contact him at edward.sobiesk@usma.edu.*