Education in Information Security

Matt Bishop

Department of Computer Science
University of California, Davis
One Shields Ave.
Davis, CA 95616-8562

email: bishop@cs.ucdavis.edu

Introduction

The last four years have seen an explosion in the concern for the security of information. People are becoming aware of how much information is publicly available, as stories in the national news media discuss the ease with which identities are stolen. On a less personal note, compromises of information involving people authorized to access that information show that organizations have problems in securing information. With this awareness has grown an understanding of our dependence on accurate, confidential information, as well as the fragility of the infrastructure we use to secure that information. Of all the questions emerging, the fundamental one is: how can we secure information? This essay discusses different forms of education relevant to the problem.

What "Information Security Education" Is

The most basic form of education is public awareness. Does the public understand there is a problem? How can we communicate the depth of the problem effectively? The public does not want to know details or technologies. The public wants to know how to keep private information private, from government entities as well as commercial and academic ones. So education at this level is primarily procedural, and should focus on making the public aware of the threats and of what individuals can do to protect themselves.

As an example, many people are connecting to the Internet using DSL, the Digital Subscriber Line technology. The marketing literature touts the benefits of speed and lack of busy signals when connecting to the Internet. The obvious conclusion, one that the members of the public do *not* make, is that DSL connects you to the Internet at all times except when your modem (or system) is turned off. This broadens the interval in which attackers can probe your machine, and increases your exposure to attack.These risks can be ameliorated somewhat by the simple precaution of turning your modem off when not connected to the Internet. The public needs to learn the latter; the reason is not important (unless someone asks, in which case it should *always* be explained, by the principle of open design [6]).

Academic education is deeper. The dictionary [7] defines "academia" as a Latin word meaning "academy." An "academy" is:

- An institution of higher learning; or
- A private secondary or high school; or
- A school for teaching a particular art or particular sciences

These definitions identify several types of education as being "academic." The types, broadly stated, are training, undergraduate education, terminal master's education, and doctoral education. The differences between these types of education are illuminating.

Training focuses on particular systems, situations, or both. How do you configure a Windows 2000 computer to be a WWW server in a DMZ separating the protected internal network from the Internet? What happens if you don't use those specific settings, and what does each setting do? Whom do you call if you are a security guard who spots the director of the CIA carrying classified material out of the building? How do you send medical records to a doctor without compromising either the confidentiality or the integrity of those records? The answers to these questions are embodied in procedures and technologies. One need not understand why these procedures are in place, or how the technologies work, in order to use them effectively. (Obviously, the more understanding the trainee has, the better he or she will handle the job. But the understanding is not needed to perform the required tasks; knowing *how* is.)

Trade organizations, professional and commercial groups provide this type of training in tutorials. These tutorials are typically intensive, may be hands-on, and have as their goal that the attendees can walk out of the tutorial and apply what they learned. One residual value of these tutorials is having the book of slides and other materials. Often too much is covered to be retained perfectly. But attendees see something, and may remember they have seen it without recalling the details. They can then review the tutorial material and refresh their memories.

One can also acquire this training on the job, provided one is willing to ask questions and is paired with a mentor who is willing to answer them, and show the trainee how the systems are configured and how to reconfigure them. Although usually slow, this technique is effective because it teaches the trainee the problems that the particular site, or system, has, and how to cope with them, rather than the more general knowledge acquired in a tutorial attended by 150 or so people. When combined with a more general tutorial, this training is particularly effective.

The goal of undergraduate education is to learn broad principles, and see how to apply them. Undergraduate education does not focus on any particular situation or system. In practice, the best instructors take case studies and generalize them to exhibit the underlying principles. This helps students acquire a sense of what is principle and what is detail, and how to differentiate them. Subsequent exercises emphasize these principles, and have the students apply the principles in different ways. Throughout, the emphasis is on *what* principles are important, and *how* to apply them.

The advantage of a good undergraduate education is the breadth of application of principles taught. For example, in computer science, classes in algorithms, databases, operating systems, programming languages, architecture, and information systems teach various principles of information security, and how to apply them in the given realm. Political science and history classes teach principles of information security in studies of government and political movements, such as discussed in Sun Tzu's *The Art of War* and Saul Alinsky's *Rules for Radicals*. Literature classes sometimes discuss those principles as they study stories such as "The Purloined Letter" and *Oliver Twist*. The idea that knowledge may come from disciplines other than those naturally allied with information security testifies to the importance of those ideas.

As an example, consider one of Alinsky's rules about tactics for organizers:

> The third rule is; *Whenever possible go outside of the experience of the enemy.* Here you want to cause confusion, fear, and retreat.
>
> General William T. Sherman, whose name still causes a frenzied reaction throughout the South, provided a classic example of going outside the enemy's experience. Until Sherman, military tactics and strategies were based on standard patterns. All armies had fronts, rears, flanks, lines of communication, and lines of supply. Military campaigns were aimed at such standard objectives as rolling up the flanks of the enemy army or cutting the lines of supply or lines of communication, or moving around to attack from the rear. When Sherman cut loose on his famous March to the Sea, he had no front or rear lines of supplies or any other lines. He was on the loose and living on the land. The South, confronted with this new form of military invasion, reacted with confusion, panic, terror, and collapse. Sherman swept on to inevitable victory. It was the same tactic that, years later in the early days of World War II, the Nazi Panzer tank divisions emulated in their far-flung sweeps into enemy territory, as did our own General Patton with the American Third Armored Division. ([1] pp. 127–128)

The relevance to information security is obvious. From the attacker's point of view, look for unexpected openings. Look at the models the defenders have used to secure their information. Find ways to sidestep the mechanisms that the model requires, or—better—invalidate the assumptions that the model makes. Dorothy Denning very eloquently made this point in her National Computer Systems Security Award acceptance speech [4], in which she describes several incidents in which supposedly secure mechanisms were breached by people who went outside the conventional modes of analysis and found forms of attack that the models did not consider. Denning's talk, incidentally, emphasizes the lesson of the Alinsky passage for defenders: expect to be attacked in ways you cannot anticipate, and be prepared for it.

Masters' level education builds on undergraduate education. It requires the student to examine a particular area of the discipline in depth either through additional course work and examinations, or through course work and projects culminating in a master's thesis. Such a thesis typically develops an application of a principle to a specific situation or set of situations, Masters' level education enables one to weigh competing interests and determine how best to apply different technologies to reach the desired balance.

Some examples of typical masters' level work are analyzing a particular network security protocol to determine if it has flaws, and suggesting changes to ameliorate the flaws; designing and implementing a library of specifications for security properties that are to be used with a testing tool; and developing a policy model for an academic institution. The first applies analytic and experimental techniques to a protocol to determine if it works correctly in the Internet. The second uncovers common flaws in programs and show how to abstract from them a description sufficient to identify previously unknown instances of the problems. The third combines technology with an analysis of the needs of the differing organizations making up an academic community, and presents mechanisms to enable the disparate groups to work together.

People with this kind of experience know how to weigh the conflicting needs of policy requirements, capabilities of technology, and human factors. They can analyze problems, look for solutions, and bring the two together. Sometimes no solutions are possible. This leads to approximations, and a good analyst can determine what the potential problems with the approximation are. In any case, these people can bring their experience in technology, principles, and

analysis together to formulate guidelines that describe the needed protection. They then can design mechanisms to provide that protection.

Graduate education at the doctoral level also builds on the undergraduate education. Unlike a masters' education, doctoral level work analyzes the principles, extends the principles, changes them, improves them, or derives new principles. The goal is to deepen the student's understanding of systems in such a way as to enable that student to add to the body of knowledge. From this are gleaned fundamental views of how to improve the state of the art and science of information security, and indeed what is, and is not, possible.

The difference between doctoral level work and masters level work lies in the nature of the concepts studied. Masters' level work typically emphasizes applications or applied research in some form. Doctoral level work emphasizes fundamental results and research, often called "basic research." Doctoral work pushes the boundaries of knowledge. The results may not be applicable immediately, or even in the short or medium term. But they help us better understand the technology, its limits, and its uses, and for that reason is critical.

Doctoral study also provides the credentials needed to be hired by a research university: testament to the ability of the student to perform original, significant research. At research universities, teaching is not only a classroom exercise. Professors work with students in their research. Students learn how to conduct research, how to ask meaningful questions, and how to design experiments to demonstrate problems and solutions. In addition, students acquire an understanding of how to abstract problems into mathematical realms where they can be analyzed formally. They also learn how to relate the formalism back to the problem to use whatever light their abstract analysis sheds on the problem.

The notion of "academic education" covers all of these forms: training, undergraduate education, masters' education, and doctoral education. It is imperative to understand that there is no hierarchy of importance or merit; someone with a doctorate is not better educated for a particular problem than someone with training to handle that problem. But someone with a doctorate can analyze that problem, abstract the problem, work with the abstraction, and suggest potential lines of research to eliminate the problem, and ones similar to it. People with Ph.D.s tend to generalize and try to solve classes of problems; people with training tend to focus on the particular problem at hand. Neither is "better;" they are different.

Compare and Contrast

Academics emphasize the principles underlying computer security. These range from the theoretical (such as the HRU result stating that, in the most general case, security is undecidable [5]) to the applied (such as Saltzer's and Schroeder's Design Principles for security mechanisms; see sidebar). The goal is to be able to apply those principles to situations; in other words, to practice the science, and art, of computer security.

Good instructors use exercises to drive the ubiquity of these principles into the students. This type of teaching requires equipment and software that reflects the principles being taught, or to which the students can apply the principles and achieve an improvement, or visible alteration, to the system being modified. The students then see that they understand the principles well enough to apply them.

Industry needs to protect its investments in people, equipment, and its intangibles – bank balances, availability of services, proprietary information, *etc*. The security mechanisms must do this effectively. The principles they embody are less important.

In this realm, computer security is applied and practical. The goal of this type of computer security education is to be able to analyze a site, balance (internal and external) threats to the company with costs of implementing security measures, and achieving a balance between the two, with a minimum cost in training to the company. Understanding principles helps develop and implement policies and mechanisms, but the results are what matter.

Government uses computer security as one of many tools to protect the national interest (we assume this is well defined). The threats arise from external attackers and from government employees who act against the best interests of the citizenry or who abuse their authority. The specific protections are legally mandated, and not subject to the same cost-benefit analysis industry can afford. Hence computer security education focuses on developing policies and systems to implement laws and regulations, and less on cost balancing.

This points out the need for education at many levels. Each level has something to contribute. Most importantly, people at each level help educate each other. For this reason, all levels must be supported, and must play a part in protecting information.

The State of Information Security Education

There is interest, and discussion, on improving the state of information system security education. The desired improvements include establishing core curricula and integrating computer security into more aspects of computer science education. Specifically, the program establishing Centers of Academic Excellence in Information Assurance Education has as one evaluation criterion that "the academic program demonstrates [information security] is not treated as a separate discipline, but as a multidisciplinary science with the body of [information assurance] knowledge incorporated into various disciplines" [3]). This program recognizes institutions that are teaching students about information security, even when the student's primary interest is not information security. The NSA's recognition of these Centers of Excellence is a first step.

It is, however, only a first step. The designation involved no support and no benefits other than being able to say that the institution was a Center of Excellence designated by the National Security Agency. To be fair, the NSA has always said that this is the only reward, but they hoped that the "Centers for Academic Excellence may become focal points for recruiting and may create a climate to encourage independent research in Information Assurance." Perhaps that will happen soon.

Problems of the past continue to recur in the present. The ILOVEYOU worm is a perfect example. In 1988, before the Internet virus appeared, the CHRISTMA EXEC worm threaded its way through several IBM networks. People received a letter telling them to save the body of the letter as a file, and then execute the file, to get a pleasant Christmas greeting. When they did this, they saw a Christmas tree with blinking lights drawn on their screens. What they did not see was the rest of the program. It then looked in the NAMES and NETLOG files to get names of other correspondents, to whom it would forward itself. The resulting E-mail storm made several IBM networks unusable until the worm was cleaned out. The ILOVEYOU worm used almost exactly the same techniques. The only differences were that the recipient had to click on a button, rather than

save the file and execute it, and the ILOVEYOU worm downloaded a second program which harvested passwords from the Windows system's cache. These are reasonable updates given the changes in our world over the previous 11 years.

In other communities, software still suffers from buffer overflows. Privileges are not constrained properly. Race conditions allow unscrupulous users to acquire control of systems. There is nothing new under the sun. What has happened before will happen again, and we are not learning these mistakes.

Nor have we improved how we design systems and programs to account for security problems. Consider Windows 2000. Microsoft's security mechanisms, in concept, are excellent. But their implementation and integration into the system seem to lack coherency and cohesiveness. Further, some subsystems have design problems and implementation problems. Microsoft has released several patches for both systems and application software, and still has numerous security-related issues pending. Similar criticisms hold for all varieties of UNIX, or UNIX-like, systems. The problem is that we do not design with security as an integral part of the design. We patch. We add security above the kernel, or retrofit it. This causes problems.

Conclusion

All forms of education, from basic research to training, are critical to responding effectively to the information security crisis we face now. In addition to focusing our efforts on training, efforts must focus on basic research and higher education. The latter two will provide the teachers and researchers needed to train system administrators, business executives, and management in the intricacies of information security that affect them and their organizations. Further, the emphasis on basic research will lead to more research faculty in the area of information security, thereby seeding more universities and academic institutions with people who can teach and do research in that area.

Throughout this, we cannot forget the dreamers, the people with long-range vision. Most education focuses on short-range or medium-range planning. While important, it cannot pre-empt the long term planning. Technologies will change; systems will become obsolete; the infrastructure will evolve in unanticipated ways. The dreamers will provide the vision. Ted Nelson conceived of hypertext in the mid-1970s as he studied how computers and books would work together; can anyone imaging the World Wide Web without clickable links, or—more properly—hypertext? Nelson was a dreamer, but he had a technologically sound vision. People like Nelson guide the way. Focusing on the immediate, and near-term, present runs the risk of creating people like General Carpenter in Alfred Bester's story "Disappearing Act."

In that story, America is involved in a war, and has become a nation of experts. "Every man and woman must be a specific tool for a specific job, hardened and sharpened by your training and education to win the fight for the American Dream." But wounds have caused some injured soldiers in a hospital to vanish and reappear at will. Investigation convinces the general that the casualties are going back into time, and he asks a historian (who is released from his prison sentence for questioning the war) to see how they do it. The historian quickly realizes that the casualties are travelling elsewhere, "back into a time of their own imagination." He continues:

> "The concept is almost beyond understanding. These people have discovered how to turn dreams into reality. They know how to enter their dream realities. They can stay there, live

there, perhaps forever. My God, Carpenter, *this* is your American dream. It's miracle working, immortality, Godlike creation, mind over matter ... It must be explored. It must be studied. it must be given to the world."

"Can you do it, Scrim?"

"No, I cannot. I'm an historian. I'm non-creative, so it's beyond me. You need a poet ..."

...

Carpenter snapped up his intercom. "Send me a poet," he said.

He waited and waited ... and waited ... while America sorted through its two hundred and ninety millions of hardened and sharpened experts, its specialized tools to defend the American Dream of Beauty and Poetry and the Better Things in Life. He waited for them to find a poet, not understanding the endless delay, the fruitless search; not understanding why Bradley Scrim laughed and laughed and laughed at this final, fatal disappearance. [2]

The worst catastrophe is to have a "cyberspace" of hardened, sharpened tools trained and educated for a specific job, and no-one who knows how to ask if there is another approach to the task, or how to look for it.

References

1. S. Alinsky, *Rules for Radicals*, Random House, Inc., New York, NY (1972).
2. A. Bester, "Disappearing Act" (1953); in *Virtual Unrealities: The Short Fiction of Alfred Bester*, Vintage Books (New York, NY (1997)
3. *Centers of Academic Excellence in Information Assurance Education (Graduate and Undergraduate Levels): Criteria for Measurement* (Oct. 1999).
4. D. Denning, "The Limits of Formal Security Models," National Computer Systems Security Award Acceptance Speech, http://www.cs.georgetown.edu/~denning/infosec/award.html (Oct. 1999)
5. M. Harrison, W. Ruzzo, and J. Ullman, "Protection in Operating Systems," *Communications of the ACM* **19**(8) pp. 461-471 (Aug. 1976).
6. J Saltzer, and M. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE*, **63**(9) pp. 1278-1308 (1975).
7. *Webster's New Twentieth Century Dictionary*, Second Edition, Simon and Schuster, New York, NY (1979).

Sidebar

Saltzer's and Schroeder's principles of secure design [6] are fundamental to any security system or mechanism. They are:

- The *principle of least privilege* says that a process should have only those right necessary to complete the task. In government and industry, this is the "need to know" principle.

- The *principle of fail-safe defaults* says that when a security mechanism or system fails, the system should revert to a known, secure state. This essentially says to deny access to sensitive information unless access is explicitly granted, again a standard when dealing with sensitive information.
- The *principle of economy of mechanism* says that security mechanisms and procedures should be as simple as possible, because as system and mechanism become more complex, more can go wrong. Further, the more complicated a mechanism, the harder it is to convince people that the mechanism works as needed. This is a general rule, born from human nature and experience. Arthur C. Clarke's marvelous short story "Superiority" casts this in terms of science fiction, in which the desire to develop complex, powerful weapons leads to defeat at the hands of simpler, less powerful, but functional weapons.
- The *principle of complete mediation* means the mechanism cannot be evaded. Denning made the importance of this principle explicit in her talk before the National Information Systems Security Conference. She pointed out that attackers often evade controls designed to stop them. The controls are never invoked, so they are completely ineffective.
- The *principle of separation of privilege* says that multiple properties must hold for access to be granted. In financial circles, this is called "separation of duty." Two people must sign checks over $10,000. Two soldier must insert keys to launch missiles. One person is easier to compromise than two who must work in concert. Again, mathematically this is a fallacy, but humans are not mathematical.
- The *principle of open design* says that the security of a system should not be based upon hiding the details of how the system functions. Hiding specific information such as passwords does not violate this principle, but hiding the general design of a security policy or system does. Attackers can construct the details of systems in a variety of ways. For security procedures, dumpster diving is effective. In 1972, Woodward and Bernstein determined the lines of reporting in the highly secretive Committee to Re-Elect the President by examining telephone numbers and seeing who had phone numbers "close" to whom.
- Finally, the *principle of psychological acceptability* says that security procedures and mechanisms must be as easy to use as ignore. This principle is usually watered down to say that using the security mechanisms must not be too onerous. Passwords and badges are generally acceptable. In high-security institutions, fingerprints provide a high degree of authentication. But requiring fingerprints for authentication to enter a university laboratory would be unacceptable, at least at the University of California. The students, staff, and faculty would simply refuse to tolerate it.

Sidebar: Example Curricula

The following are outlines of topics discussed in the general computer security classes at the University of California at Davis. Special topics courses cover specific material in more depth.

The undergraduate class (ECS 153) focuses on applications of the principles of computer security. It emphasizes how to protect systems, and discusses some broader principles and models. The main focus is on how to apply the models.

- Introduction and what computer security is, basic principles; ethics
- Models: confidentiality, integrity (Bell-LaPadula, Biba, Clark-Wilson, Chinese Wall)

- Assurance: robust programming, security in programming, specification, design, testing, proving programs correct
- Cryptography: basics, authentication, key management, example protocols
- Mechanisms: identity, access control lists, capabilities
- Attacking and defending: models of vulnerabilities, penetration testing, malicious logic

The graduate class (ECS 253) focuses on the theory of the principles of computer security. It covers theoretical foundations as well as much deeper analyses of models. Many of the topics in ECS 153 are covered, but with an emphasis on theory as opposed to application.

- Introduction and what computer security is, basic principles; ethics
- Foundations: access control matrix model, HRU result, Take-Grant Protection Model, undecidability results
- Cryptography: key management, cipher techniques, example protocols
- Models: confidentiality, integrity (Bell-LaPadula, Biba, Clark-Wilson, Chinese Wall), noninterference and non-deducibility security, information flow models
- Assurance: building secure systems, specification, design, testing, proving programs correct
- Mechanisms: identity, ACLs, C-Lists, ring-based protection, PACLs, confinement problem, information flow models
- Attacking and defending: models of vulnerabilities, penetration testing, malicious logic, auditing, intrusion detection