2005

Teaching Information Security Courses: Objectives, Requirements, and Challenges

Bradley K. Jensen  
*University of North Texas, jensenb@unt.edu*

Melinda Cline  
*University of North Texas, clinem@unt.edu*

Follow this and additional works at: [http://aisel.aisnet.org/amcis2005](http://aisel.aisnet.org/amcis2005)

Recommended Citation

[http://aisel.aisnet.org/amcis2005/272](http://aisel.aisnet.org/amcis2005/272)

This material is brought to you by the Americas Conference on Information Systems (AMCIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in AMCIS 2005 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Teaching Information Security Courses: Objectives, Requirements, and Challenges

Dr. Bradley K. Jensen  
University of North Texas  
jensenb@unt.edu

Dr. Melinda Cline  
University of North Texas  
clinem@unt.edu

ABSTRACT

Given the magnitude of real and potential loses associated with security breaches, public employers increasingly expect graduates of management information systems (MIS) programs to have a broad understanding of information security concepts. Support for requiring this broad understanding are based on industry estimates that security breaches affect 90% of all businesses every year and cost some $17 billion (Austin & Darby, 2003). In response to these needs, undergraduate and graduate courses were developed where the primary course objectives discussed involve network security, information warfare, and computer forensics. The infrastructure requirements for the courses include the establishment of appropriate course prerequisites, setting up a secure laboratory environment to accommodate the development of viruses and worms, and white hat agreements to protect universities and faculty members involved with these courses. White hat agreements with the students are a key element to the enforcement of policies associated with these courses. Based on both classroom experience and collaboration with information security industry executives, including Federal Bureau of Investigation (FBI) and Secret Service representatives, the authors conclude with a discussion of “lessons learned” and suggestions for safely teaching effective information systems security courses.

Keywords: Information Security, Course Development.

INTRODUCTION

According to industry estimates, security breaches affect 90% of all businesses every year and cost some $17 billion (Austin & Darby, 2003). Given the magnitude of real and potential losses, both private and public employers increasingly expect graduates of management information systems (MIS) programs to have a broad understanding of information security concepts. This paper discusses the course objectives, infrastructure requirements, and related challenges associated with offering graduate and undergraduate information security courses. The primary course objectives discussed involve information technology security, enterprise security architecture, network security, information warfare, cyber warfare, cryptography, and computer forensics. Differences between graduate and undergraduate expectations are highlighted. The infrastructure requirements discussed include the establishment of appropriate course prerequisites, setting up a secure laboratory environment to accommodate the development of viruses and worms, and white hat agreements to protect universities and faculty members involved with these courses. A sample white hat agreement is included as Appendix A. Based on both classroom experience and collaboration with information security industry executives, including Federal Bureau of Investigation (FBI) and United States Secret Service representatives, the authors conclude with a discussion of “lessons learned” and suggestions for safely teaching effective information systems security courses.

OBJECTIVES AND COURSE DESIGN CONSIDERATIONS

As a result of the increased focus on security, objectives for the development of these courses include the development of a security curriculum that meets the needs of the curriculum advisory board, attracts students to the IS program, and establishes a foundation for offering certification and degree programs in information security in the future. Several universities have either started to expand their curriculum to incorporate information security in their computer science departments (and in some cases, their business schools) or are considering this for the near term.
Initial course design is based on research that involved investigating how other security courses have been developed. Both Computer Science (CS) and Business Information Systems (MIS) courses were reviewed. This review indicated that there are a limited number business oriented security courses currently being offered at universities. However, there are several good computer science security courses (Dunigan, 2004, Koc, 2004, Aycock, 2005), which we used to help determine course topics. We then modified the approach from a computer science to a business perspective. These modifications occur in the areas of security risks, security countermeasures, and cryptography (Dunigan, 2004, Koc, 2004). For example, Computer Science courses examine cryptography from an algorithmic perspective. We used the cryptographic elements, but oriented them towards a business oriented application perspective by having students apply various methods of encryption and testing their effectiveness. Aycock (2005) offers one course on writing computer viruses and malware and another course covering spam and spyware, both of these courses address root issues associated with security. Aycock’s viruses and malware course has students reviewing existing viruses and generating viruses. As a result of Aycock’s emphasis on malware, we set out to not only have students learn about and experience viruses and malware generation – but, to concentrate on the architecture associated with preventing them and minimizing their impact. Again, the focus of our course development was on the information technology/systems student (business orientation) and more as a complement to the existing base of computer science based information security courses.

One of the primary goals was to offer students a unique perspective as to the approach to implement an effective security architecture within a corporation. One goal associated with developing this curriculum involved establishing an undergraduate course that is a prerequisite for the graduate course. With this in mind, the goals of the undergraduate course are to:

- Provide students with an introduction to various technical and management aspects of information security (IS) and information assurance (IA).
- Promote a more comprehensive understanding of security requirements within an organization.
- Promote an understanding of the threats of malware through the analysis and generation of worms, viruses, Trojans, and logic bombs.
- Make students aware of the various technologies to implement appropriate security measures within an organization.
- Provide an understanding of how to inspect and protect information assets as well as how to plan and respond to information security from technical and managerial perspectives.

This course is designed to provide the foundation for understanding the key issues associated with protecting information assets, determining the levels of protection and response to security incidents, and designing a consistent, reasonable information security system with appropriate intrusion detection and reporting features.

To promote a more comprehensive understanding of security requirements, students are required to analyze and generate worms, viruses, Trojans, and logic bombs from an academic perspective. They are also exposed to the spectrum of security activities, methods, methodologies, and procedures. An element of exposure to this spectrum includes labs where they write and analyze malware, implement and apply various forms of intrusion detection, firewalls, anti virus applications, and analyzers. The labs and lectures are intended to instruct students in the inspection and protection of information assets, detection of and reaction to threats to information assets, and examination of pre- and post-incident procedures, technical and managerial responses and an overview of the information security planning and staffing functions.

Required textbooks for the undergraduate course are Whitman’s *Principles of Information Security* and Howard’s *Writing Secure Code*. Whitman’s text was chosen to provide students with the fundamentals associated with information security requirements and principles from a business perspective. Two key items were missing from the content of Whitman’s text, an exposure to the nature of malware and the significance of security principles throughout the system’s development life cycle (SDL). Howard’s text was chosen for its emphasis on the importance of employing security principles during the entire SDLC, not just as a milestone following the generation of the code.

The goals of the graduate course are to:

- Provide students with an understanding of the field of Enterprise Architecture for Information Technology Security.
- Expose students to the various technical and management aspects of physical, architectural, topographical, and enterprise security.
- Promote legal and ethical considerations of information security.
Help students understand the importance of computer forensics.

Provide students with an understanding and application of information warfare and cyber warfare.

This course builds on the foundation of the undergraduate Introduction to Information Technology Security course (BCIS 4630). Topics for the graduate course include: enterprise security, information warfare, cyber warfare, and computer forensics. The enterprise security sections includes coverage of the basics and architecture of security within the enterprise; management of the physical, network, and information security constructs; issues associated with WAN/LAN and wireless security; dealing with hackers and hacking; and issues associated with an enterprises distributed systems. Legal and public relations implications of security and privacy issues and the laws governing these issues are also covered in the graduate course. Required textbooks for the graduate course are Campbell’s *Security+ Guide to Network Security Fundamentals*, Furnell’s *Cybercrime Vandalizing the Information Society*, and Nelson’s *Guide to Computer Forensics and Investigations*.

**CHALLENGES**

One of the most challenging aspects of teaching information security courses involves the use of labs to develop malware (viruses, worms, Trojans, and logic bombs). It is important to have students understand the difficulty in the generation of malware as well as to develop a solid understanding of how malware functions. The belief being that students that have a solid understanding about malware are better suited to protect against it. There is concern that students may propagate malware not only within the confines of a university’s intranet, but that there may be potential ramifications associated with the accidental (or purposeful) release of malware onto the Internet.

To limit this form of exposure it is important to have separate workstations/servers dedicated to the security courses for lab work. To achieve the most realistic business environment in a cost effective way, students should be divided into teams with each team provided with a client and a server connected to other teams clients and servers via a switch. The workstations should be connected on a private network and not to the university's intranet or to the Internet. In addition, the USB, floppy drive, and ZIP drives should be disabled to prevent moving malware from the dedicated security workstations/servers to other workstations. The source for input of pre-existing material is through a read only CD-ROM. Therefore, there is no way for students to physically remove any code generated on these machines from the lab. All work remains on the security client and server workstations. Required physical output is sent to a printer that is attached to this private security network.

**CONCLUSION**

Since their inception, both courses have been popular among business and computer science students alike. As a result of lessons learned, the following are some suggestions for other faculty incorporating a security curriculum into their program:

- The faculty member should have a good understanding of information security principles and challenges, knowledge of one or more programming languages, knowledge of security and malware tools and generators, and exposure to networking tools.
- Prerequisites for students include knowledge of at least one programming language and a good understanding of networking fundamentals.
- The university needs to be able to support a dedicated lab and be able to work with the faculty to install and maintain appropriate workstation configurations. On these machines, students should have the ability to troll for or generate malware.

Departments electing to undertake the complexities and challenges associated with an information security curriculum will be rewarded with the popularity of the courses among students. In our case, several local corporations are having their employees and potential new hires take the undergraduate course at a minimum and, preferably, both the undergraduate and graduate courses prior to being hired by their information security organization. As information security demands continue to increase, these courses provide students with sought after skills and they do so in such a way as to emphasize the business considerations and consequences of effective information management.
REFERENCES


Appendix A

Acknowledgement Statement

The Fundamentals of Information Technology Security course offered by the University of North Texas Business Computer Information Sciences department includes information concerning known computer viruses, worms, Trojans, and logic bombs. The course also includes information about the generation of software for purposes of determining propagation and threat characteristics to assist in successful intrusion detection and prevention. The intellectual property associated with the output from the labs and the material presented during lectures is to remain an academic research endeavor and may not be applied or otherwise used for inappropriate or unlawful purposes.

In consideration for being permitted to participate in the Program, I hereby understand and acknowledge that:

1. Some of the content of this course may be considered controversial and information learned in this course must be used only for the express purposes of academic research or other academically accepted purposes. The intentional or negligent application of information offered in this course may constitute a violation of federal or state law and subject me to criminal, civil and university sanctions.

2. I am solely responsible for my intentional or negligent use of information offered in this course. I further expressly acknowledge that the University of North Texas, its academic departments, faculty, staff and agents are not responsible for student intentional or negligent use of information offered in this course.

3. Computer resources and data are considered valuable assets of the University of North Texas. Further, computer software purchased or leased by the University is the property of the University or the company from whom it is leased. Any unauthorized access, use, alteration, duplication, destruction, or disclosure of any of these assets may constitute a computer-related crime, punishable under Texas and federal laws.

4. Misuse of the University's computer resources and the content of information offered in this course is strictly prohibited. Misuse of computing resources includes, but is not limited to: criminal and illegal acts, including support of illegal activities such as unauthorized access of university, proprietary or other information technology resources, intentional corruption or misuse of computer resources, theft, obscenity, and child pornography.

5. I am responsible for obtaining and following applicable University of North Texas computer use policies.

5. Violation of this Acknowledgement Agreement constitutes a violation of the University of North Texas student code of conduct and may result in disciplinary action, to include suspension or expulsion.

By signing this Acknowledgement Agreement, I expressly represent that I understand and agree to abide by its terms and conditions and that I will use the materials associated with this class purely for academic purposes.

Signed this _____ day of month & year.

Printed Name of Student: ________________________________

Student Signature: ________________________________