# Network Security Course Model

Mariana Hentea, Ph.D.

Assistant Professor, Information Systems and Computer Programming, Purdue University Calumet

2200 Wicker Avenue, Hammond, IN 46323, Telephone: 219-989-3225, Email: henteam@calumet.purdue.edu, Fax: 219-989-3187

Susan E. Conners, Ph.D.

Associate Professor, Information Systems and Computer Programming, Purdue University Calumet

2200 Wicker Avenue, Hammond, IN 46323, Telephone: 219-987-2605, Email: conners@calumet.purdue.edu, Fax: 219-987-2858

## ABSTRACT

The objective of this paper is to present a model for an undergraduate Network Security Course. The components in the model are designed to be core concepts and do not necessarily represent any particular vendor's system. It is a generic course model with emphasis on security issues and technologies. The primary components of the course and the importance of the topic being added to core curricula are discussed in the paper.

## INTRODUCTION

The growth of computer networks has been phenomenal over the last several years and they are a major communication link for people around the world. Computer networks and their related technologies have evolved at a rapid pace with the hardware and software constantly changing and challenging networking professionals to keep pace.

These networks are used by government, public and private entities to communicate with the world. Securing the networks has become of paramount importance. "The terrorist attacks of last September permanently changed the terms of debate for subsequent discussions of IT security and the technical response to potential terrorist threats", (Coffee, p. 25,2002). There is currently a national discussion on how best to secure government networks.

The security of corporate networks is of equal concern. "CIOs are most worried about internal and external security breaches and cyber terrorism", (Kirkpatrick, p.67, 2002). The nation's economy relies on business networks being operational and secure. The failure or compromising of large-scale corporate networks will severely hamper business operations.

In addition to the larger issues of government and corporate network security, the networks accessed for personal reasons should be equally secure. The old conventional wisdom of find the best hackers and hire them to secure your network is not a wise path to follow. Clearly, this topic is an educational priority for IT programs. These courses must be offered in higher education programs with trained educators and researchers working in this field.

This paper discusses a model for a network security course in a curriculum, the course model, the specific components of the model, and the technologies used to teach the course at the undergraduate senior 400 level. This course supports scholarly education and does not focus on topics for certification exams.

## OVERVIEW OF NETWORKING CURRICULUM

The current program that utilizes this course is a four-year baccalaureate degree in computer technology with a specialization in systems and networking. The overall program includes core technical courses, general education courses, and a specialization sequence in networking courses. The core technical courses include programming, systems analysis, web development, and database. The general education courses consist of math, English, physics, economics, communications, humanities and social science. The networking courses are comprised of operating systems classes, data communications, local area networks, wide area networks, hardware and software evaluation, and network security.

The issue of security covers multiple areas and there are security components in applications, network software, the operating system, hardware, and others. All of these forms of security are important to the overall security of information, which is what is protected [Maiwald, p. XXVI, 2001]. Throughout the curriculum, security is discussed as a component of each of the various courses on operating systems, local area networks, wide area networks, and system administration. Students are continually taught the importance of security at all levels of the courses and the programs.

The significance of the topic of network security requires a separate course to integrate the components of the previous courses and build upon that knowledge. This is not an introductory level course. The course model is presented with the understanding that the prerequisite courses have been completed and the students have studied various aspects of security in their other courses. These prerequisite courses discuss the details of security as it applies to the specific topic taught in the course. The network security course is taught in the senior year of the program and requires students to integrate and synthesize the prior knowledge. Placing the course in the senior year prepares students to enter the workforce with the most recent issues on security. The course model is constructed to provide information for other programs wishing to develop a similar course.

## OVERVIEW OF COURSE MODEL

The objective of the class is to allow students to obtain the skills required to pursue a job in all areas of the Security Industry: Consulting (Professional) Services, Developers for Security Products, and Managed Security Service Providers. The course provides an integrated, comprehensive, up-to-date coverage of the techniques, security tools, and applications vital to Internet applications and networking. The classroom instruction provides a practical approach of both the principles and practice of network security. Topics include system-level security issues, types of attacks, information security services, information security process, and information security best practices such as use of firewalls, routers, and trusted systems, monitoring and detection techniques, virtual private networks, E-commerce security needs, encryption, intrusion detection, and configuration recommendations for common operating systems (Windows NT, Unix, Linux, and Windows 2000) as well as security trends and new technologies (see Appendix A).

Students are taught ethics and professionalism as required of the work force in the information security industry. The ethics imply integrity, trust, correctness, assurance and confidence that no intentional attacks are made against any system. They also learn key architecture issues for securing the network and Internet connection. In addition, students learn how to set up and work with firewalls, authentication and encryption techniques, access controls, discovering and handling an actual attack, recovery from security breaches, and prevention of hacker

usoaoyousa

site, installation in the designated machines, and verification of the updating process as well as testing the new features supplied with the most current version of the software. When implementing a security policy for a lab assignment that used Microsoft Windows 2000, students assessed the security flaws published by various sources (see Appendix C) before planning and writing the security policy. This is the basis of the future security professional awareness for checking the most recent published vulnerabilities.

In addition, the Web is used by students for getting informed about the quality ratings of the products used in the information security industry including the products used for the lab assignments and demonstration of the technologies. These all concur to advantages for students such as easy and quick access to information, familiarity with the real business problems to be solved, etc.

The web based system Blackboard (www.blackboard.com) is used as a mechanism of delivering the course material, instructor's notes, homework and lab assignments, and delivery of messages.

## SUMMARY AND CONCLUSIONS

The course model discussed provides an example for a network security course. The importance of these types of courses must be emphasized in Information Technology programs to provide government and business the trained professionals required to secure their networks. In light of recent events, this topic has gained national prominence in government and corporate circles. Academic programs and departments should work with government and industry to educate IT students and professional on network security. This model is presented to assist other institutions that wish to incorporate a network security course into their curriculum.

This course model integrates specific skills from lower level courses and integrates them to form a knowledge base for further study of network security. The course covers techniques, security tools and applications that are essential to every business and computer system. In addition to technical skills, the topics of ethics and professionalism are addressed. The components of the course include also aspects of the security model, authentication mechanism, encryption, and interfaces for MS Windows 2000, Unix, and Linux operating systems. The technologies utilized in the class are hardware (firewalls and routers with firewall capabilities) as well as software products for network security. In addition, automated tools for penetration testing are used for the verification of the implemented security policy.

In conclusion, the importance of the network security course and other courses described in the paper are aligned with the national, regional, and local security concerns. Models for security courses and programs of study must be developed to meet this challenge. Consequently, all Information Technology and related programs need to include the network security training in their curricula. This is an opportunity for academic programs to provide government and industry with trained IT professionals ready to meet the security challenge.

## APPENDIX A: TOPICS TAUGHT IN CLASS

1. Information Security Basics
2. Types of Attacks
3. Information Security Services
4. Legal Issues in Information Security
5. Policy
6. Managing Risk
7. Information Security Process
8. Information Security Best Practices
9. Internet Architecture
10. Virtual Private Networks
11. E-Commerce Security Needs
12. Encryption
13. Hacker Techniques
14. Intrusion Detection
15. UNIX Security Issues
16. Linux Security Issues
17. Windows NT Security Issues

18. Windows 2000 Security Issues
19. SNMP v3
20. Biometric Systems
21. Information Security Products Evaluation
22. Current and Future Information Security Industry Trends

## APPENDIX B: SUGGESTED TOPICS FOR PRESENTATION

1. Data Encryption Standards
2. General Authentication Techniques
3. Network Backups
4. Types of Attacks
5. Security Issues for Wireless Networks
6. Security Devices and Measures
7. Firewalls and Building Internet Firewalls
8. Recent Advances in Intrusion Detection
9. Biometric Systems
10. Security Architecture for Enterprise
11. Writing a Security Policy
12. Security Requirements for Systems
13. Virtual Private Networks (VPNs)
14. Router Attacks and Reconfiguration
15. Security Issues for Microsoft Windows 2000
16. Security Issues for Microsoft Windows NT
17. Security Issues for Linux and UNIX Systems
18. Security for Internet and Standards
19. Applied Cryptography
20. Recovery from Security Attacks
21. Prevention versus Detection
22. Web Security
23. SNMP Security Issues
24. Security Management
25. Electronic Mail Security
26. IPSec Standard Implementation
27. Passwords Vulnerabilities
28. Testing Network for Vulnerabilities
29. Auditing Techniques
30. Security Awareness Training
31. Server Security
32. Security Maintenance

## APPENDIX C: SUGGESTED WEB SITES

1. www.cerias.purdue.edu
2. www.cert.org
3. www.ietf.org/rfc
4. www.gocsi.com
5. www.securityfocus.com
6. www.snmp.org
7. http://csrc.nist.gov/icat
8. www.sans.org
9. www.nipc.gov
10. www.fedcirc.gov
11. www.sei.org
12. www.isalliance.org
13. www.antionline.com
14. www.loph2.com
15. www.infowar.com

## APPENDIX D: LIST OF HARDWARE AND SOFTWARE TO BE USED FOR THE LAB ASSIGNMENTS

1. 4 Cisco 2621 routers
2. 3 Firewall appliances (different technologies and manufacturers: Nokia, Global Technology Associates, SonicWall)
3. 6 3COM LAN switches
4. Hubs, cables, connectors, adapters
5. 25 Personal Computers
6. CheckPoint FireWall-1 Next Generation
7. Microsoft Windows 2000 Server Software
8. Microsoft Windows 2000 PC Software

9. Linux Red Hat  Software
10. Penetration testing tools (free download)
11. Intrusion Detection (free download)
12. Anti-virus software (free download).

## REFERENCES

Assaf, N., Luo, J., Dillinger, M. and Menendez, L., Interworking between IP         Security and Performance Enhancing Proxies for Mobile Networks, IEEE         Communications Magazine, May 2002, Vol. 40, No. 5, pp. 138-144.

Chang, R.K.C., Defending against Flooding-Based Distributed Denial-of-Service         Attacks: A Tutorial, IEEE Communications Magazine, October 2002, Vol. 40,   No. 10,   pp. 42-51.

Coffee, P., 2002, Focus on Identity, Vigilance. EWeek v19 n36, p.25. Ziff Davis Publications.

Cybenko, G., Giani, Annarita, Thompson, P., Cognitive Hacking: A Battle for the Mind, 2002,  COMPUTER, Vol. 35, No. 8, pp. 50-56.

Frischholz, R. W., Dieckmann, U., BioID: A Multimodal Biometric Identification System, 2000,         COMPUTER, Vol. 33, No. 2, pp. 64-68.

Jamsa, J., 2002, Hacker Proof, The Ultimate Guide to Network Security, Second Edition, Thomson Delmar Learning, United States.

Kara, A., Secure Remote Access from Office to Home, IEEE Communications Magazine, October 2001, Vol. 39, No. 10, pp. 68-72.

Kenneally, E., Who's Liable for Insecure Networks?, Computer, June 2002, Vol.    35, No.   6, pp. 93-95.

Kirkpatrick, T. A., 2002, Rethinking Risk, CIO Insight. September 2002, n18 Ziff Davis            Publications.

Klevinski, T. J., Laliberte, S., Gupta, A., 2002,  Hack I.T. – Security Through Penetration Testing, Addisson-Wesley, New York, New York.

Maiwald, E., 2001, Network Security: A Beginner's Guide, Osborne/McGraw-Hill, New York, New York.    Manikopoulos,    C.    and Papavassiliou, S., Network Intrusion and Fault Detection:    A Statistical Anomaly Approach, IEEE Communications Magazine, October    2002,    Vol. 40, No. 10, pp. 76-82.

Miller, S.K., Facing the Challenge of Wireless Security, 2001, COMPUTER, Vol. 34, No. 7, pp. 16-18.

Oppliger, R., Security at the Internet Layer, 1998, COMPUTER, Vol. 31, No. 9, pp. 43-47.

Pankanti, S., Bolle, R. M., Jain, A., Biometrics: The Future of Identification, COMPUTER, 2000, Vol. 33,        No. 2, pp. 46-47.

Papadimitratos, P. and Haas, Z.J., Securing the Internet Routing Infrastructure, IEEE         Communications Magazine, October 2002, Vol. 40, No. 10, pp. 60-68.

Phillips, P. J., Martin, A., Przybocki, M., An Introduction to Evaluating Biometric Systems, 2000,         COMPUTER, Vol. 33, No. 2, pp. 56-63.

Stallings, W., 2000, Network Security Essentials: Applications and Standards, Prentice Hall, Upper  Saddle River, New Jersey.

# Related Content

### Performance Optimization of DWT-Based Image Watermarking Using Genetic Algorithms
Ali Al-Hajand Aymen Abu-Errub (2009). *Utilizing Information Technology Systems Across Disciplines: Advancements in the Application of Computer Science  (pp. 210-221).*
www.irma-international.org/chapter/performance-optimization-dwt-based-image/30727

### What Will Entail Adoption of a Mobile Coaching Service?: The Case of Smoking Cessation Services
Silvia Cacho-Elizondo, Niousha Shahidiand Vesselina Tossan (2019). *Handbook of Research on the Evolution of IT and the Rise of E-Society (pp. 455-485).*
www.irma-international.org/chapter/what-will-entail-adoption-of-a-mobile-coaching-service/211628

### The Key Role of Interfaces in IT Outsourcing Relationships
Francois Duhamel, Isis Gutiérrez-Martínez, Sergio Picazo-Velaand Luis Felipe Luna-Reyes (2012). *International Journal of Information Technologies and Systems Approach (pp. 37-56).*
www.irma-international.org/article/key-role-interfaces-outsourcing-relationships/62027

### Barcodes vs. RFID and Its Continued Success in Manufacturing and Services
Amber A. Smith-Ditizioand Alan D. Smith (2018). *Encyclopedia of Information Science and Technology, Fourth Edition (pp. 5273-5284).*
www.irma-international.org/chapter/barcodes-vs-rfid-and-its-continued-success-in-manufacturing-and-services/184232

### Discovering Patterns using Process Mining
Ishak Meddahand Belkadi Khaled (2016). *International Journal of Rough Sets and Data Analysis (pp. 21-31).*
www.irma-international.org/article/discovering-patterns-using-process-mining/163101