A Course on Computer and Network Security: Teaching Online Versus Face-to-Face

Suresh Kalathur, Lubomir T. Chitkushev, Stuart Jacobs,
Tanya Zlateva, and Anatoly Temkin

Department of Computer Science, Metropolitan College, Boston University,
808 Commonwealth Avenue, Room 250, Boston, MA 02215, USA
{kalathur,ltc,sjjacobs,zlateva,temkin}@bu.edu

Abstract. The paper presents an overview of the Computer and Network Security course offered through distance education division as part of the online degree program. Topics presented in the online format are compared with those presented in a traditional curriculum in the face-to-face format. The pros and cons of each of the formats are discussed. Unique to the online course are weekly discussion topics that require each student's participation and the follow-ups to postings of other students. A distinguishing aspect of the online course is a three week based case study assignment exploring a practical security framework encountered in real companies.

Keywords: Computer security, network security, software security, distance education.

1 Introduction

Computer and network security is one of the fastest growing fields in information technology that poses a two-fold challenge to the educator: i) designing curricula that reflect the inter-disciplinary aspects of information security and integrate fields as diverse as technology, law, economics, management, policy, and ethics; and ii) finding delivery formats that make information security education widely available and at high quality. Online education is *the* fastest growing segment of the educational and training sector. It has firmly entered the mainstream: more than 3 million students were enrolled in at least one online course in 2005 as compared to 2.3 million in 2004 and this trend is expected to continue [1-2]. This evolution has led some researchers to describe online learning as a revolution in the nature of higher education that will result in a radical transformation from the currently predominant teacher-centered, face-to-face pedagogy to an online and hybrid, student-centered approach [3]. But even if one does not embrace the new delivery format, one can hardly overstate its importance and implications for the development of the workforce. This brings the question of the quality of online education—both its perception as well as actual documented learning outcomes—front and center in the discussion of new educational technologies. A growing number of publications are devoted to educational technologies that are based on the inherent characteristics of the new medium, espe-

cially multimedia, collaborative learning environments, learning networks, simulations and gaming [4].

This paper presents our experience with teaching a computer and network security course in an online delivery format, and striving to meet the demands of a highly technical, interdisciplinary subject in the context of the possibilities and limitations of the online medium. The course is part of the online MS CIS with concentration in information security. Boston University's information security programs [5] are nationally certified by CNNS and the University is recognized as a Center of Academic Excellence in Information Assurance Education. We have extensive experience with various distance education modes, more specifically we have offered videoconferencing courses (1996-2000), blended programs [6], and have currently one of the largest online graduate programs in security with over 300 students enrolled.

As part of our security curriculum, we offer the core course on computer and network security in both the face-to-face and online formats. The face-to-face course, on average, has approximately 20 students in each offering. The online classes, on the other hand, have an enrollment of approximately 120 – 150 students in each offering. The lecture materials for the online course are prepared by the instructor well in advance and exported by instructional designers into the online courseware system. During each course offering, the online course is divided into sections of 15 students each. A facilitator is assigned to each section and is solely responsible for the smooth running of that section, taking care of day-to-day interaction with the students, grading the assignments, monitoring the discussions, and providing timely feedback. The instructor assigned to the course oversees the facilitators and provides guidance and instructions to the facilitators in order to ensure uniform criteria are applied across all the sections by the various facilitators. Another major distinction between the two formats is the fact that the face-to-face course spans a 14 week period, whereas the online course runs during a 7 week time frame.

With face-to-face instruction there are a number of advantages – the instructor is able to take advantage of student *body language*, communication with students occurs in *real-time* as a dialogue, corrections may be rapidly disseminated, and the lecture material can be expanded upon extemporaneously and presented to all students immediately. However face-to-face instruction has some disadvantages – lecture material has to be preplanned to fit within a fixed class period time window, student attention during a class period may not be optimal, and student attendance may be prevented due to non-academic forces.

On the other hand, fixed class durations necessitate careful consideration of what, and how much, material will fit into the available time. This reality may impact the logical flow from subject to subject. Another reality of set class schedules is that a class may be scheduled at a time when a student's attention span is not optimal, such as in the evening after a student has already spent the day at their full time place of employment. If a student has no time for a break between work and class, then he/she can easily miss a meal or attend to other pressing activities. Given that students have non-academic responsibilities, these obligations can cause a student to miss a class. Lecture notes, or slides, are not as comprehensive as textbooks and typically serve as talking points for the instructor's lecture. So by missing a class, the student is unable to hear what the instructor presents in class, and being able to obtain the notes for the missed class does not fully make up for having missed the instructor's actual presenta-

tion. With the *distance/online* instruction, a student is able to choose when the best time is for reviewing the lecture material and is in a position to work around non-academic obligations.

2 Online Curriculum

The online course, *Computer and Network Security for Business* (MET CS695), is a required course for the students in the security concentration of the Master's program in Computer Information Systems. Prior to taking this course, students take the *Business Data Communications and Networks* (MET TC625) course as a prerequisite.

The following subsections describe in detail the contents covered during each week of the course. Aside from the lecture material provided to the students, communication amongst the students is strongly encouraged through weekly discussion topics. Assignments for each week ensure that the students do not lag in the study material for the week. The references listed in [7-11] are the primary materials referenced in the both the online and face-to-face courses.

2.1 Introduction and Security Overview

The material presented during the first week gives a bird's eye view of the security landscape from the perspective of a computer user – why is the user important to computer security, what are the threats to the user's computer, and as a user, what remedies are available. The notion of *defense*, *deterrence*, and *detection* and how they complement each other along with the controls and strategies required for a comprehensive security policy are then detailed. The *Common Body of Knowledge* and its domains and briefly explored during this lecture. Application security vulnerabilities are discussed with specific examples that include *SQL Injection*, *Cross-site scripting* and *buffer overflow* problems and case studies like the SQL Slammer, W32/Sobig.F worm, and W32/Blaster worm and their devastating capabilities are shown to the students.

2.2 Access Control and Operating System Security

The topics covered during this week include the security protection offered by the operating system itself. The address protection methods like fence registers, base and bound registers, segmentation, and paging techniques are explored here. Access control is then introduced from the perspective of a *reference monitor.* The concept of a subject, an object, and the access operations are illustrated.

Access control structures are then explored from an abstract viewpoint of the access control matrix and concrete implementations like the access control lists and the capability lists. The *Bell-LaPadula* security model for the confidentiality and the *Biba* model for the integrity of the data are shown. The *Chinese-Wall* model is then illustrated to handle the situations so that no conflicts of interest would ever occur in

the system. Lastly, the *Clark-Wilson* model is shown in preserving the integrity within commercial applications.

The last lesson in this week's content presents the first half of the operating system security topics that include UNIX security and a practical illustration of role based access control in the *Solaris* operating system. Topics including user and group accounts, *setuid* and *setgid* attributes, and audit logs that record the security related events are explored.

2.3 Windows Security, Application Security, and Cryptography

A majority of the students work with Microsoft Windows based operating system and hence it is equally important to educate the students with the various aspects of Windows security. Starting with the Windows security architecture, the access control model is shown in terms of the *access tokens* and the *security descriptors*. The *discretionary access control list* and the *system access control list* (SACL) are shown with examples. The role of the *trust relationships* and *active directory* and the mechanisms to define them are depicted with real examples. The lesson on Windows security is wrapped up with a case study of how the *role-based access control* is set up in Windows Server 2003 and its distinction from the group-based access control.

The second lesson during this week's lecture material focuses on the buffer overruns resulting from poor coding practices, lack of safe string handling functions, stack and heap overruns, array indexing errors, etc. With the help of a few simple "C" programs, the above problems are demonstrated step by step and the outcomes before and after the problem code in question is executed are presented.

The next lesson primarily takes the *Java* programming language as the basis and presents the various security aspects from the perspective of the language itself. This week concludes with the lesson on the cryptographic functions and their uses. Public and private key encryption, confidentiality and authentication, substitution and transposition, mono alphabetic and poly alphabetic ciphers, DES and AES, RSA, message digest and fingerprints are thoroughly presented with examples.

After the first three weeks, the mid term exam is administered and then the curriculum proceeds with the network security part. The Network Security portion has been divided in three areas, each covering a week of online content. Our general idea was to start with the introduction of network security principles and authentication techniques, followed by network layer security framework and firewalls, and concluded by higher layers security protocols.

2.4 Network Security Principles and Authentication Protocols

The first week of network security (NS) covers the following topics: Rational for NS; Objectives for NS; Overview of Network Architectures (OSI and Internet Network model); NS Issues; Security of network layers; Security threats, risks, safeguards and vulnerability; Network threats and safeguards (covering LAN, WLAN, MAN, WAN and the Internet); NS services and mechanisms; Models of NS; Authentication protocols (Kerberos and X.509 Authentication service). Discussion topics for this section

focus on key security concepts, such as security implications of centralizations based on key distribution schemas using an access control center or key distribution center. Other topics discussed are related to the ethics of network security, such as how should a CSO relate to vulnerabilities, both in the products used and in the products created by the company. Also how should the manufacturer (hardware and software) act when confronted with vulnerabilities found in their products are discussed.

2.5 Network Layer Security

The second week of material covers Network layer security framework, namely, the IP security framework; IPSec implementations; security associations; Key management and firewalls. In this section, the students learn about the challenges of providing security in a connectionless IP environment and the specific techniques used in the IPSec framework. Discussion topics for this week cover questions related to firewalls, such as why the firewalls should be configured to inspect both outgoing and incoming traffic. Also, they cover questions related to IPv6 such as whether the adoption of IPv6 in a near time would be more of a boost or a hindrance to security. Also how should a company approach the migration, and whether it will be additional burden on the company when time comes to adopt IPv6 are discussed.

2.6 Higher Layers Security

The last week of the network security part of the online course covers security of the transport and application layers. The topics covered are: SSL and TLS; Web security and Email security; and Secure electronic transactions (SET). The intent of this section is to expose the students in a systematic way to the main security protocols used for communication at the transport layer, and the advantages and ways of providing application layer security.

Discussion topics for this section focus on the advances made in application level security, and the fact that despite them we are still quite vulnerable to spamming and phishing, which costs the industry and the end-user millions of dollars each year. The students are asked to discuss what the weak points are and what would they suggest be done about them.

3 Face-to-Face Curriculum

The course, *Network and Software Security* (MET CS654), is offered every semester in the traditional face-to-face instruction. The following sections describe our face-to-face approach to the subject of information security. This course places the classic subjects of computer and communications security into the context of an over-arching security governance program and spans the major security knowledge domains in the Common Body of Knowledge recognized by the International Information Systems Security Certification Consortium (ISC).

3.1 Introduction to Information Security and Computer Security Concepts

These lectures (over a 4 week period) begin with business drivers, security policies, security domains, and security models. Vulnerabilities, formal threat concepts and basic attack concepts are then presented along with taxonomies of threats, threat agents, and attacks. An overview of the concepts of security services and security mechanisms is presented followed with a review of cryptography concepts (symmetric & asymmetric encryption, keyed hashes, digital signatures, and cryptanalysis). Also covered are protection in Operation Systems (OS), OS memory security mechanisms, user authentication and protection of passwords, and the need for file system security. OS security layers/rings are presented with details on OS Security controls. A review of basic networking concepts (protocols, routing and network types) and current security mechanisms/capabilities by protocol concludes this section.

3.2 Security of Specific Operating Systems

These lectures (over a 4 week period) present security within typical operating systems, namely: UNIX security, UNIX Best Practices, Linux Security, Solaris OS & Role Based Access Control (RBAC), Embedded OS Security, and Windows. Database management systems (DBMS) security is discussed along with the application of Clark-Wilson concepts to DBMS. The following lectures consider the application of encypherment for the following areas – authentication (symmetric, asymmetric, hashes), confidentiality (symmetric, asymmetric), integrity (symmetric, hashes), non-repudiation (asymmetric), and conclude with a discussion on key management (KDCs-Kerberos, PKI-Digital Certificates, Key Distribution Keys vs. Session Keys).

3.3 Networking Security Mechanisms and Security Management

These lectures (over a 4 week period) begin with a discussion of current authentication, confidentiality & integrity deficiencies within protocol layers. Mechanisms to mitigate networking vulnerabilities are presented including: IEEE 802.1x, IPsec, TLS-DTLS-SSL, SSH, firewalls, application gateways, deep packet inspection, network application security (e.g., Email, VoIP), and the usefulness of XML security mechanisms. A series of network security use cases are presented (ISP, Enterprise, and Service Provider) to demonstrate the layering of the aforementioned security mechanisms. The final lecture tackles the issue of managing deployed security mechanisms from a TMN Model perspective and then focuses in on Security Service Management (Security Event-Fault-Attack Management, Security Configuration Management, Login Access Management, Authentication Credentials Management, and Verification and Validation Management).

4 Assessments

In the case of the face-to-face course, students are evaluated through a set of homework problems, a mid term exam, a final exam, and student participation through the duration of the course. The online course, on the other hand, has weekly discussion topics, weekly assignment problems, a mid term exam, and a final proctored exam. The discussion topics for each week are prepared in advance by the instructor. Participation is graded based on the student's contribution to the original topic and as well as their follow up postings on other students' postings. The mid term exam, in most part, consists of a series of short paragraph style questions, and students have a fixed duration of 3 hours from the time they start the assessment at any time during the mid term exam week. The final exam is a proctored 3 hour exam, proctored at an authorized test site, or through a designated proctor when a test site is unavailable within a reasonable geographic distance.

A notable feature of the online class for the network security portion is a 3-week single assignment, with deliverables expected in each of the three weeks. The students are required to develop a case study and submit a report in the form of a short paper exploring the points requested. When developing the case study the students are free to use the material covered in the lectures, textbook as well as other sources that have to be mentioned in the bibliography. Each weekly assignment is worth the same number of points.

During the first week the students are asked to assume the role of a CSOs (Chief Security Officers) for a newly formed company (such as a bio-technology start-up) The students are given the main information about the structure of the company and their international divisions, as well as the work process requirements pertaining to data stored in its internal network. For the first week the students are required to provide a rationale for the level of security they think should be enforced. They are required to give a topology of the suggested network and explain the choices made, and characterize the protocols (both transport and application) present in the suggested topology, and the rational for selecting them.

During the second week the students are required to provide a threat assessment report for the internal network(s) of the company as defined in the first assignment, and point the mechanisms used to mitigate these threats, and where they'll be used. They can also include any other form of security prevention measure (choice of OS, hardware, vendor, etc.).

During the third week the students are required to refine the second week's work by adding application-level security. Also, students have to analyze security threats and address each of them, by proposing an appropriate security mechanism. The three weekly portions of the assignment form a logical sequence that enables students to learn the subject through applied exercises of increasing complexity, and have been positively mentioned in student evaluations.

5 Conclusion

In the above sections, we presented the topics presented to the students in the on-line program versus the face-to-face course. The course evaluation for the face-to-face program currently uses different criteria from the online program. We are in the process of developing a uniform set of student assessment criteria for both these programs. In the face-to-face course, the instructor is solely responsible for the success of the course. In the case of our online program, the facilitators along with the instructor play a crucial role in maintaining the day-to-day interaction and meeting the expectations of a wider body of students. By developing a richer assortment of interactive modules, the satisfaction rate of the online students can be significantly increased. All these components, otherwise unavailable to the face-to-face instructor and the students, can be incorporated into the traditional curriculum and provide a greater experience to their audience as well.

References

1. Allen, E.; Seaman, J.: Entering the Mainstream: The Quality and Extent of Online Education in the United States, 2003-2004. Sloan Center for Online Education at Olin and Babson College, Needham, MA 2004.
2. Allen, E.; Seaman, J.: Making the Grade: Online Education in the United States 2006. Sloan Center for Online Education at Olin and Babson College, Needham, MA 2006.
3. Hiltz, S.R.; Turoff, M.: The Evolution of Online Learning and the Revolution in Higher Education. Communication of the ACM, October 2005, vol. 48, No. 10.
4. Hiltz, S.R.; Goldman, R. (Eds): Learning Together Online: Research on Asynchronous Learning Networks. Erlbaum, Mahwah, NJ, 2005.
5. Zlateva, S.; Kanabar, V.; Temkin, A., Citkusev, L.T.; Kalathur, S: Integrated Curricula for Computer and Network Security Education, Proceedings of the Colloquium for Information Systems Security Education, Society for Advancing Information Assurance and Infrastructure Protection, Washington, D.C., June 3-5, 2003.
6. Zlateva, T.; J. Burstein: "A Web-Based Graduate Certificate for IT Professionals - Design Choices and First Evaluation Results". Proceedings of the 2001 Annual Conference of the American Society for Engineering Education(ASEE), June 24-27, Albuquerque, New Mexico.
7. Anderson, R.: Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 2001.
8. Gollmann, D.: Computer Security, 2nd edition. Wiley, 2006.
9. Howard, M. and LeBlanc, D.: Writing Secure Code, 2nd edition. Microsoft Press, 2002.
10. Stallings, W.: Network Security Essentials: Applications and Standards, 3rd edition. Prentice-Hall, 2007.
11. Charlie Kaufman, Radia Perlman and Mike Speciner, *Network Security -- Private Communication in a Public World, 2nd Edition*, Prentice-Hall, 2002.