AC 2008-1592: INTEGRATING THE SECURITY+ EXAM OBJECTIVES INTO INFORMATION TECHNOLOGY CURRICULA

Akram Al-Rawi, KFU

Akram Al-Rawi is a Professor of Computer Science at King Faisal University, Saudi Arabia. He has worked at several academic institutions of which the last three were Zayed University, University of Missouri- Columbia, and Columbia College, MO. His teaching interests include programming languages, networks, logic design, and computer architecture. His research interests include computer simulation, wireless, security, embedded systems, and curriculum design. He holds certifications in A+, Network+, Sun Certified Java Programmer, ICDL, i-Net+, Server+ and CCAI.

Azzedine Lansari, Zayed University

Azzedine Lansari received a PhD in Bioengineering from North Carolina State University in 1992. From 1992-1998, he was a senior researcher at Computer Sciences Corp. and MANTECH, Inc. He joined Zayed University in August 1998. Currently he is an associate professor of Information Technology. His teaching interests include instructional technology and statistical modeling. His research interests include systems modeling, educational technology and curriculum design.

Integrating the Security+ exam Objectives into Information Technology Curricula

Abstract

Security is a fairly new field in the information technology (IT) knowledge domain and has recently become a critical area in IT curricula. While some IT programs in the US offer only one security course in their undergraduate programs, others offer up to four courses. The first objective of this paper is to review the offering of security courses in undergraduate programs and then examine their content to investigate the possibility of integrating the CompTIA Security+ exam objectives. The second objective of this paper is to review industrial certificates that are currently available in security and examine their possible integration in an IT curriculum. The last objective of this study is to compare the objectives of the Security+ exam with the two Cisco Networking Academy security courses. The Security+ certification exam objectives cover most of the basics of security and they can be integrated into the first security course of most IT programs. Finally, a master course syllabus that covers the Security+ exam objectives is developed to map each course objective with its corresponding certification objective. It is anticipated that colleges and universities will benefit from this study by using the proposed course syllabus as a framework for integrating the Security+ certification exam objectives into their curriculum.

Introduction

Certification establishes a standard of competency in specific areas of the IT field which helps industry determine whether prospective employees meet the required credentials for different job roles. Therefore employees holding the required IT certificates may require less training or even no training during the initial employment period. Hence, some job criteria require individuals to be certified in order to be considered for employment. To the certified individual, certification provides a greater sense of confidence in their abilities and a measure of professional expertise and understanding of the job and products used in that role. It is for these reasons that certification is becoming increasingly popular and in high demand. Some IT certificates are specific to a narrow field or even individual products. The aim is to provide targeted skills that have immediate applicability in the workplace[1,2].

The IEEE and ACM recognize the importance of certification and provide its members with over six hundred online courses leading to professional certifications, such as CompTIA Network+ and Cisco CCNA. Moreover, ACM has developed a K-12 computer science curriculum[3] that recommends three IT certifications; the A+ Certified Technician, the i-Net+, and the Certified Internet Webmaster. The ACM report suggests that students who complete certification courses should be encouraged to take the corresponding exam as proof of acquired knowledge.

Academic institutions worldwide are constantly trying to refine or even reinvent their Information Technology (IT) curricula to address the needs of industry and government. As many new IT curricula emerge, a number of them do not satisfy well recognized standards and sometimes even lack critical curricular components. Furthermore, a highly competitive IT global

market is putting pressure on colleges and universities to include IT certification in their curricula. The ACM IT 2005 Curriculum includes 23 hours out of 281 hours in information assurance and security, in the IT body of knowledge[4]. The report also includes an additional two hours under networks, called network security. While the IT 2005 curriculum report defines each area of the IT body of knowledge in detail, the contents of security courses in different universities varies substantially. The numbers of courses offered by different universities also vary substantially. For example, some colleges offer only one course while others offer up to four courses. Several IT programs in the US are examined to investigate what courses they offer in security and the content of their courses.

IT 2005 Model Curriculum

The IT 2005 Model Curriculum[4] lists one major area called information assurance and security in the IT body of knowledge. The curriculum also includes security under the Networking body of knowledge. The number of hours dedicated to security in the IT model curriculum is 25 hours out of 281 hours, which represents the core of the curriculum. A three credit-hour course generally requires 45 hours of instruction. This means the IT model curriculum includes approximately two credit-hours of security in its core curriculum. The security topics which are included in the model curriculum are summarized next.

The Information Technology Body of Knowledge

The IT 2005 report divides the IT body of knowledge in to twelve areas, these are:

- ITF. Information Technology Fundamentals (33 core hours)
- HCI. Human Computer Interaction (20 core hours)
- IAS. Information Assurance and Security (23 core hours)
- IM. Information Management (34 core hours)
- IPT. Integrative Programming & Technologies (23 core hours)
- NET. Networking (20 core hours)
- PF. Programming Fundamentals (38 core hours)
- PT. Platform Technologies (14 core hours)
- SA. System Administration and Maintenance (11 core hours)
- SIA. System Integration and Architecture (21 core hours)
- SP. Social and Professional Issues (23 core hours)
- WS. Web Systems and Technologies (21 core hours)

The core curriculum includes one area in information security and one area in networks as shown below:

IAS. Information Assurance and Security (23 core hours)

- IAS1. Fundamental Aspects (3)
- IAS2. Security Mechanisms (Countermeasures) (5)
- IAS3. Operational Issues (3)
- IAS4. Policy (3)
- IAS5. Attacks (2)
- IAS6. Security Domains (2)
- IAS7. Forensics (1)
- IAS8. Information States (1)

- IAS9. Security Services (1)
- IAS10. Threat Analysis Model (1)
- IAS11. Vulnerabilities (1)

NET. Networking (20 core hours)

- NET4. Security (2)

Since IT systems are increasingly under attack, the knowledge of Information Assurance and Security (IAS) is of paramount importance to the profession of IT. The IT professional must understand, apply, and manage information assurance and security in computing, communication, and organizational systems. It is also important for the IT professional to provide users in an organization with a framework to be sufficiently aware of security issues for the users to be an asset to the organization rather than a liability. IAS includes operational issues, policies and procedures, attacks and defense mechanisms, risk analyses, recovery, and information security. The learning outcomes of each area are described in the IT 2005 model curriculum[4].

CompTIA Security+ Certificate Objectives

The Security+ exam was developed in 2002 to address the rise of security issues and validate the foundational knowledge of security professionals. Security+ objectives were derived through input from the government, academia and the IT industry. Security+ validates knowledge of communication security, infrastructure security, cryptography, operational security, and general security concepts. It is a vendor-neutral certification that is taught in colleges, universities and commercial training centers around the world. Although not a prerequisite, it is recommended that Security+ candidates have at least two years on-the-job experience in networking with an emphasis on security. The Network+ certification is also recommended. CompTIA's Security+ exam (SY0-101) is the sole requirement for information technology (IT) professionals seeking the association's Security+ certification.

Security+ SY0-101 Exam Details

The Security+ exam consists of 100 multiple choice questions and the allocated time to finish the exam is 90 minutes. These questions are drawn from the five Security+ certification domains in proportion to predefined exam weightings (shown in Table 1). The exam objectives are clear and easy to follow. Unlike Cisco CCNA exam, the time allocated for the exam is enough to complete the exam. However, unlike all other CompTIA certification exams, the passing score is 764/900 (85%) which makes it harder to pass. This makes the integration of the certification exam in a Security course rather challenging as some students may be able to pass the course but may not be able to pass the certification exam. This is also true with Cisco networking academy courses, most students manage to complete the Networking Academy courses CCNA1-CCNA4 successfully but are not able to pass the CCNA certification exam which also requires 85% to pass. However, with the CCNA exam the time is the most critical factor, it is very hard to complete the exam in 90 minutes and achieve a score of 85%. The format of the CCNA exam (640.802) also contributes to the difficulty of passing the exam.

Table 1: Security+ Exam Domains	
Security+ Certification Domain	**Exam Weight**
1.0 General Security Concepts	30%
2.0 Communication Security	20%
3.0 Infrastructure Security	20%
4.0 Basics of Cryptography	15%
5.0 Operational / Organizational Security	15%

Like most IT certification exams, testing centers administer SY0-101 electronically. Test scores provided by the computer at the end of the exam, fall somewhere in the range of 100-900, where 764 (85%) is the minimum passing score. The certification exam may be taken through one of two testing partners, Pearson VUE or Thomson Prometric. Both vendors administer the same exam and charge the same fee ($250). The details of the Security+ objectives can be found at the CompTIA home page. For the purpose of this study only the main topics or domains are listed below.

Domain 1.0 – General Security Concepts

1.1 Recognize and be able to differentiate and explain the access control models
1.2 Recognize and be able to differentiate and explain the methods of authentication
1.3 Identify non-essential services and protocols and know what actions to take to reduce the risks of those services and protocols
1.4 Recognize the following attacks and specify the appropriate actions to take to mitigate vulnerability and risk
1.5 Recognize the following types of malicious code and specify the appropriate actions to take to mitigate vulnerability and risk
1.6 Understand the concept of and know how to reduce the risks of social engineering
1.7 Understand the concept and significance of auditing, logging and system scanning

Domain 2.0 – Communication Security

2.1 Recognize and understand the administration of remote access technologies
2.2 Recognize and understand the administration of email security concepts
2.3 Recognize and understand the administration of the Internet security concepts
2.4 Recognize and understand the administration of the directory security concepts
2.5 Recognize and understand the administration of the file transfer protocols and concepts
2.6 Recognize and understand the administration of the wireless technologies and concepts

Domain 3.0 Infrastructure Security

3.1 Understand security concerns and concepts of the network devices

3.2 Understand the security concerns for the network media
3.3 Understand the concepts behind different kinds of Security Topologies
3.4 Differentiate the types of intrusion detection, be able to explain the concepts of each type, and understand the implementation and configuration of each kind of intrusion detection system.
3.5 Understand the concepts of Security Baselines, be able to explain what a Security Baseline is, and understand the implementation and configuration of each kind of intrusion detection system.

Domain 4.0 Basics of Cryptography

4.1 Be able to identify and explain the different kinds of cryptographic algorithms
4.2 Understand how cryptography addresses security concepts
4.3 Understand and be able to explain the concepts of PKI (Public Key Infrastructure)
4.4 Identify and be able to differentiate different cryptographic standards and protocols
4.5 Understand and be able to explain the concepts of Key Management and Certificate Lifecycles

Domain 5.0 Operational / Organizational Security

5.1 Understand the application of the concepts of physical security
5.2 Understand the security implications of disaster recovery
5.3 Understand the security implications of business continuity
5.4 Understand the concepts and uses of policies and procedures
5.5 Explain the concepts of privilege management
5.6 Understand the concepts of forensics
5.7 Understand and be able to explain the concepts of risk identification
5.8 Understand the security relevance of the education and training of end users, executives and human resources.
5.9 Understand and explain the documentation concepts

A comparison of the Security+ topics and the IT 2005 model curriculum indicates that the Security+ cover more topics in security than the IT 2005 core curriculum. This indicates that the Security+ objectives cover almost all the topics of the IT 2005 core curriculum in security. The IT 2005 model curriculum report recommends one course in security in the core curriculum, and four courses as electives in security. Two more courses are recommended under network. The names of the seven courses are shown below[4]:

IT410. Information Assurance & Security (Core Curriculum)
IT311. Cryptography
IT312. Forensics and Incident Response
IT313. Biometrics
IT314. Security Policies and Procedures
IT344. Data Compression
IT345. Network Security

The IT 2005 model curriculum includes only one course (IT410) in its core curriculum[3]. However, the core curriculum is very limited with approximately 19 credit hours. This course is a survey of the Security+ topics and can be integrated within a course which covers the objectives of the Security+ exam.

Security Offering in US Institutions

Several IT programs were reviewed to examine their offerings in Security. While in programming we found that almost all institutions offer two to three courses in programming, such as CS1 & CS2, in Security there seems to be no conclusions as to how many courses are needed. Some institutions offer one course in Security, others offer two, and others may offer up to four courses. For example, East Carolina University (http://www.ecu.edu) offers four courses, the first course is mapped to cover the CompTIA Security+ certificate objectives[5,6], the second[7] is Principles of Information Security, the third course is introduction to intrusion detection and the fourth is in information assurance technologies. The syllabus of the first course did not show if students have to take the Security+ exam or not, though it indicates that Cisco CCNA is a prerequisite for most of their information technology program courses.

Another example is Kennesaw State University (http://www.kennesaw.edu), it offers a major in Information Security and Assurance. The curriculum includes thirteen courses in security; nine courses in the core curriculum and four electives. However, there was no indication as to the possibility of integrating IT certificates in any courses of the curriculum. The CSIS department, on the other hand, offers its own certificate in Information Security & Assurance by completing fifteen credit hours in information security.

Cisco Networking Academy & Security

Cisco Networking Academy offers five courses in security; Fundamentals of Network Security, Fundamentals of Network Security: PIX, Fundamentals of Network Security: Router, Network Security 1, and Network Security 2. Each course requires 75 hours of instruction and it includes a lab component. The five courses put emphasis on packet filtering and router/switch configuration. The first Network Security course focuses on network security concepts and the second Network Security course include a component about intrusion detection. Though the five courses are very useful, none of them can be effectively integrated into a general IT security course.

CISSP (Certified Information Systems Security Professional)

The International Information System Security Certification Consortium $(ISC)^2$ was founded in 1989. This not-for-profit organization manages the CISSP (Certified Information Systems Security Professional) certification. This advanced-level certification is meant for IT security professionals with the following level of experience: a minimum of four years of professional experience in the field of information security. A bachelor degree can substitute for one of these required years. Additionally, a Master degree in Information Security can substitute for one year towards the four-year requirement. The experience requirement essentially forms the prerequisite for this vendor-neutral certification, although $(ISC)^2$ other, lower-level certification, the SSCP

(Systems Security Certified Practitioner), is also recommended as a prerequisite. Though, this is a well known certificate but it can not be integrated into an IT course.

Cisco Certified Security Professional (CCSP)

Cisco offers several certificates such as CCNA, CCNP, and CCSP. However, the CCSP certificate requires five exams: 642-501 (Securing Cisco IOS networks), 642-511 (Cisco Secure VPN), 642-521 (Cisco Secure PIX Firewall Advanced), 642-531 (Cisco Secure Intrusion Detection System), and 642-541 (Cisco SAFE Implementation). Though CCSP is becoming very popular, it cannot be easily integrated into an IT course. Cisco Networking Academy offers five courses in security where each course requires 75 hours of instructions to prepare students for this certificate.

Integrating CompTIA Security+ Certificate Objectives into an IT Course

The Security+ Certificate Objectives can be integrated into a three to four credit hour course in Network Security Fundamentals. The following sections give a partial description of the master syllabus of the Network Security Fundamentals course.

I. Course Purpose

The goal of this course is to provide the student with a fundamental understanding of computer network security principles and implementation scenarios. A variety of security topologies will be presented, as well as technologies and concepts used for providing secure communications channels and secure internetworking devices and network mediums. Moreover, a lab component reinforces concepts and theories presented in the course.

II. Course Objectives

Upon completion of this course students will be able to:

1. Explain the goals and factors involved in a network security strategy.
2. List and explain the various means to insure authentication through something one knows, something one has, or something one is.
3. List and explain computer and network attacks, including DOS, DDOS, spoofing, protocol attacks, and social engineering.
4. List and explain the various protocols and applications used in remote access, such as L2TP, PPTP, SSH, TACAS+, and VPN.
5. Explain the concepts configuration for email, email security methods, and email vulnerabilities and dangers.
6. Explain the concept of web security and explain several security implementations such as SSL/TLS, HTTPS, and web security vulnerabilities.
7. Discuss directory and file services issues that are related to a secure network.
8. Explain the concepts of wireless data transfer security issues and techniques used to secure wireless data, such as WAP, WTLS, and WEP.
9. Explain the security issues related to network devices such as routers, switches, and firewalls.
10. Explain and model the different strategies used to lessen catastrophic media disaster and encrypt data.

11. Explain and model computer network security perimeters.
12. Define intrusion detection system (IDS) and honey pot, and provide examples of several detection methods.
13. Explain the need and implementation methods of security baselines, and Provide several examples.
14. Understand and demonstrate the use of cryptography, PKI certificates, and hash, asymmetric and symmetric algorithms.
15. Identify and explain physical security and natural disaster countermeasures.
16. Correctly identify and explain disaster recovery techniques and business continuity strategies.
17. Explain basic computer forensics and risk management.
18. To pass the CompTIA Security+ exam (85% minimum)

III. Course Content

This course is an introduction to Network and Information Security. There are many terms and concepts that the student must master. Weekly exams will cover content from that week's chapter(s), lab material, and on-line supplemental material. The final exam is a comprehensive exam and will be taken in a testing center. The passing score for the final exam is 85% and the exam fee is $250. Table 2 shows the weekly coverage of the course topics along with the distribution of the Security+ certification objectives.

Table 2. Network Security Fundamentals Master Syllabus

Week #	Topics/Chapter	Certification Objectives #
1	Ch.1 Information Security Fundamentals (pp.1-28)	
2	Ch.2 Attackers and Their Attacks (pp.29-68)	1.4, 1.5, 1.6
3	Ch.3 Security Basics (pp.69-102)	1.1, 1.2, 1.7, 3.5
4	Ch.4 Security Baselines (pp.103-137)	1.3
5	Ch.5 Securing the Network Infrastructure (pp.139-188)	3.1, 3.2, 3.3, 3.4
6	Ch.6 Web Security (pp.189-224)	2.2, 2.3, 2.5
7	Ch.7 Protecting Advanced Communications (pp.225-269)	2.1, 2.4, 2.6
8	Ch.8 Scrambling Through Cryptography (pp.271-305)	4.1, 4.2, 4.4
9	Ch.9 Using and Managing Keys (pp.307-339)	4.3, 4.5
10	Ch.10 Operational Security (pp.341-379)	5.1, 5.2, 5.3, 5.4, 5.5
11	Ch.11 Policies and Procedures (pp.381-416)	5.7
12	Ch.12 Security Management (pp.417-444)	5.6, 5.8, 5.9
13	Ch.13 Advanced Security and Beyond (pp.445-474)	
14	Review of the Security+ Exam(from the reference CD)	
15	Final Exam, Comprehensive, Security+ exam	

IV Textbook[4] / Lab[5]

Ciampa, Mark, Security+ Guide to Network Security Fundamentals, Course Technology, 2005. http://www.course.com

Cretaro, Paul, Lab Manual for Security+ Guide to Network Security Fundamentals, 2nd ed., Course Technology, 2005. http://www.course.com

Reference book

Pastore, Mike and Dulaney, Emmett, CompTIA Security+ Guide, Deluxe ed., Wiley publishing, 2006 http://www.cybex.com

Note about the Textbook and Reference

The reference book may help the student pass the Security+ certification exam, however it is not written as a textbook. Students are encouraged to read both books simultaneously.

Grading Policy

In order to complete the course successfully, student must pass the Security+ certification exam (85% or better). The course grade components are calculated as follows:

1. Thirteen Chapter Quizzes (40%)
2. Lab Projects (20%)
3. CompTIA Security+ exam (40%)

Conclusions

Revising the Information Technology curriculum and keeping it current to meet the demands of the IT market remains a challenging experience. Although passing a vendor specific certification exam is not an explicit goal of many IT programs, students should look into acquiring IT certificates in order to be prepared to join a competitive job market. Employers prefer to hire graduates which hold IT certification to minimize on the job training. A review of the IT 2005 model curriculum revealed only one security course in the core curriculum and four elective courses. An examination of US universities indicated that their offering in security varies. Two examples were discussed: East Carolina University and Kennesaw State University. An interesting finding was that some universities are starting to offer a major in Information Security & Assurance. The requirements of popular Security Certificates were discussed, and the possibility of integrating IT certificate objectives in IT courses was investigated. It is concluded that the only security certificate which can be effectively integrated into a single IT course is the CompTIA Security+ certificate. However, even though the objectives of the Security+ can be integrated into one three to four credit IT course, passing the certification exam will be a challenge because the current passing score is 85%. Colleges who aspire to include IT certification tracks in their Security courses will benefit from this study by using the proposed master course syllabus as a model for integrating the Security+ certification exam objectives.

Bibliography

1. Zeng, Fanyu, "A new approach to integrate Computer Technology Certification into Computer Information System Programs", Proceeding of the 2004 American Society for engineering education annual conference & Exposition", Session 2558. http://www.asee.org

2. Koziniec, Terry & Dixon, Michael, "ICT Industry Certification: Integration Issues for post Secondary Educational Institutions in Australia", InSITE, June 2002. http://proceedings.informingscience.org/

3. A Model Curriculum for K-12 Computer Science: Final Report of the ACM K-12 Task Force Curriculum Committee, October 2003. http://www.acm.org/education/curric_vols/k12final1022.pdf

4. IT Model Curriculum 2005, http://www.acm.org/education/curric_vols/IT_October_2005.pdf

5. Ciampa, Mark, "Security+ Guide to Network Security Fundamentals", 2nd edition, Course Technology, 2005 http://www.course.com

6. Cretaro, Paul, "Lab manual for Security+ Guide to Network Security Fundamentals", 2nd edition, Course Technology, 2005. http://www.course.com

7. Whitman, Michael & Mattord, Herbert, "Principles of Information Security, Course Technology, 2003.