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

A Human Endeavor

Lessons from Shakespeare and Beyond

Matt Bishop
University of California, Davis

Deborah Frincke
Pacific Northwest National Laboratories

As the fall term begins, computer security students expect to buy heavy textbooks filled with equations, information theory, and programs that sort, encipher, and route network packets. Yet, nontechnical classes with very different kinds of textbooks also have much to offer today's security students. In addition to satisfying most colleges' general education requirements, such classes provide core background material that explains aspects of computer security that most technical courses overlook.

Twenty years ago, it was unusual for colleges to offer even one course in computer security, privacy, or information assurance. In 2005, the US National Security Agency certified 67 academic institutions as Centers of Academic Excellence in Information Assurance Education, which means they offer academic programs that emphasize computer security. A wide spectrum of colleges offer courses in digital forensics, security in electronic commerce, privacy law, certification standards such as the Common Criteria, and other specialized topics.

The positive aspect of this proliferation is that these technical classes make information available to students who would have struggled to find it earlier. The negative aspect lies in the all-too-frequent assumption that computer security is primarily a technical subject. This ignores the fact that computer security's technical aspects are founded on critical principles common to many fields of learning. As with any principles, students who see them applied to different fields learn to adapt them to diverse situations and environments—both key elements to career success. In this article, we highlight important noncomputer disciplines that modern undergraduate or graduate technology students' educations often neglect.

Psychology

To begin, consider that people are the cornerstone of computer security. To understand people, we must turn to the study of the mind and behavior: psychology. Among its many applications, psychology can help us determine why someone might want to breach a system's defenses. What do they hope to gain? Why are they attacking this particular system or site rather than another? This speaks to threat modeling and risk analysis—determining what resources need to be protected and where to place the greatest efforts in developing security mechanisms.

Psychology can also help us determine who's likely to be attacked. Why do people give out passwords when asked? How do attackers target victims who are more apt to click on links that say "special offer" or open email attachments that appear to come from someone they know? Cognitive psychology courses examine how people understand such stimuli, and how and why they react as they do. Armed with this knowledge, we can more effectively minimize the likelihood that people will react as attackers desire. This speaks to which types of controls, warnings, visual or auditory cues, and other defenses are likely to be effective, and which will likely fail.

Another application of psychology is in understanding how people might breach a system's defenses. This helps us determine the specific security mechanisms to use. Is supplying a password sufficient for authentication, or should DNA analysis be required? The principle of *psychological acceptability*[1]—which states that security mechanisms shouldn't make the resource more difficult to access than if the mechanisms were absent—implies that security mechanisms should be as unobtrusive as possible. It also means they must be designed to be usable.

Donald Norman's wonderful book, *The Design of Everyday Things*,[2] describes design principles for daily life and provides insight into why so many things are hard to use. The principles also apply to configuring computer security mechanisms. For example, does a requirement that people change passwords every 90 days lead them to select easy-to-guess passwords or write them on notes they stick to their monitors? This speaks to the implementation of the security mechanisms.

Without understanding something about how people interact with mechanisms, it's easy to blame users for security breaches that actually arise from shortcomings in the mechanisms. A security mechanism should be fail-safe and should provide feedback to tell those configuring it exactly what it will do. It should detect any inconsistent or anomalous settings, assume that people are trying to breach or evade it, and warn the administrators. Unless all these characteristics are present, you can't blame the user.

Many nontechnical works present themes that are directly applicable to technical issues … Literature can help us look at underlying assumptions and the impact of change.

Shifting focus suggests another application of psychology—understanding the attacker. How can we trick attackers into wasting their efforts or taking actions that let defenders figure out what they're doing, what they want, and where they're coming from? Cliff Stoll's success shows the benefits of applying basic psychology to defense.[3] He tricked an attacker into downloading a very large file that kept the attacker's telephone line open long enough for authorities to trace the call—which was international.

Bill Cheswick shows another approach: deceiving attackers into thinking they have access to the system.[4] His classic paper explains the choices he made to convince an attacker that responses were coming from the computer rather than from him. Had Stoll not known anything about psychology, he couldn't have created a convincing file or gotten authorities interested in the attack. Similarly, Cheswick would have been unable to deceive his attacker without an understanding of psychology.

Literature

Like psychology, literature teaches about people. Basic human and societal needs—for safety, love, understanding, knowledge, privacy, and so on—run through stories and myths of all cultures. Indeed, many nontechnical works present themes that are directly applicable to technical issues. Shakespeare's plays, for example, provide insight into the need for various computer security mechanisms. Consider *A Comedy of Errors*, in which everyone confuses twins for one another. What better metaphor for the problems a lack of authentication can create? Or consider *Julius Caesar* for a tragic study of the insider threat—Caesar's assassin, Brutus, was his trusted friend. A pivotal scene in *The Merchant of Venice* shows the effects of imprecision in specifications.

Modern fiction provides similar insights. Isaac Asimov's "Nightfall" shows the effects of assumptions gone awry. Cordwainer Smith's "The Crime and the Glory of Commander Suzdal" shows the repercussions of using an effective security mechanism without considering the environment in which it is used.

Turning to the classics, we find that Homer's *Odyssey* presents the most famous use of malware—the original Trojan horse. The trick Odysseus used to persuade the Trojans to bring the horse inside the unbreachable city walls, the Trojans' ignoring of warnings from Cassandra and Laocoön, and the resulting sack of the city parallel modern attackers' methods for tricking users into executing programs that breach security mechanisms as well as the aftereffects of ill-founded trust.

Nonfiction is another source of useful information. Consider Sun Tzu's *The Art of War*. This 2,500-year-old work brilliantly illuminates best practices for attacking and defending systems with its descriptions of planning, approaches, strategies, tactics, and, most important, what not to do.

In a broader sense, literature can help us look at underlying assumptions and the impact of change. Alfred Bester's *The Demolished Man* asks how, in a society with telepaths, someone can commit an undetectable murder. Larry Niven's "The Alibi Machine" looks at teleportation devices in the context of crime. James Halperin's *The Truth Machine* presents a world in which infallible lie detectors are widely available. These works all examine the disruptive effects of new technologies and new rules and how societies react to them. The effects of introducing new security technologies or changing policies and procedures are less dramatic, but a common theme remains: we must consider how changes will affect people and recognize that those changes might affect them in unexpected ways.

Other topics

Combined with telephone and fax mechanisms, the Internet has triggered a revolution in information dissemination, and societies are struggling to cope with the new global system and the security and privacy issues it presents.[5] Views differ greatly in the multiplicity of political jurisdictions that this web of information reaches. Yet, how many students graduate with more than a shallow understanding of the practical effects of these varying views? Political science courses can help students understand the gulfs between cultures and better equip them to provide solutions that can be widely adopted. For example, cultural differences among the United States, France, and China with respect to protecting "privacy" have vast implications for the kinds of defenses, auditing, and regulations that are appropriate for development—particularly when they extend beyond national boundaries. Maintaining sensitivity to local mores while supporting global interaction is difficult, and it's likely to become even more complex—whether interconnectivity has become a basic human need is an existential question for this century.

To face the challenges of risk and cost-benefit analysis, technical students can benefit greatly from courses in economics and business. For example, how much does it really cost for a campus to teach all incoming freshmen to install and maintain up-to-date virus protection on their laptops? How much does it cost not to? Is it cheaper to hand out free copies of antivirus software to incoming students or to enforce a policy that requires that antivirus software be up-to-date before connecting to campus systems? Simply defining business costs for security is difficult, let alone computing them and getting people to agree on issues such as whether to include salaries of system administrators and help-desk personnel based on the time they put in, or whether to exclude salaries for those who would be paid anyway.

This illustrates the need for persuasion skills. Security analysts can rarely just decide that a security mechanism or policy should be put into place and then demand that it be done. They normally have to convince management that the change is needed. That means being able to make a business case—to show that the cost of not implementing the change is greater than the cost of implementing it—which requires knowledge of the business as well as the ability to analyze alternatives, present information in writing, and speak publicly. These skills are the province of English and rhetoric (or public speaking)—two more subjects well worth a technology student's study.

This brings us to arguably the most important nontechnical aspect of a computer security student's education: the study of teamwork and the dynamics of teams. Although already a core discipline in modern society, the subject is often neglected or, at most, taught by simply organizing students into groups and telling them to work on the same project. Two interlocking problems commonly arise in this approach: some team members undertake most of the work while others neglect their responsibilities, believing (or knowing) that other team members will cover for them lest all suffer. A course taught by an instructor who knows how to organize teams and teach how team members work together is invaluable. Security students might thus do well to take up team sports because good coaches are experts at this.

Ultimately, computer security is more about people than about computers and information. Security solutions that fail to take human nature into account are doomed. We've touched on a few nontechnical areas of study with direct applications to computer and information security. Many other disciplines offer equally relevant lessons, although space precludes our mentioning them all. Both traditional and lifelong-learning students can broaden their horizons beyond the newest books on network security to encompass other important, but less obvious, possibilities. □

Ultimately, computer security is more about people than computers and information. Security solutions that fail to take human nature into account are doomed.

References

1. J. Saltzer and M. Schroeder, "The Protection of Information in Computer Systems," *Proc. IEEE*, vol. 63, no. 9, 1975, pp. 1278–1308.
2. D. Norman, *The Design of Everyday Things*, Basic Books, 1988.
3. C. Stoll, *The Cuckoo's Egg*, Pocket Books, 1995.
4. W. Cheswick, "An Evening with Berferd, in which a Cracker is Lured, Endured, and Studied," *Proc. Winter Usenix Conf.*, Usenix Assoc., 1972, pp. 163–173.
5. T. Friedman, *The Lexus and the Olive Tree: Understanding Globalization*, Farrar, Straus, and Giroux, 2000.

Matt Bishop *is a professor of computer science at the University of California, Davis. His research interests include vulnerability analysis and denial-of-service problems, formal modeling (especially of access controls and the Take-Grant Protection Model), and intrusion detection and response. Bishop received a PhD in computer science from Purdue University. He is a charter member of the Colloquium for Information Systems Security Education and author of* Computer Security: Art and Science *(Addison-Wesley, 2002). Contact him at bishop@cs.ucdavis.edu.*

Deborah Frincke *is chief scientist of the CyberSecurity group of the Pacific Northwest National Laboratory. Her research interests include security of high-speed systems and system defense, especially intrusion detection. Frincke received a PhD in computer science from the University of California, Davis. She is currently on leave from the University of Idaho, where she is a professor and was director of the Center for Secure and Dependable Systems. She is also a charter member of the Colloquium for Information Systems Security Education. Contact her at deborah.frincke@pnl.gov.*