https://doi.org/10.48009/2_iis_2011_217-222

Issues in Information Systems

Volume XII, No. 2, pp 217-222, 2011

INFORMATION SECURITY CURRICULUM: A PEDAGOGICAL ANALYSIS OF CURRENT DEGREE PROGRAMS

Someswar Kesh, Department of Computer Information Systems , e-mail:kesh@ucmo.edu

ABSTRACT

This paper provides a pedagogical analysis of current information systems security programs from various U.S. universities and classifies the coursework offered in these universities into common themes. It is expected that universities planning to offer degree programs in information systems security can use these themes as the fundamental basis for developing a structure of their own degree program consistent with their needs. Universities currently offering such programs may also utilize the thematic structure to reevaluate their programs and make changes, if necessary.

Keywords: Information Security Education, Pedagogical Analysis

INTRODUCTION

Information systems now control many critical aspects of our lives; including nuclear power plants, defense equipment, financial transactions etc. At the same time, attempts or probability of an attempt to attack these systems have increased significantly (http://www.sans.org/top-cyber-security-risks/trends.php)**.** This has resulted in an increased demand for I.T security as well as professionals trained in I.T. security. Many universities have responded to this increased demand by offering degree as well as certificate programs. This paper provides a thematic structure for I.T. security programs. This structure has been developed by analyzing the coursework of the current degree programs. Along with the structure, other issues such as the location and level of the programs have also been considered. It is expected that this analysis will be useful to the colleges and departments contemplating opening up new programs or making modifications to existing programs.

WHAT IS INFORMATION SECURITY?

While there are many ways in which information security may be defined, it is perhaps appropriate to examine the components of information security rather than attempt to define it. Information security is based on the CIA triad; confidentiality, integrity and availability. Based on this, the International Information Systems Security Certification Consortium or $(ISC)^2$, provides ten domains of information security that provides a basis for the field (Gregory, 2010). A brief description of these ten domains will provide us with a glimpse of what the field consists of.

Access controls control the user's access to information systems. This includes software, hardware and networks. Access controls can either be implemented manually or be automated. Manual access controls are more commonplace in smaller organizations that may not be able to afford automated systems, while it may be impractical and uneconomical for larger organizations to have manual access control systems. Access controls can also be role-based (Ferraiolo and Kuhn, 2009). Application security, the second domain deals with either off-the shelf software or applications developed in-house. With the development of cloud computing, application security has gained significant importance (Chow et al. 2009). Irrespective of any security measure that an organization may have taken, disaster may strike. The third domain, business continuity and disaster recovery provides knowledge of management techniques and technologies to recover from a disaster like a successful virus attack. Cryptography, the fourth domain, provides the science behind encrypting information so that it does not make sense even if it falls into the wrong hands. The fifth domain deals with risk management and provides a formal mechanism for managing risk. I.T. security managers should be aware of the myriad legal and compliance issues that they have to face. That is why, the sixth domain of information security relates to knowledge regarding legal, regulations, compliance and investigations. The seventh domain discusses operations security from a day-to-day perspective. Domain eight is about physical (environmental) security. For example, the ability to provide for uninterrupted power supply is part of this domain. The ninth domain deals with the design aspects of security, while the tenth domain deals with telecommunications and network security.

Analyzing the ten domains of information security, it can be seen that they do not necessarily fall into the knowledge space of a single department or college. For example, the foundations of cryptography may fall under the purview of the computer science department, while disaster recovery may be done by departments such as safety science.

ANALYSIS OF CURRENT PROGRAMS

We have performed an Internet search to locate Information security curriculum. We used words like information security, management of information security, information assurance etc. for the search. Based on that, we discuss three issues related to those programs; the level, location, and structure of the program.

Level and Location

Data from forty U.S. universities was collected and analyzed. The universities had degree programs in information security and were identified through Google search. Of these, 21 universities had undergraduate degree programs, 36 had master's level programs, and 13 had Ph.D. programs. There was very little inter-departmental collaboration in these degree programs. Practically all the degree programs were located either in the information systems department or the department of computer science.

Structure of the coursework

After analyzing the coursework, we have identified nine themes in the information security curriculum for undergraduate and graduate programs. These themes were based on the commonality of the course content. The themes are shown in Figure 1.

Theme 1: Information Systems and Technology

This theme provides the student with the grounding needed in the fundamentals of information technology. The courses in this theme can be grouped into three sub-categories; courses related to programming, database management systems and operating systems.

The programming courses were mostly on object oriented programming and current programming languages and architectures or platforms like Java.

The database management courses typically included a database design and implementation course. The implementation courses almost definitively cover SQL. However, many schools have more advanced courses that include physical database design and transaction processing. Depending on the orientation of the program, concepts such as transaction processing may be extremely important particularly when the course relates to controls. For example, security related to financial controls may benefit significantly from students having knowledge of transaction processing. Other courses related to data warehousing and data mining have also been used in the information security curriculum. Data mining in particular may be extremely useful in information security curriculum for two reasons; first data mining may lead to significant security and privacy breaches and second data mining itself may be useful to unearth potential security violations (Mena, 2003). Similarly, the structure and design of distributed database systems becomes important from a security standpoint because of the potential database breach. For example, in a clustered system not all the servers may be equally protected, and in a distributed database system how they are all equally protected becomes an important concept.

A second group of courses in this category is related to operating systems. Particularly interesting was the focus on the UNIX operating system, and on multi-processor operating systems. Other courses in this category were about wireless networking and mobile computing as well as modeling and simulation.

Theme 2: Internet Technology

The internet technology theme courses focused on the technical aspects of the Internet as well as the applications. Courses such as Internet Services and Protocols cover many aspects of TCP/IP and DNS. However, it may also cover courses related to Voice-Over-IP protocols. Other technical courses focused on web development. Applications oriented courses discussed the business aspects of electronic commerce.

Theme 3: Cryptography

Courses on cryptography take two distinct approaches. The first, relate to fundamental development in cryptography and cover the mathematical aspects of cryptography. For example, the Feistel Cipher Structure (Stallings, 2010) that provides the underlying structure for encryption algorithms like the DES can be discussed in courses with a mathematical orientation. Other mathematical topics covered are probability theory and information theory, including concepts such as entropy. Such courses also cover abstract algebra concepts like Groups, Rings and Fields. Complexity and Number Theory are two of the other topics frequently covered in this group (Menzes, Oorschot, and Vanstone, 1997).

The applied orientation for cryptography focus primarily on the fundamental encryption methodologies like substitution, transposition, running key cipher etc. The differences between symmetric and asymmetric keys and the application and management of cryptography are all part of this group. Some encryption alternatives like steganography and watermarking are discussed in these courses.

Theme 4: Legal and Social Informatics of Security

Information security programs that are more oriented toward information security management include this theme. Also, security courses related to Criminal Justice may use courses in this theme. Courses in this theme can be categorized into the legal and ethical aspects of security. Legal aspects of computer security cover a wide variety of U.S. and international laws. Some significant U.S. laws that are covered in this category include the U.S. Intellectual Property laws, privacy laws and various crime laws. The Digital Millennium Copyright Act (DMCA) of 1998 is an example of a law discussed under intellectual property. Similarly, Children's Online Privacy Protection Act (COPPA) and the Health Insurance Portability and Accountability Act (HIPAA), are example of privacy laws. The Computer Security Act of 1987 and the Sarbanes-Oxley Act of 2002 are examples crime laws that are taught in these courses. Examples of European laws that may be taught are the Anti-terrorism, Crime and Security act 2001 that gives the UK government additional powers to seize terrorist funds.

Closely related to the legal issues are courses related to I.T. controls. Examples of control frameworks are COBIT (Control Objectives for Information and Related Technology), that contains key control objectives as well as provides a life cycle of planning for internal audit.

Theme 5: I.T. Security Management

Courses in this group focus strongly on the management aspects of IT security. These discussions include how to create a strategic plan for I.T. security. Also, planning for contingencies that include business impact analysis and incidence response is part of the courses. Any management oriented course in I.T. security will be incomplete without discussion on the development and implementation of an Enterprise Information Security Policy (EISP) (Whitman and Mattord, 2008).

Risk management forms a core component of the management oriented security courses. A wide array of risk management concepts that include how risk is identified and assessed and various risk control strategies like risk avoidance, mitigation etc. are typically included in these courses. Some widely used risk management models like OCTAVE or the NIST SP 800-26 security self assessment guide for information technology systems should be part of this section.

Managing an information security project requires having many of the common skills and methodologies required for managing any other project. However, I.T. security projects also have a certain sense of criticality. Courses in this section include various project management knowledge areas identified in the project management book of knowledge (PMBoK). Examples of such knowledge areas are project integration, quality, procurement etc.

Theme 6: Network Defense

The network defense courses deal with a wide variety of attack threats like viruses, worms, Denial-of-Service attacks etc. A wide variety of defense mechanisms like design, placement and configuration of firewalls, setting up Virtual Private Networks (VPNs) are part of these courses. Preventive measures on Intrusion Detection System (IDS) and how to capture packets and perform packet analysis, and how to respond to incidents should also be part of these courses. Courses in this category should also be very hands-on lab oriented courses.

Theme7: Computer Forensics

Computer forensics combines law and computer so that data from various types of systems and wireless devices can be collected in a manner that is admissible in the court of law (http://www.us-cert.gov/reading_room/forensics.pdf, 2008). Therefore computer forensics will include elements of law as well as how evidence is collected. This includes collecting and analyzing data from log files, investigating network traffic, investigating web attacks including SQL-injection attacks, investigating internet and e-mail attacks. Many corporate espionage investigations and child pornography investigations fall under this category as well.

CONCLUSIONS

This research has classified the coursework used in various universities across the U.S. for information security curriculum and grouped them into themes based on commonality of the courses. These themes should be considered as the starting point for any discussion. Depending on the orientation of the I.T. security program and the background of the students, one or more of these themes may be emphasized. For example, if students have significant I.T. knowledge or have a background in that area, then courses in the information systems and technology theme may be deemphasized. I.T. security programs that are more criminal justice oriented will most likely emphasize themes on legal and social informatics as well as computer forensics. Theoretical computer science programs may have the same themes as more applied programs as like Information Systems, however may explore and emphasize the mathematical aspects of computer security like cryptography to a great extent. The size of the program will also influence the selection of themes. For example, a certificate program may simply focus on a single theme like computer forensics.

Overall, the program will determine how to combine the themes. Given the rapid growth in technology, the nature of security will also evolve. However, it is expected that the fundamental themes will remain time-invariant for some time in the future.

Theme 1: Information Systems and Technology
Programming Concepts and Languages
Object Oriented Programming
Database Design and Implementation
Transaction Processing
Data Warehousing and Data Mining

Theme 2: Internet Technology
TCP/IP and DNS
Internet Services
VOIP
Web Development
Wireless

Theme 3: Cryptography
Cipher Structures
Probability and Information Theory
Groups, Rings and Fields
Complexity Theory
Cipher Theory
Cryptographic Algorithms

Theme 4: Legal and Social Informatics of Security
Intellectual Property Laws
Children’s Protection Act
Health Insurance Portability and Accountability Act (HIPAA)
European Laws

Theme 5: I.T. Security Management
Contingency Planning
Enterprise Security Policy development
Risk Management
OCTAVE /NIST Models
Security Project Management

Theme 6: Network Defense
Virtual Private Networks
Intrusion Detection Systems
Packet Analysis

Theme 7: Computer Forensics
Log File Analysis
Network Traffic Investigation
E-mail Investigations

Figure 1: I.T. Security Themes

REFERENCES

1. Chow, R. et al., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control", ACM Cloud Computing Security Workshop, 2009, pp. 85-90.
2. Ferraiolo, F.D., Kuhn, D.R., "Role-Based Access Controls, Proceedings of the 15th national Computer Security Conference, Baltimore, MD, pp. 554-563, 1992 (revised 2009).
3. Gregory, P., CISSP Guide to Security Essentials, Course Technology, Boston, 2010.
4. Holden, G., Guide to Network Defense and Countermeasures, Course Technology, Boston, 2003.
5. Mena, J., Investigative Data Mining for Security and Criminal Detection, Elsevier Science, Burlington, MA, 2003.
6. Menezes, A.J., Oorschot, P.C. van, Vanstone, S.A., Handbook of Applied Cryptography, CRC Press, Boca Raton, 1997.
7. Parnas, D.L., Madey, J., Asmis, G.J.K., Assessment of safety-critical software in nuclear power plants, Nuclear Safety, Vol. 32, No. 2, pp. 189-198, 1991.
8. Stallings, W, Cryptography and Network Security, Prentice Hall Press, Upper Saddle River, NJ, 2010.
9. Whitman, M.E., and Mattord, H., Management of Information Security, Second Edition, Course Technology, 2008.