

Teaching Computer Security Concepts - Let's Get Physical!

***Abstract*—Information security is a critical topic for computer science students to understand. Different teaching approaches can be effective in helping the students understand abstract principles. This paper explores the idea of solving common physical problems as a vehicle for discussing and understanding security concepts. Our experience with a version of this approach is described in detail.**

***Index Terms*—information security education**

I. INTRODUCTION

Information security is an important educational topic that is receiving a lot of attention in recent years. Part of this emphasis is a result of greater public awareness due to highly publicized computer attacks in the media. The oft-quoted dangers of identity theft and daily doses of compromised privacy information fuel this sense of urgency in protecting our systems and information. The United States government contributes to the prominence of information security as a hot topic. The President's Information Technology Advisory Committee reports the information technology infrastructure of the United States is highly vulnerable to premeditated attacks and is a prime target for cyber terrorism [1]. A key priority in the National Strategy to Secure Cyberspace is to increase security training and awareness through enhanced education programs [2]. To encourage security education, increase research, and produce a growing number of information assurance professionals, the National Security Agency in conjunction with the Department for Homeland Security created and administers the Centers of Academic Excellence (CAE) in Information Assurance Education Program [3]. Schools with the CAE designation must meet strict guidelines in educational and research excellence. Security as a topic in computer science education is now listed in the ACM Computing Curricula 2005 as an emphasis area along with more traditional computing concepts [4].

As a result of this emphasis in information security in education, much has been published on how to

effectively integrate security into existing curricula [5,6], how to set up new programs and concentrations in information security [7,8,9], and successful classroom and laboratory experiences in teaching specific security topics [10,11,12]. Additionally, a number of organizations, workshops, and conferences (such as ACEIS) have been created to provide a forum for promoting information security in higher education and exchanging ideas and techniques. A direct result of these efforts is that there is a great deal of reference material and resources available for teaching computer security concepts: textbooks, student competitions, exercise ideas, interactive visualizations, laboratory experiences, etc.

Different institutions have taken different approaches to teaching computer security topics. While many of the topics lend themselves to a traditional lecture approach, several programs have espoused a hands-on approach. This includes the development of exercises and use of existing hardware and software tools for monitoring, analyzing, and (possibly) compromising security. The issue of whether or not to teach compromising techniques has led to discussions of classroom ethics and educating students about professional responsibility [13]. The use of a hands-on approach may also necessitate (for the administration's comfort) providing an isolated or secure network laboratory [14]. A related approach to hands-on is the use of student competitions to generate interest and student motivation [15]. Local, regional, and now national "cyber exercises" raise the visibility of security education. Another approach to teaching security topics is "scenario-based" and places the student in simulated exercises in which they have to handle security occurrences as they arise [16].

At our institution, information security has been an integral part of our computer science curriculum for over a decade. We have taught security topics in several of our standard computer science courses, and have created specific courses in cryptography, information warfare, and network security. Our motivation has been both the increased security emphasis within general computer science education, as well as preparing our students for their future role in protecting the nation. The computer science program offers a concentration in information

assurance, and our institution has been designated as a CAE in information assurance education.

II. RELATING SECURITY CONCEPTS TO PHYSICAL SECURITY

A common approach when teaching computer security concepts is to relate them to some type of physical security issue that students are familiar with. While physical security itself is a viable topic for information assurance, the idea here is to use physical security as a metaphor for more abstract concepts. For example, the utilization of a safe to protect valuables can be used to demonstrate concepts such as passwords (the combination), security logs (keeping a record of safe contents and who adds/removes things), and risk assessment (measuring the strength of the safe and the amount of effort to crack it). One can think of several examples such as keys to a house, making a cash or credit purchase, physical alarm systems, and eavesdropping on phone calls. Such physical examples are a natural part of explaining security topics and occur often in lectures and reading material.

An variation of using physical security to demonstrate more abstract security concepts is to start with a common physical problem, allow the students to struggle with, analyze, and attempt to solve it, and then relate their experience back to the computer security realm. Ideally, the physical problem is a common one that they are familiar with, so little or no background is necessary for them to explore possible solutions. For example, having them analyze the weaknesses in a sophisticated physical alarm system would require too much background work to understand the system and be counter to the idea of keeping it simple. The problem should also be something that they can physically work with, and not simply consist of a mental exercise. The following are some examples of simple physical problems that could be used for this approach.

A. Locked Out

An experience that almost everyone has had in one situation or another is to be accidentally locked out of a space. Leaving keys in a locked car, losing or forgetting a house key, or needing access to a room that you don't have the key for is familiar to all. A passive approach to using this analogy is to have students describe an experience, how they solved it, and discuss other options they could have used. Many solutions can be directly related to security concepts. Finding an open entry (backdoor), breaking a window or shimmying a lock

(hacking), and getting a key from someone in authority (trusted third party) are all examples of security analogies that can be made. A more active approach which may or may not be practical would be to actually provide students with a locked room such as a classroom or lab space that they need to get into (legitimately). Certain restrictions and/or coordination would be necessary to assure protection of property, avoidance of local security violations, and possibly ensuring personal safety. The advantage of an active approach is that students are all confronted with the same scenario and can work as a team to brainstorm creative ideas to solve the problem. The instructor should decide ahead of time how far they want to let the students go in their quest. After the experience, a full discussion with security analogies can be conducted.

B. Puzzle Solving

A perhaps more manageable physical problem to solve would be the use of puzzles in the classroom. Many topics in cryptography can be illustrated with approaches to solving common "brainteasers". For example, the daily *Cryptoquote* in the paper is a substitution cipher that students are familiar with. As an out-of-class exercise, students can be given puzzles to solve. Rather than simply coming up with the answer, students should be encouraged to write down their approach to the problem and describe how their methodology could be translated into an algorithmic solution. Classroom discussion can focus on the effectiveness of the various approaches, ease of computer implementation, relative security of this encryption technique, and possible variations to make it more secure. Another example of a common puzzle to solve is the "hidden picture in the picture" which can easily be related to steganography. The literature is ripe with examples of historical uses of steganography such as the slave quilts from the civil war [17].

C. Game Collusion

Another physical problem approach which we have used successfully is to set up collusion between some number of players in a game and challenge the students to detect it. For example, two players want to help each other out in a poker match. They can do so by communicating surreptitiously (covert channel) or by finding a way to share their cards. They must do so in a way that is transparent to the other players and observers in the game who are trying to detect any collusion. One or more colluding pairs can be prearranged and kept secret so that the players do not know who they are. The colluding players work together ahead of time to

coordinate their approach, and a game is played. All of the students try and identify who the colluders are (if any) and how they are collaborating. Obvious clumsy approaches such as trying to pass cards are most likely quickly identified. More subtle approaches such as using body language and bidding sequences to communicate information have a greater chance of going undetected. Discussion after the game can focus on several aspects such as how easy or hard the collusion was to detect, the effectiveness of the technique, how it might be improved, what the expected payoff is, and a risk assessment of how likely such an approach might be versus the cost of being detected. Several direct comparisons to information security in network communication can be made with the emphasis on covert channel detection. More exotic approaches such as tampering with the deck and the use of sophisticated communication technology (ala Mission Impossible) can be brainstormed as part of a discussion on cost/benefit tradeoff. The obvious ethical issues should also be part of any security discussion. A simplified version of this approach is a variation of Johnny Carson's *Mighty Karnak*, in which the audience agrees on a secret number while Karnak is out of the room. Upon reentering and with the appropriate theatrics, he is able to magically "guess" the number through a prearranged covert channel with a shill in the audience. We have successfully done this much to the entertainment of our students.

III. SECURITY OF THE COMMON COMBINATION PADLOCK

The Computer Security and Information Warfare class at our institution has been taught for over a decade. Through that experience, the course has continually evolved using some of the aforementioned techniques to try to instill the more abstract security design concepts. Concepts such as the need for rigor, the methodical measurement and assessment of a proposed configuration or design, the importance of raising the cost, in terms of resources, to the attacker and consideration of worst case scenarios for use in reduction arguments to raise assurance of a system are sometimes difficult to teach from passive strategies. In the Spring of 2006, the physical metaphor approach was tried in a new way.

A. *The Physical Problem*

Inspired by Matt Blaze's paper [18], the class was asked to research attacks on ordinary combination padlocks such as those protecting their personal items at

the gym. This is a common problem that all students were familiar with and several had faced at one time or another. Although physical locks were not passed out as part of the assignment this semester, it would have been a simple addition, and would have added elements of both entertainment and competition to the assignment. We plan to make this part of the exercise in future course offerings.

B. *Student Findings*

Based on the results of the student's research, classroom discussion focused on all discovered attacks on a padlock. In addition to the obvious solutions of using bolt cutters, "shoulder surfing", and trying all possible combinations, students found several other approaches. One of the surprising results to the students was how easy it is to figure out an unknown combination for several different common types of padlocks. The most popular attack for a common brand combination lock which was readily found on the internet reportedly allows a single attacker to determine the padlock combination in less than 100 guesses. Other attacks included the use of external physical devices such as shims, prying the lock apart, and variations on a "safe cracking" approach (turning the dial and paying attention to where it sticks).

C. *Relating it to Computer Security*

The student's findings led to a discussion about the extent of the threat this vulnerability poses to a variety of situations in which a padlock may be employed. In particular, the class discussed the notion of measuring the security they expected for protecting their gym clothes and personal valuables in a gym locker. Each known attack was listed along with an estimate on the cost of the attack in terms of time and resources. Resources included man-power and dollars. Also considered was the threat model. What type of individuals pose a real threat to those articles in the gym locker? What is their motivation? How much risk is the attacker willing to accept during the exploit?

In particular, many students expressed a positive attitude to this "new attack" because they felt they could now recover from the denial of service incurred from forgetting their combination. They would not necessarily have to just cut off the lock or buy a new one.

After discussions, the class decided that while the ease of determining the combination was surprising, few felt that their articles were less secure than previously

imagined. The main reason for this was the existence of other attacks that are much less costly in time, resources, and risk to the attacker than that attack. Bolt cutters and shoulder surfing being the most common types of attacks cited in this regard.

The class proceeded to contrast this assessment of security with that typical of security metrics in cryptography. Algorithms which are considered to be computationally secure lend themselves to very formal and rigorous arguments justifying that claim. Within cryptography a discussion about a specific threshold on the minimum amount of work required under a given threat model which defines a secure algorithm is not discussed. Primarily this is due to the fact that we are readily able to produce efficient and scalable algorithms allowing a much higher threshold to be set.

As Blaze points out, the physical security world does not appear to have the ability to create physical security mechanisms which would meet a strict definition of computationally or perfectly secure analogous to the cryptographic definitions. As discussed in that paper, the practicalities, economics, and threat models all combined into a design which in some sense is a justified best estimate sufficient protection.

However, the physical security realm, the computer security realm, and the cryptographic realm all share the common problem of trying to estimate the amount of time for which the system should be considered to be secure. This time estimate can only be based on estimates of growth in technology, historical evidence, and the best estimate of the current capabilities. Given the padlock experience, students seem to come to these conclusions independently and quickly.

All of these issues arise in the architectural considerations of security. Understanding the services, the criticality of the services provided, and the impact of the loss of those services rings true in the computer security arena as well. This metaphor also paves the ways for more discussion of when it is appropriate to require more formal analysis and how that impacts assurance. Topics such as protection profiles, the Common Criteria, policy authorship, and enforcement are more readily seen as necessary components to the primary technical solutions of the system.

The lesson also highlights the need to know when more details about a system are truly required in order to

make informed security decisions. Even configuration decisions can be simpler and more robust in some circumstances when more understanding of the functionality and architectural design of security details are known.

A final security discussion resulted from the ethical question of whether it was appropriate for Blaze to publish his paper in the first place. Was he encouraging people to break into safes and providing them with the means to do so? This led to a discussion of published versus private security methods, or so-called “security through obscurity”. Many historical examples offer good fodder for this discussion.

IV. CONCLUSION

The use of a physical problem as an exercise and metaphor for security concepts proved to be an effective means to motivate students and enliven classroom discussions. The students could easily understand the ideas of threat assessment, cost/benefit tradeoffs, and risk analysis as applied to their personal lives in this common example. Based on our positive experience, we are planning on investigating and trying other physical exercises to use in future course offerings.

As a closing note to this experience, one of our faculty members became motivated to further understand combination locks and attacks on them including their deconstruction to better understand the locking mechanisms. He was able to refine the attacks published online, and became quite adept at opening locks in a matter of minutes. In addition, he came up with an effective social engineering technique that worked directly with the lock manufacturer to receive the combination. However, in the latest demonstration of his newly found skills, he discovered that the lock manufacturer who was the subject of his studies was also apparently aware of their product’s weaknesses, and the newest version of their product on the market is significantly more secure against published attacks.

REFERENCES

- [1] Benioff, M., et al. 2005. Cyber Security: A Crisis of Prioritization. A Report to the President from the President’s Information Technology Advisory Committee, (Feb. 2005).
- [2] The National Strategy to Secure Cyberspace. 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf. (Feb. 2003).

- [3] The National Centers of Academic Excellence in Information Assurance Education Program. 2005. <http://www.nsa.gov/ia/academia/caeiae.cfm>.
- [4] ACM Curricula Recommendations. <http://www.acm.org/education/curricula.html>.
- [5] Petrova, K., Philpott, A., Kaskenpalo, P., and Buchan, J. 2004. Embedding information security curricula in existing programmes. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 20-29.
- [6] Vaughn, R. B., Dampier, D. A., and Warkentin, M. B. 2004. Building an information security education program. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 41-45.
- [7] Azadegan, S., Lavine, M., O'Leary, M., Wijesinha, A., and Zimand, M. 2003. An undergraduate track in computer security. In *Proceedings of the 8th Annual Conference on innovation and Technology in Computer Science Education* (Thessaloniki, Greece, June 30 - July 02, 2003). D. Finkel, Ed. ITiCSE '03. ACM Press, New York, NY, 207-210.
- [8] Bacon, T. and Tikekar, R. 2003. Experiences with developing a computer security information assurance curriculum. *J. Comput. Small Coll.* 18, 4 (Apr. 2003), 254-267.
- [9] Crowley, E. 2003. Information system security curricula development. In *Proceeding of the 4th Conference on information Technology Curriculum* (Lafayette, Indiana, USA, October 16 - 18, 2003). CITC4 '03. ACM Press, New York, NY, 249-255.
- [10] Mattord, H. J. and Whitman, M. E. 2004. Planning, building and operating the information security and assurance laboratory. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 8-14.
- [11] Schafer, J., Ragsdale, D. J., Surdu, J. R., and Carver, C. A. 2001. The IWAR range: a laboratory for undergraduate information assurance education. In *Proceedings of the Sixth Annual CCSC Northeastern Conference on the Journal of Computing in Small Colleges* (Middlebury, Vermont, United States). Consortium for Computing Sciences in Colleges. Consortium for Computing Sciences in Colleges, 223-232.
- [12] Walden, J. 2005. A real-time information warfare exercise on a virtual network. In *Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education* (St. Louis, Missouri, USA, February 23 - 27, 2005). SIGCSE '05. ACM Press, New York, NY, 86-90.
- [13] Harris, J. 2004. Maintaining ethical standards for a computer security curriculum. In *Proceedings of the 1st Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, October 08 - 08, 2004). InfoSecCD '04. ACM Press, New York, NY, 46-48.
- [14] Hill, J. M., Carver, C. A., Humphries, J. W., and Pooch, U. W. 2001. Using an isolated network laboratory to teach advanced networks and security. In *Proceedings of the Thirty-Second SIGCSE Technical Symposium on Computer Science Education* (Charlotte, North Carolina, United States). SIGCSE '01. ACM Press, New York, NY, 36-40.
- [15] Conklin, A. 2005. The use of a collegiate cyber defense competition in information security education. In *Proceedings of the 2nd Annual Conference on information Security Curriculum Development* (Kennesaw, Georgia, September 23 - 24, 2005). InfoSecCD '05. ACM Press, New York, NY, 16-18.
- [16] Irvine, C., Thompson, M. and Allen, K. 2005. CyberCIEGE: An extensible tool for information assurance education. In *Proceedings of the 9th Colloquium for Information Systems Security Education* (Atlanta, Georgia, June 6-9, 2005). pp. 130-138.
- [17] National Security Agency. Follow the drinking gourd. <http://www.nsa.gov/publications/publi00011.cfm>.
- [18] Blaze, M. 2004. Safecracking for the Computer Scientist. U. Penn CIS Department Technical Report. 7 December 2004.