The Graduate MIS Security Course: Objectives And Challenges

Bradley K. Jensen, University of North Texas, USA
Carl S. Guynes, University of North Texas, USA
Andrew Nyanoga, William Paterson University, USA

ABSTRACT

Given the magnitude of real and potential losses, both private and public employers increasingly expect graduates of management information systems (MIS) programs to understand information security concepts. The infrastructure requirements for the course includes setting up a secure laboratory environment to accommodate the development of viruses and worms. The labs and lectures are intended to instruct students in the inspection and protection of information assets, as well as detection of and reaction to threats to information assets.

Keywords: MIS, enterprise security, information warfare, cyber warfare, computer forensics

INTRODUCTION

According to industry estimates, security breaches affect 90% of all businesses with cost estimated at $17 billion [1]. Given the magnitude of real and potential losses, both private and public employers increasingly expect graduates of management information systems (MIS) programs to understand information security concepts. The Department of Homeland Security has awarded more than $18 billion to state and local governments associated with security. Associated with this effort were strategies targeted at securing cyberspace, and assets and infrastructures considered vital. As a result of this increased focus on security, objectives for the development of these courses included the development of a security curriculum that would meet the needs of the curriculum advisory board, attract students to the MIS program, and establish a foundation for offering certification and degree programs in information security for the future. A second consideration when developing this curriculum was the need to recapture students for MIS programs. With the drop in enrollment by as much as 70% in MIS programs at universities around the United States, there has been a concerted drive to increase interest. The two major areas of consideration for this have been gaming and security. As a result, several universities have either started to expand their curriculum to incorporate information security in their business schools, or are considering this for the near term.

This paper discusses the course objectives, infrastructure requirements, and related challenges associated with offering successful graduate information security courses. Issues related to instructor training, setting up a isolated learning infrastructure, and requisite knowledge is also discussed. Primary course objectives involve information technology security, enterprise security architecture, network security, information warfare, cyber warfare, cryptography, and computer forensics. Based on both classroom experience and collaboration with information security industry executives, including Federal Bureau of Investigation 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.

COURSE DESIGN CONSIDERATIONS

Initial course design for this curriculum is based on research that involved investigating how other security courses have been developed. Information Systems courses were reviewed through an Internet search that involved keyword and specific university criteria. 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 [2, 4, 6] which were used to help determine course topics. While the CSCI courses involved a high degree of concentration on cryptographic algorithms, the MIS courses should only require a basic understanding of cryptographic principles because business students only need to be able to understand and apply the constructs. The determinate of Information Security Course Success is based on Figure 1.

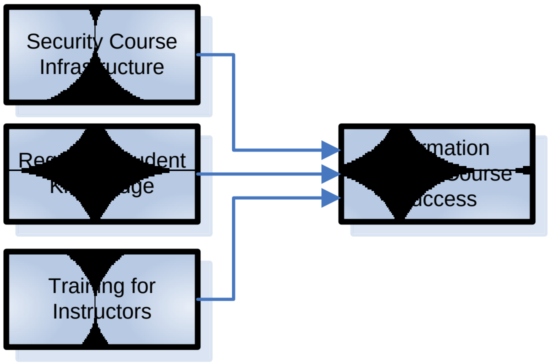
Security Course Infrastructure
Required Student Knowledge
Training for Instructors
Information Security Course Success

Figure 1

These Information Security Course Success factors involve modifications to existing courses in the areas of security risks, security countermeasures, and cryptography [4, 6]. Again, Computer Science courses examine cryptography from an algorithmic perspective. These cryptographic elements should be presented, but oriented towards a business oriented application perspective by having students apply various methods of encryption and then testing their effectiveness. Aycock [2] 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.

COURSE GOALS

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. The primary goals of the graduate course are to:

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

Topics for the graduate course include: enterprise security, information warfare, cyber warfare, and computer forensics. The enterprise security section 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*[3], Furnell's *Cybercrime Vandalizing the Information Society*[5], and Nelson's *Guide to Computer Forensics and Investigations*[7].

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

Following are some suggestions for other faculty incorporating a security curriculum into their program:

1. The faculty member should have a good understanding of information security principles and challenges, knowledge of one of more programming languages, knowledge of security and malware tools and generators, and exposure to networking tools.
2. Prerequisites for students include knowledge of at least one programming language and a good understanding of networking fundamentals.
3. 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 a computer security course prior to being hired by their information security organization. As information security demands continue to increase, security 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.

AUTHOR INFORMATION

Brad Jensen is an Assistant Professor of Information Systems at the University of North Texas. He received his Ph.D. from the University of North Texas. His research interests include computer security, organizational change, privacy, impacts of new technologies, and software development. He has published articles in Computers *and Society, and Computer Science Education*

C. Stephen Guynes is a Regents Professor of Business Computer Information Systems at the University of North Texas. He received a doctorate in quantitative analysis from Texas Tech University. Dr. Guynes' areas of specialization are client/server computing, end-user computing, data administration, and information resource management. His most recent research efforts have been directed in the areas of client/server computing and data administration. Some of the journals in which Dr. Guynes has published include and *Communications of the ACM, Information & Management, The Journal of Information Systems Management, Journal of Accountancy, Journal of Systems Management, The Journal of Database Management, The CPA Journal, The Journal of Computer Information Systems, Information Strategy, Computers and Security, and Computers and Society* .

Dr. Andrew B. Nyaboga earned his Ph.D at Stevens Institute of Technology, Hoboken New Jersey in 2000.Currently he is an associate professor of Accounting and Law at William Paterson University in Wayne New Jersey and teaches courses in accounting and accounting Information System. His research interests are in technology management, knowledge management and strategic Management. His work has been published in numerous refereed journals.

REFERENCES

1. Austin, Robert D. and Christopher A.R. Darby (2003), "The Myth of Secure Computing," *Harvard Business Review*, 81(6), p.120 –126.
2. Aycock, John (2005), http://pages.cpsc.ucalgary.ca/~aycock/, University of Calgary.
3. Campbell, Paul, Ben Calvert, and Steven Boswell (2003). *Security+ Guide to Network Security Fundamentals.* Thomson Course Technology.
4. Dunigan, Terry (2004), http://www.cs.utk.edu/~dunigan/cns04/, University of Tennessee.
5. Furnell, Steven (2002). *Cybercrime Vandalizing the Information Society,* Addison Wesley.
6. Koc, Cetin Kaya (2004), http://security.ece.orst.edu/koc/ece575/, Oregon State University.
7. Nelson, Bill, Amelia Phillips, Frank Enfinger, and Chris Stuart (2004). *Guide to Computer Forensics and Investigations,* Thomson Course Technology.