A WEB SECURITY SYSTEM MODEL
TO ASSIST CIS/MIS COURSES DESIGN

Kuan C. Chen, Ph.D.
School of Management
Purdue University Calumet
E-mail: kchen@calumet.purdue.edu

ABSTRACT

This paper demonstrates a model of Web security system based on nowadays Web server management set up and theory. The relationships in the model are designed to be simple and functional and do not necessarily represent any particular Web security environments. It is meant to be a generic Web security system model with implications for MIS/CIS security course instructional design. It allows Web security instructors to move away from the discrepancy between the courses and body of knowledge. The interrelationships of five primary sectors that are at the Web security system are presented in this paper. This integrated model includes [1] web characteristics, [2] network security, [3] cryptography, [4] user, and [5] resources management. There are interactions within each of these sectors depicted by system loop map.

Keywords: Web security system, CIS/MIS, courses instructional design, integrated model, interrelationships.

INTRODUCTION

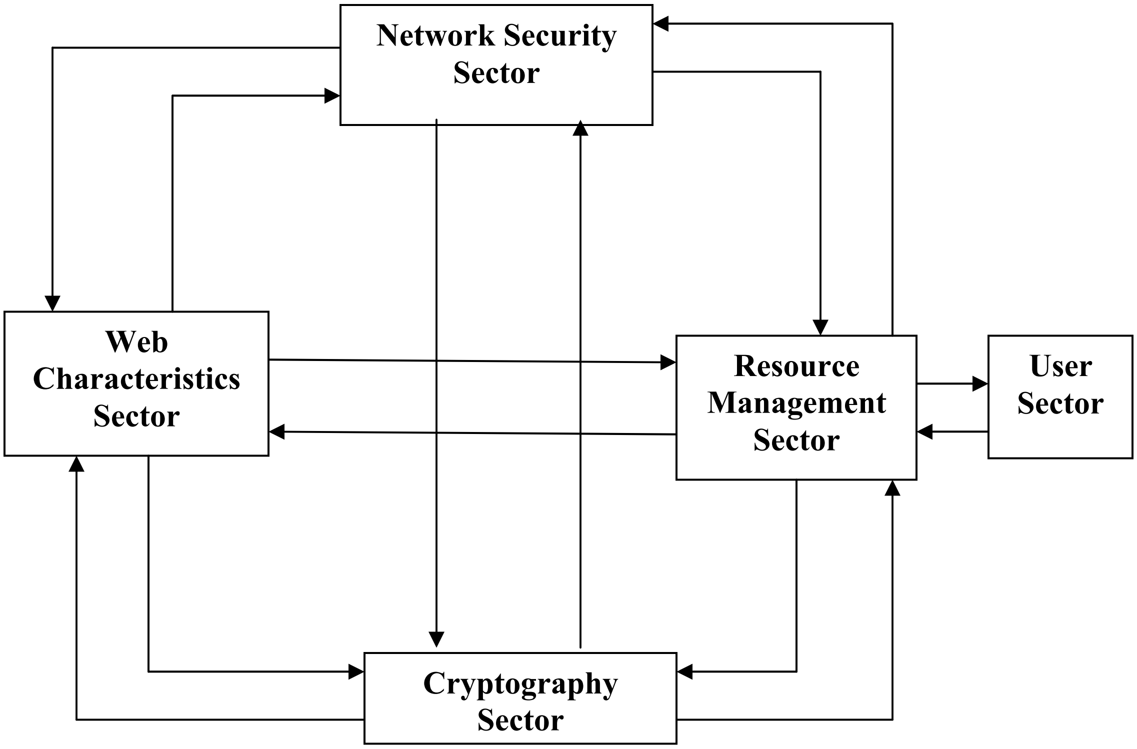
In 2001, Carnegie Mellon University's Computer Emergency Response Team (CERT) Coordination Center handled 52, 658 computer security reports, more than twice the number handled during the previous year. Information security has become a high priority in all facets of life. Information security is not a new field or concepts; the field has been around as long as computer. Nowhere is data protection more indispensable than within Web environments. The power of Internet becomes the daily tools for entertainment, business, communication, shopping, and education. Web security, sub-sector of information security, is gaining more recognition as a critical information technology and systems function. Most MIS/CIS program in universities/colleges have information or network security courses. However, Web security is a complex topic, encompassing computer system security, network security, authentication services, message validation, personal privacy issues, and cryptography. Those topics can be instructed in a single course to a series of courses. From the instructor standpoints, how to teach students and learners to grab the logical thinking and problem solving skills to the web security management is very vital. In general, it is very hard to teach Web topic without touching the web site programming. It is impossible to teach the web server security set up without knowing the networking protocol. This paper presents a model of web security instructional system that can be used as a framework for analyzing web security system characteristics to assist the CIS or MIS courses instructional design.

Specifically, this paper demonstrates a model of Web security system based on nowadays Web server management set up and theory. The relationships in the model are designed to be simple and functional and do not necessarily represent any particular web security environments. It is meant to be a generic web security system model with implications for course planning sequences. It allows Web security instructors to move away from the discrepancy between the courses and body of knowledge. The interrelationships of five primary sectors that are at the Web security system are presented in this paper. They include [1] Web characteristics, [2] network security, [3] cryptography, [4] user, and [5] resources management. There are interactions within each of these sectors depicted by system loop map.

A WEB SECURITY SYSTEM MODEL

The literature provides some guideline for a generic course development model of a Web security model. Web security features that are commonly listed under part of information security include operations systems, legal and ethical issues, network security, risk management, and technical disciplines. Some of these features are necessary for or related with other courses. For example, risk management needs to have legal and ethical discipline up front.

Based on our review of the literatures, which listed in the references section, and our examination of current Web security curriculum, we propose a Web security system model hat consists of five sectors: [1] Web characteristics, [2] network security, [3] cryptography, [4] user, and [5] resources management. How these areas function together and interact with each other is shown in Figure 1. We next describe each of the sectors in Figure 1. Then, the implications of MIS/CIS courses development will be discussed.



Web characteristics

If we make the Web connection as a simple model, it only covers three components: The Web browser, The Web server, and the connection between the two. The Web characteristics capture the whole concept of these three components. The main purpose of Web security is to ensure that these three components remain valid. Based on Stein (1998) Web security has three parts: Client-side security, Server-side security, and Document confidentiality. The disciplines of Web characteristics will be on the basis of network design and security issues, which are tightly related with the functions and concepts inputs from network security sector and cartography sector. However, the strong Web characteristics knowledge will enhance the network security deployment and cryptography methods selection.

Web characteristics sector for MIS/CIS courses include the client-side and server-side programming, multimedia design, database administration, and Web site administration.

Network security

The network security sector provides a way to infuse service into a variety of destinations. In other words, the network security includes three elements, server security, access control and data transmission security. This involves the security of servers and clients, keeping hackers at bay and determining access control (who has access to the company's network and the level of access each user has to the network).

The network security sector has a direct relationship to the resource management sector, cryptography sector and the Web characteristics sector. Using valid cryptography algorithm to protect the Web site on the basis of effective resource control is the key knowledge in Web security area. In other words, effective network access control and security plan will be feedback the resource management later on. The network security sector will cover the wide range of body of knowledge in all network design to administration. Course contents can be included in network operations systems (i.e. Microsoft Windows 2000 Server plus the Internet Information Server; UNIX/Linux Apache Server), protocol administration (i.e. TCP/IP, SNA), network design, network management, Web server administration, information security, Web security , and database administration.

Cryptography

When an instructor teaches Web security, cryptography is often the first thing that put into the course contents. Cryptography does play an important role on the Web security. It enables confidential information to be transmitted from location to location across insecure networks without risk of interception or tampering. In general, a cryptography sector includes four components: cryptographic (encryption) algorithm, network transformation, hardware and software selection, and programming. From the system, some knowledge can be conveyed from network security and Web characteristics sectors. But, specifically cryptography still needs programming and hardware discipline in addition to basic mathematical backgrounds. This is very critical for MIS/CIS curriculum design to consider the pre-requisite from different areas,

User

The user sector includes the inside and outside the organization. The organization is defined as the working surrounding of Web professionals. In other words, for the users, other than the technical aspects, the legal and psychological aspect security should be included in the course contents. Specifically, it includes the ethical and computer crime definition, identifying threat, policy and security regulation development, Internet law as well as styles of attack. In this sector, it is tightly related to resource management because effective resource management will reduce the risk via user disciplines. The user training will be feedback to effective resource control.

Course topics in user sector area on legal aspect, standards, and ethics could be taught in a survey course and integrated into computer and information technology program as well as other programs across the college, including law enforcement, criminal justice, and business management.

Resources management

Resource management involves protecting sensitive information on devices attached to a Web server by controlling access points to that information. In general, it is the center discipline in the Web security area. The resource management will include the business and economics issues related to network security deployment, the network security will be impacted by effective and efficient management functions. Also, it will be the interrelated with cryptograph due to the risk management functions in risk-based assessments and disaster planning.

The courses in the resource management on project control and reducing risk and vulnerability could be included in specific security courses (i.e. network security, information security, Web administration), computer and information technology courses (i.e. network administration, database administration, computer security), and business and management courses (i.e. general management, economic impact and planning, project management, risk management, network management).

IMPLICATIONS FOR MIS/CIS COURSES DEVELOPMENT

Many existing courses in Web security can be filled with two years. For a four-year MIS/CIS program, students with the degree can be a network or security administrator or technician, and can be security department manger to deploy the security system. The best academic preparation for Web security courses may be three disciplines: network management, Web architecture and project (risk) management.

However, current courses or programs may not effectively provide the holistic required for a Web security management major. Web security majors may need specific security training, but this training will be based on the premise that a system possesses fundamental Web knowledge and skills to advanced network administration and security. This system model may provide courses developers and instructors with an alternative to the body of knowledge of the courses contents, pre-requisites, sequences, and structure. The system sectors are grouped together for ease in implementation and thinking, but are not necessarily independent or designed to be taught in separate courses.

In conclusion, the system components that make up this model are [1] Web characteristics, [2] network security, [3] cryptography, [4] user, and [5] resources management. The systems model is an instrument that can be used as a map that captures and activates knowledge. It can also be viewed as a framework that filters and organizes knowledge. Integrated models are micro worlds for experimentation, cooperation, and learning. Relationships in models are designed to be simple and do not necessarily represent any Web curriculum. The purpose of a sport Web security system model is for planning and decision making.

REFERENCES

1. Campbell, P., Calvert, B. and Bosewell, S. (2003). Network security fundamental. Boston: Course Technology.
2. Carlson, Tom. (2001). Information Security Management: Understanding ISO 17799. White paper, Lucent Technologies Worldwide Services.
3. Clarke, R. (1998). *Message Transmission Security (or 'Cryptography in Plain Text').* Retrieved April 02, 2002, from the Australian National University, Engineering and Information Technology site: http://www.anu.edu.au/people/Roger.Clarke/II/CryptoSecy.html
4. Chen, K. C. (1998, April 2-4). The community economic impacts of sport activity: A sports tourism system approach. Paper presented at the Southern Regional Science Association, Savannah, Geogeria.
5. Davis, P. & Lewis, B. (1996). Computer security for dummies. Foster city: IDG Books.
6. Larson, E. and Stephens, B. (2000). Web servers, security, & maintenance. Upper Saddel River: Prentice Hall PTR.
7. Leinwand, A. and Conroy, K. F. (1996). Network management: A practical perspective. Reading: Addison-Wesley.
8. Maiwald, Eric (2001). Network security: a beginner's guide. New York: Osborne.
9. Mackey, D. (2003). Web security for network and system administrators. Boston: Course Technology.
10. National Science Foundation Report. (2002). Protecting information: The role of community college in cybersecurity education. Washington, D.C.
11. Protocols.com. (2002) Retrieved April 05, 2002 from http://www.protocols.com/
12. Schneider, Gary P. & Perry, James T. (2001). Electronic Commerce (2nd ed). Canada: Course Technology.
13. SecurityWatch.com. (2002). Retrieved April 7, 2002 from http://www.securitywatch.com/
14. Stein, L. (1998). Web security: A step-by-step reference guide. Boston: Addison-Wesley.