Teaching Computer Security with a Hands-On Component

Narayan Murthy

Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

TEACHING COMPUTER SECURITY WITH A HANDS-ON COMPONENT

Narayan Murthy

Pace University, New York
nmurthy@pace.edu

Abstract

To address national needs for computer security education, many universities have incorporated computer and security courses into their undergraduate and graduate curricula. Our department has introduced computer security courses at both the undergraduate and the graduate level. This paper describes our approach, our experiences, and lessons learned in teaching a Computer Security Overview course.

There are two key elements in the course: Studying computer security topics from a current textbook and online and experimenting with security tools. While the textbook and online material expose students to current security topics, projects that involve experimenting with security tools motivate students to explore computer-security techniques, providing a framework for a better understanding of the security topics and strengthening students' ability to put what they learnt in the classroom into practice in their organizations tomorrow.

1 Introduction

We all have seen the dramatic development of new and improved technologies. In July 2010, Facebook reached over 500 million active users, there were 85,500 iPhone apps, and 2 billion downloads occurred. Fifty-six percent of Americans say that they have at some point used wireless devices such as laptops, cell phones, and game consoles for online access.

There has also been an increase in the number, and sophistication, of Internet threats being produced by cyber criminals. According to an Internet security software and service provider Trend Micro study on Threat Predictions for 2011, threat researchers have found that more than 80% of the top malware uses the web to arrive on users' systems, and every second, 3.5 new threats are released by cyber criminals [8]. The Verizon Business website gives an excellent list of recent data breach statistics [9].

The annual CSI/FBI computer crime and security survey has shown that information security has continuously been a top priority in many organizations. This trend brings a great demand for qualified Information Assurance (IA) professionals [4].

In the field of computer security, malicious actors seem to outsmart the good guys. The offenders always seem to be one step ahead of the defenders. We believe that students have to learn defensive techniques by learning how the offense works. Learning successful defensive techniques in sports means observing the offensive tactics of the opponent. On the same lines, students should first be made to appreciate hacking techniques before moving on to defensive roles.

Our Overview of Computer Security course has been developed with this philosophy in mind. The purpose of this paper is to provide our experience in designing information assurance courseware that combines theory with practice. Using well-designed hands-on laboratory exercises, we allow students to experience the technical details of what they have learned [3]. There are two key elements in the course: studying computer security topics from a current textbook and online and experimenting with security tools. In addition to learning pedagogies and theories from the textbook, the course will focus on the use of technology to help students gain insight into the usefulness of what they have learned from the textbook.

Each lesson includes both lecture and hands-on labs to reinforce concepts. Students practice their craft either on their own machines or on the university machines in a controlled real-world environment. The university security lab is a local area networked lab, which is an isolated environment without any connection to the outside world. This isolation enables us to provide an increased level of threat. Students conduct both defensive and offensive experiments in this lab.

Some people argue that labs are so much more engaging than reading and study that they tend to drive out the latter. Given that a course such as this one requires a huge amount of reading and understanding topics such as encryption algorithms, network protocols, software security, and so on, such people say that this course should be light on the labs and strong on essential theory.

We believe that this argument is valid for students with math and programming backgrounds. By definition, the course in question is open to non-computer science majors. We strongly believe that computer security is too important to make this program available only to computer science majors.

2 Our Institution

For more than 100 years, Pace University has been preparing students to become leaders in their fields by providing an education that combines exceptional academics with professional experience and the New York advantage. Pace has three campuses in New York City, Westchester, and White Plains. A private metropolitan university, Pace enrolls approximately 13,500 students in bachelor's, master's, and doctoral programs in the Dyson College of Arts and Sciences, Lienhard School of Nursing, Lubin School of Business, School of Education, Seidenberg School of Computer Science and Information Systems, and School of Law.

Pace University, through the efforts of the Seidenberg School, was redesignated a National Center of Academic Excellence in Information Assurance Education for the academic years between 2007 and 2012. The original designation was awarded in 2004. The National Centers of Academic Excellence in Information Assurance Education (CAEIAE) Program is an outreach program designed and operated by the National Security Agency (NSA) and the Department of Homeland Security (DHS) [5]. The goal of the program is to reduce vulnerability in our national information infrastructure by promoting higher education in information assurance (IA) and graduating a growing number of professionals with IA expertise in various disciplines.

To attain certification, an institution must demonstrate commitment to academic excellence in IA by meeting rigorous requirements in areas such as curriculum, faculty qualifications, research efforts, laboratory and library resources, and partnerships. Pace is currently one of only about 120 institutions nationwide to be recognized as a Center.

Students attending these designated schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

3 Our Programs

IA academic programs have faced several challenges recently. As a way to broaden the appeal of their graduates as well as expand the scope of their computing programs, many computing programs have either integrated the IA curriculum into existing information technology, information systems, or computer science programs or have at least designed a single course to cover IA topics [3]. However, educators have proposed changes in the IA curriculum to cover both technical and nontechnical aspects of information security in order to keep up with the fast-changing security requirements for the public, industry, and the government [3].

At the undergraduate level, our department offers an interdisciplinary minor in collaboration with the Department of Criminal Justice.

At the graduate level, we offer a concentration in information assurance in a master's in information systems program.

The programs are by design not programming focused (we don't offer a software security course) so that it is open to non-CS majors.

3.1 Undergraduate Minor: Information Assurance in the Criminal Justice System

This minor was developed in response to faculty in the Criminal Justice Department who maintained that their students would benefit from information security courses.

They might not necessarily plan to work as security professionals but need to deal with security problems in their own field.

The minor consists of the following six courses:

CRJ 150 Introduction to Criminal Justice
CRJ 247 Introduction to Private Security
CRJ 346 Terrorism and Society
IT 300 Computer Security Overview
IT 304 Network and Internet Security
IT 308 Computer Forensics

Of these six courses, the first three (with the CRJ prefix) are offered by the Criminal Justice Department, and the last three (with IT) are offered by the Computer Science Department.

All three IT courses are a combination of textbook study and hands-on lab work. The course this paper is discussing is IT 300.

3.2 Graduate Concentration: Security and Information Assurance

This is one of the concentrations available to students in the MS in Information Systems program. Here is a description of the concentration: As organizations become more aware of computer and information security requirements, there is a growing need for IT professionals who understand the technologies and concepts of information assurance, including encryption, threat analysis, access control, and social engineering.

Concentration courses:
IT 603 Overview of Information Security
IT 660 Network Security
IT 662 Web and Internet Security
IT 664 Computer and Internet Forensics
IT 666 Information Security Management
The course discussed in the paper is IT 603.

3.3 Topics in IT 603 Overview of Information Security

The textbook used is *Corporate Computer and Network Security* By Raymond R. Panko.

Topics covered (from the book) are Access Control and Site Security; Review of TCP/IP Internetworking; Attack Methods; Firewalls; Host Security; The Elements of Cryptography; Cryptographic Systems: SSL/TLS, VPNs, and Kerberos; Application Security: Electronic Commerce and E-mail; and Incident and Disaster Response.

3.4 Hands-on security experiments

For each of the hands-on experiments, the instructor provides a document with background material on the experiment to be done.

- **Steganography**

Students learn various steganography techniques, including the LSB method. They work on three careers (an image file, a sound file, and an HTML file) to retrieve hidden messages using a standard steganography tool.

- **Windows password hashes**

Students learn about the following topics: how Windows stores passwords—LAN Manager hash and NTLM hash; SAM file; and how password hacking programs work—dictionary method, brute force method, and hybrid method. Students use one of LC4, a combination of **Proactive System** and **ophcrack or LCP** by LCPSoft v5.04, to extract several passwords of various complexities (very simple to very complex).

- **MBSA**

Students learn to use Microsoft Baseline Security Analyzer (MBSA), an easy-to-use tool designed for the IT professional that helps small- and medium-sized businesses determine their security state in accordance with Microsoft security recommendations and offers specific remediation guidance. It is possible to improve the security management process by using MBSA to detect common security misconfigurations and missing security updates on computer systems. For the sake of experimenting, students introduce several loopholes and run MBSA. Students fix all the loopholes identified by MBSA and run MBSA again to make sure everything is fixed.

- **PGP**

Students learn about key ideas of encryption. They gain a detailed understanding of symmetric key encryption and public-key (asymmetric-key) encryption.

Students download and install PGP on their computers, generate a key pair, publish their public key on the PGP Global Directory, take the instructor's PGP public key from the PGP Global Directory, and create a small text file (making sure to include their full names in it). They save the file as their last name, encrypt the file using instructor's public key, and submit the encrypted file as an email attachment.

- **Nessus**

Nessus is a free (distributed by GNU), powerful, and easy-to-use remote security scanner developed and maintained by Tenable Network Security. Nessus is a vulnerability scanner that scans a target network to seek vulnerabilities in the network such as software bugs, backdoors, and so forth. The program is developed by Renaud Deraison. This is a very useful tool for network and system administrators to identify problems and security loopholes in their systems.

Students install Nessus and experiment with it. They run Nessus against any server and generate a report.

- **Nikto**

Nikto is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 3,200 potentially dangerous files/CGIs, versions on over 625 servers, and version-specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated if desired (see http://www.cirt.net/code/nikto.shtml).

Students install Nikto, run it against a server, and submit a report of vulnerabilities on the server.

- **Web: Security, Cookies and History**

Students learn about web insecurity on various levels, addressing digital certificates, browsers' encryption strength, application security, cookies, index.dat file, and browser history. Web Historian is a program that is used to analyze browser history. Students download and install Web Historian and analyze browser history.

- **Phishing**

Students learn about identity theft and phishing. They see several examples of phishing emails. They learn to analyze phishing emails. They also learn email spoofing using port 25.

4 Conclusion

We administer course evaluations by students at the end of the semester. Judging from these evaluations, it is clear that the students enjoyed the hands-on component of the course.

The following is a sample of comments by students on the evaluation forms:
"The weekly lab assignments were extremely relevant and current. I learned a great deal by working through the labs."
"The lab assignments were great. Learned new techniques."
"Lab assignments gave exposure to the tools used to scan for vulnerabilities."
"The lab assignments helped to understand the material better."

Most valuable: "… having us work hands-on with different software."
Most valuable: "Lab assignments."
"The labs made me understand the material."
"All lab assignments were very helpful to understand the objective of this course."
Most valuable: "The hands on projects."

I believe that the hands-on component helped students appreciate and understand computer security.

References:

1. Boleng, Jeff, and Dino Schweitzer. "A Hands-on Approach to Information Operations Education and Training." *14th Colloquium for Information Systems Security Education*. Baltimore, MD. 7-9 June 2010.
2. Centers of Academic Excellence—Institutions. National Security Agency, http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml. (3 Feb. 2011.)
3. Chen, Li-Chiou, and Chienting Lin. "Combining Theory with Practice in Information Security Education." *11th Colloquium for Information Systems Security Education, Boston University*. Boston, MA. 4-7 June 2007.
4. Lin, Chienting, and Li-Chiou Chen. "Development of an Interdisciplinary Information Technology Auditing Program." *13th Colloquium for Information Systems Security Education*. Seattle, WA. 1-3 June 2009.
5. *National Centers of Academic Excellence*. National Security Agency, http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml. (3 Feb. 2011).
6. Riabov, Vladimir V., and Bryan J. Higgs. "Running a Computer Security Course: Challenges, Tools and Projects." *River Academic Journal* 6.1 (2010).
7. Sharma, Sushil K., and Joshua Sefchek. "Teaching Information Systems Security Courses: A Hands-On Approach." *Computers & Security* 26 (2007): 290-99.
8. *Trend Micro Threat Predictions for 2011*. http://affinitypartner.trendmicro.com/announcements/trend-micro-threat-predictions-for-2011.aspx (3 Feb. 2011).
9. Verizon Business. *Anatomy of a Data Breach*, http://www.govinfosecurity.com/external/rp_2009-data-breach-investigations-supplemental-report_en_xg.pdf (3 Feb. 2011).