AC 2008-1228: TEACHING A COMPUTER SECURITY COURSE FOR COMPUTER ENGINEERING AND ELECTRICAL ENGINEERING TECHNOLOGY PROGRAMS

Xuefu Zhou, University of Cincinnati

Xuefu Zhou is an Assistant Professor of Electrical and Computer Engineering Technology at the University of Cincinnati. He received both his M.S. and Ph.D. degrees in Electrical Engineering from the University of Cincinnati in 2002 and 2006, respectively. His research interests lie on wireless communications, wireless and mobile networks, wireless network security. He is a member of IEEE and ASEE.

Teaching a Computer Security Course For Computer Engineering and Electrical Engineering Technology Programs

Abstract

During the past decade, computers and networks, particularly the Internet and wireless technologies, have become an integral part of our lives. With the explosive growth of computer systems and Internet applications, there has been a steady rise in occurrence of security attacks which resulted in significant attentions on computer security and the imperative need for its education and training. A computer security course usually has been considered as an abstract academic discipline in most of science and engineering programs, and thus it is still not commonly offered in related engineering technology programs, i.e. computer engineering and electrical engineering technologies. Since security defense occurs at different levels, from personal level to corporate and national levels, it will be imperative to teach the EET/CET students the knowledge and skills of computer security and prepare them for the future jobs since most of them are working in the industry to develop, to maintain and operate the computers and networks. This paper describes such a course developed for EET/CET programs including the objectives, course content and lab exercises.

1. Introduction

The explosive growth of computer systems and Internet applications has increased our dependence on the information stored and its transmission. Computer system security is more than 30 years old. Despite its many intellectual successes, the large amount of deployed computer systems, networks, and smart devices together with the Internet has made computer security defense more difficult than before. In addition to its technical difficulty, the unmatched awareness of security defense by most of the computer users cause flaws in the computer systems. According to the annual survey (2007) [1] conducted by America's Computer Security Institute (CSI), the estimated average loss has nearly doubled to $350k per organization per annum; financial frauds caused the greatest financial losses and 29% of organizations reported security incidents to law enforcement. This survey also indicates training individuals with responsibility for sensitive enterprise databases is clearly part of the security agenda. However, The survey found that almost half (48%) of the organizations spend less than one percent of their security dollars on awareness programs. Meanwhile, the National Strategy to Secure Cyberspace considered the security awareness as one of the key priorities. Since most of the graduates from EET and CET programs are going to practice in the industry to develop computers, to maintain and operate computer systems and networks, it will be extremely important to help them understand the fundamental concepts of computer security. This will be immediately beneficial to themselves and their employers as well.

Although courses on computer security (or network security, for the brevity purpose, the computer security term used here include the topics related to network security as well) have been well developed in most Computer Science or Engineering programs, they are not commonly offered in Electrical and Computer Engineering Technology (ECET) programs

because of the following reasons. First, most of the science and engineering program courses on security focus primarily on engineering topic with in-depth discussion on mathematics, algorithms, data structure and protocols, which apparently does not work for the engineering technology programs. Second, as engineering technology programs emphasize hands-on experience and practicing skills, to define the right balance between the necessary theoretical concepts and practical applications is a challenge. Third, the breadth of practical applications, attacks and tools often presents the other significant challenge to students and the teaching of these courses.

Despite these difficulties and limitations in the current computer security education, our observation of the importance of computer security in the real world, and the local industrial demand convinced us to incorporate a computer security course into our ECET curriculum. The author attempted to balance the concepts and practical applications in this course. This course has been taught four times during the past two years. This is a four-credit-hour course consisting of three credit hours of lecture and one credit hour of laboratory. The evaluation and feedback from students show that it is considered as one of the fun courses they had which helps them understand many of the topics in computer and network security field, and gain some hands-on experience and skills to defend computer systems.

The remainder of this paper is organized as follows: Section two discusses course development and describes the context, course objectives, references, and laboratory exercises. Section three presents our teaching experiences and reflections and, finally, Section four presents our conclusions.

2. Course Development

A Curriculum Context and Course Objectives

In our ECET curriculum, there are a few existing courses pertaining to the computer security course. They are Computer Networks, Wireless Communications and Networks, Computer security discussion may be involved those courses, and we believe that it will be much better to introduce the security topics systematically in this course. This will allow students be aware that security is an integral part of computer and network applications. Besides the technical solution to secure computer systems, topics related to social engineering such as ethics and laws can be discussed in-depth as well.

As an integral part of computer engineering technology program, the primary goal of this course was to provide a broad understanding of computer security issues, from high-level to low level topics in security, privacy, ethics and politics. The ten objectives for this course are as follows

1) To be aware of IEEE and ACM ethics codes
2) To understand the impact of social engineering on computer security.
3) To learn the basic computer security principles, terms and concepts.
4) To learn access control concepts and techniques
5) To understand the basic principle of symmetric and asymmetric cryptography, typical applications and their strengths and weakness;

6) To learn techniques to secure UNIX/Windows OS;
7) To explore the security issues inherent in wireless networks
8) To understand common security flaws in software programming process
9) To be familiar with malwares and common defense techniques
10) To gain hands-on experience on the application of various security software tools

To accomplish these objectives, the mathematical contents of the course such as cryptography and algorithms were treated as a tool to illustrate concepts or "can-do" instead of as the central core of the course.

C. References and Course Content

Although an ideal textbook on computer security for an engineering technology program is still lacking, we adopt [2] as a textbook for this course. However, a majority of lectures are developed by referring [3]-[6] and publications as well. The authors tailored eight lecture modules in this course, for about 30 hours in total.

The first module is an introduction to computer security problems, computer professional's ethical behavior and the impact of social engineering to computer security. It appears to the authors that some students are very interested in developing hacking skills and may abuse some of the knowledge they will obtain from this course. Thus, we feel it imperative to teach our students the related ethics codes such as IEEE and CM ethics codes, and inform related law enforcements. In addition, we guide the students to the impact of social engineering to the computer security and understand that there must be a comprehensive program of ensuring information security, which includes a continual security awareness program.

The second module is to introduction students the basic concepts and terms which answer the following questions, i.e., what is computer security? What are those basic components of security? Topics of C.I.A (confidentiality, integrity and availability) and 3A (authorization, auditing and authentication) are discussed. Additionally, terms such as policy vs mechanism, service, threats, attacks, incidents, and security goals together with various commonly used security mechanisms are also introduced.

The third module is to examine the concept of access control and illustrate how access to systems, resources and data can be controlled. The access rights implemented in UNIX file systems, standalone room access control devices will be used as examples. Further, students gain some hands-on experience through the first lab in which they will develop a simple website with different directories and set up the access control.

The fourth module introduces cryptography, including both symmetric and asymmetric cryptography. The approach we adopted to teach this topic is to briefly introduce the principle by demonstrating that how encryption, decryption and public key generation work. In the symmetric cryptography, we demonstrate the Caesar cipher, Wheatstone-Playfair Cipher and one-time pad. By demonstrating the cryptanalysis of Caesar cipher, Wheatstone-Playfair Cipher, the students are aware of the fact that cryptography is only an improvement, not a perfect security solution. After the study of symmetric cryptography, the students are introduced to

public key cryptography. This usually is one of the interesting and amazing topics to the students. Though we will not touch much about the theory, a simple numerical example of RSA algorithm to generate the public and private key pair process is demonstrated. The applications of asymmetric cryptography for confidentiality, integrity, authentication, digital signature, VPN and secure shell are emphasized in the lecture module.

The fifth module is to teach the students the security design principles and the life-cycle processes in which we examine the security flaws resulted from design, implementation and operation and introduce the general design or security defense guidelines.

The sixth module explores the most commonly used authentication techniques such as password and biometrics techniques. Emphasis is placed on the strengths and limitations associated with each technique. Specifically, students are guided on how to select good passwords. Password failures are demonstrated through various examples and lab experiments.

The seventh module investigates secure programming issue, specifically on the issue of buffer overflow and integer overflow by reviewing those common programming bugs in the C/C++ programs. Tips for low level programming are also introduced.

The eighth module is to investigate the threats from malwares. It also introduces students the common software tools and tips to defend against malwares.

The ninth module is to examine the incoherent security threats present in wireless communications and networks. We examine the design, implementation and operational flaws of the Wi-Fi networks.

C. Laboratory Exercises

In companion with the lecture, there is a three-hour weekly laboratory section for this course in which students will gain hands-on experience with various security topics discussed in the lecture class. Seven lab exercises we developed for this course are as follows.

- Laboratory one is developed to have students gain hands-on experience with access control for a website. In this lab, students need to set up a personal website with a few directories, and set up the webpage access control via simple command such as *htpasswd* and *.htaccess*.

- Laboratory two introduces the Ethereal, a packet sniffer, to students. Students gain hands-on experience to use Ethereal to diagnose and analyze networks. They become aware of the potential threats if plaintext message can be sniffed by using simple software tools. This lab further introduces students to use the Ethereal to capture the password they set up in lab 1 and understand the need of cryptography for some critical applications.

- Laboratory three has students work in pair to implement a public key encryption and decryption program in C/C++ in which students will face the integer overflow problem and learn some basic skills for secure programming.

- Lab four has students gain hands-on experience on how to secure a Windows XP window station. Techniques include administering the accounts, locking down the data and systems, limiting services and rights, logging and other tips for removing spyware etc.

- Lab five is a password selection and password recovery experiment. The first part of the lab is to teach how to set up password policy in the windows XP systems. The second part is to have students obtain the hash function and the encrypted password file, then use password recovery techniques to obtain the password. By examining different password configuration, students understand that a good password can be effectively against attacks.

- Lab six is to use OPNET IT GURU to investigate the deployment of VPN and firewall for corporation networks.

- Lab Seven is a two-week laboratory exercise. It demonstrates the WI-FI WEP flaws. Students explore the flaws with WI-FI WEP and experience the cracking of WEP.

3. Student Feedback and Teaching Reflection

Various methods were used to formally assess the effectiveness of this course, including tests, the evaluation of student work, and the instructor's assessment of laboratory work. The overall response from students regarding whether the course met their expectations was very positive. Summarized student comments are:

- This course presents interesting topics and helps them to learn new technologies.
- They have a better understanding of computer security and network security issues.
- Though some of the labs are difficult, but it is rewarding to see the outcomes.
- This course helps students learn various software tools to secure computers and networks.

One issue we realized in this course is that students may use the techniques and skills maliciously outside of the classroom. Thus, as an instructor of computer security, the legal issue of malicious activities should be continuously stressed in the class. In addition, instructors may require students to sign contracts saying that they will not use knowledge and techniques gained in the classroom or laboratory to conduct unlawful activities. Our future improvement for this course is to add some special topics such HIPAA (Health Insurance Portability and accountability) patient privacy, remote monitoring systems to this class.

4. Conclusion

The explosive growth of computer systems and Internet applications has increased our dependence on computers and networks. This dependence and frequently occurred computer attacks have resulted in an imperative need for computer security education and security awareness promotion. This paper provides a brief summary on a computer security course taught for CET/EET program. Overall, response from students shows that this new course is successful in helping them learn fundamental knowledge on computer security and gain basic skills to defend computer systems.

References

1. CSI's 12th Annual Computer Crime and Security Survey, available online at http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2007.pdf
2. M. Bishop, Introduction to Computer Security, , Addison-Wesley-Longman.
3. W. Stalling, Network Security Essentials, Addison-Wesley.
4. C. Eastton, Computer Security Fundamentals, Prentice Hall.
5. C.P. Pfleeger , Security in Computing, Prentice Hall.
6. R. Anderson, Security Engineering, Wiley.