MIS 605 CA
Principles of Computer Security and Forensics
Fall, 2008

Instructor: Bob Swindler
Office: Mc113
Phone: 628-4185
Office Hours: 7:30 -Noon M-F
Email Mc113a@yahoo.com

ISBN 0-07-225509-9

Course Description
This course addresses the rapidly emerging area of computer security and forensics. Topics covered will include security concepts, cryptography, public key infrastructure, standards and protocols, impact of physical and network security, infrastructure security, wireless and instant messaging, instruction detection, risk, change, and privilege management and computer forensics dealing with security and law. Course includes the learning requirements for certifications in the Com TIA Security Plus, the (ISC) 2 SSCP, and NSTISSC 4011 Examinations.

Prerequisites:
The primary prerequisite for this course is at least 1 year of solid computer experience and MIS 101 or instructor discretion.

Chapter Objectives:
Chapter 1
List and discuss recent trends in computer security
Describe simple steps to take in order to minimize the possibility of an attack on a system
Describe various types of threats that exist for computers and networks
Discuss recent computer crimes that have been committed

Chapter 2
Define basic terminology associated with computer and information security
Describe the basic approaches to computer and information security
Describe various methods to implement access controls
Identify and explain methods used to verify the identity and authenticity of an individual
Describe some of the basic models of security used when implementing security in operating systems

Chapter 3
Describe the various operational aspects to security in an organization
Explain how social engineering is used as a means to gain access to computers and networks and how an organization should deal with it
Explain how the growing use of wireless cellular technology has impacted data transmission and how factors such as location affect our ability to secure it
Describe how the use of shielding technology can prevent disclosure through electronic emanations
Describe various fire suppression systems designed to limit the damage caused by fires

Chapter 4
Define basic terminology associated with Social Engineering
Describe a number of poor security practices that may put an organization’s information at risk
Describe methods attackers may use to gain information about an organization
List and describe ways in which users can aid instead of detract from security

Chapter 5
Identify and describe the three types of cryptography
List and describe current cryptographic algorithms
Explain how cryptography is applied for security
Chapter 6
Explain the basics of public key infrastructures
Describe the role of certificate authorities
Describe the role of registration authorities
Describe the purpose of certificate repositories
Explain trust and certificate verification
Be able to use digital certificates
Compare and contrast centralized infrastructures and decentralized infrastructures
List and describe means of ensuring private key protection
Describe the role of public certificate authorities
Describe the purpose of in-house certificate authorities
Describe the purpose of outsourced certificate authorities
Describe various trust models used when tying different PKIs together

Chapter 7
List and explain various standards involved in establishing an interoperable Internet PKI
Describe interoperability issues with PKI standards
Describe how the common Internet protocols use and implement the PKI standards

Chapter 8
Describe how physical security directly affects computer and network security
Discuss how steps can be taken to help mitigate risks

Chapter 9
Learn the basic network architectures
Discover basic network protocols
Examine routing and address translation

Chapter 10
List and describe various types of network devices used to construct networks
List and describe the types of media used to carry network signals
List and describe various types of storage media used to store information
Describe how the use of security zones and various other topologies provide network-based security
Define basic terminology for a series of network functions related to information security

Chapter 11
Describe various methods and protocols for remote access to networks
Define and describe authentication, authorization, and accounting (AAA) protocols
Describe various wireless protocols and the security implications in their use
Define virtual private networks (VPNs) and describe their security aspects
Define Internet Protocol Security (IPSec) and describe its use in securing communications

Chapter 12
Describe the security implications of wireless networks
Describe the security implications of instant messaging

Chapter 13
Explain host-based intrusion detection systems
Explain network-based intrusion detection systems
Describe honeypots and explain what they are used for
Describe how to conduct incident response operations

Chapter 14
Describe ways of hardening various operating systems
Describe methods for hardening network devices
Describe issues related to hardening various applications
Chapter 15
Describe various types of computer and network attacks, including Denial-of-Service, spoofing, hijacking, and password guessing
Describe the different types of malicious software that exist, including viruses, worms, Trojan horses, and logic bombs
Explain how social engineering can be used as a means to gain access to computers and networks
Explain the importance of auditing and what should be audited

Chapter 16
List various security issues associated with e-mail
Describe some of the security practices for e-mail
List and describe software used to improve e-mail confidentiality

Chapter 17
Describe the protocols used with web components, including SSL/TLS protocol suite, LDAP, and FTP
Describe web applications, such as Web Services and plug-ins, and explain their associated security issues
Describe and explain secure file transfer options
Explain how directory services can be used to aid in data retrieval
Describe how scripting and other Internet functions can cause security concerns
Describe how using cookies maintains parameters between web pages

Chapter 18
Describe how security can be incorporated into the software development process
List types of coding errors and their root cause
Describe good software development practices and explain how they impact application security
Describe how using a software development process enforces security inclusion in a project

Chapter 19
Describe the various ways backups are conducted and stored
Explain different strategies for alternative site processing
Describe the various components of a business continuity plan
Explain how policies and procedures play a daily role in addressing the security needs of an organization

Chapter 20
Explain the purpose of risk management and describe an approach to effectively manage risk
Describe differences between qualitative and quantitative risk assessment
Explain, by example, how both approaches, qualitative and quantitative risk assessment, are necessary to effectively manage risk
Define important terms associated with risk management
Describe various tools related to risk management

Chapter 21
Explain why change management is an important enterprise management tool
Describe the key concept of segregation of duties
Describe the essential elements of change management
Describe a process for implementing change management
List the concepts of the Capability Maturity Model

Chapter 22
List and describe the rules and types of evidence
Describe issues involved with the collection of evidence
Describe issues involved with the preservation of evidence
Explain the importance of a viable chain of custody
Describe the steps in investigating a computer crime or policy violation

Chapter 24
List and describe laws and rules concerning importing and exporting encryption software
List and describe laws that govern computer access and trespass
List and describe laws that govern encryption and digital rights management
List and describe laws that govern digital signatures
List and describe laws that govern privacy in various industries with relation to computer security
Explain the role of ethics in computer security
List and describe laws that enforce ethical behavior

**Instructional Technique:**
Instruction entails reading of the text, working assignments, and participation on Blackboard (exams etc).

**Textbook:**

**Evaluation:**
The grading system is based primarily (but not solely) on the instructor's judgment of your performance on assigned work, including tests and quizzes. Each item is intended to measure performance on a particular skill. The level of performance required varies from item to item.

### Grading Scale

<table>
<thead>
<tr>
<th>Percent</th>
<th>Letter Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>90 – 100</td>
<td>A</td>
</tr>
<tr>
<td>89 - 80</td>
<td>B</td>
</tr>
<tr>
<td>79 - 70</td>
<td>C</td>
</tr>
<tr>
<td>69 - 60</td>
<td>D</td>
</tr>
<tr>
<td>59 and below</td>
<td>U</td>
</tr>
</tbody>
</table>

**Course Policies:**

- **General** - Unless noted elsewhere in this document, all FHSU and College of Business policies apply to this course. Consult appropriate University publications or officers for details.

- **Late work** is not accepted unless you or a close relative have experienced a physical emergency. Don't ask for exceptions.

  **Plagiarism** or other forms of cheating will be dealt with mercilessly. The penalty for any instance of plagiarism will be **failure for the entire course**. By remaining enrolled in the course after receiving this syllabus, you give your consent to this policy. If you are caught cheating, you will probably (but not certainly) be given an opportunity to drop the course if the University permits. It is not plagiarism if you work jointly with other students on assignments in which the instructor has indicated acceptable. However, in any such case, you must indicate clearly who you worked with and what work was done by each person. Also unless such permission has been given; it is plagiarism to copy from textbooks, publications, or other students’ work without attribution. If you don't know what plagiarism is, **ASK!!!**

- **English Usage.** You are expected to use correct academic English in class and in all written work for this class. You can be downgraded severely (to the point of failure) for poor English usage.

- **Graduate Credit.** If you are taking MIS 605 for graduate credit you must contact the instructor immediately to establish the graduate paper subject and parameters needed to fulfill the graduate requirements of this course.