

COURSE DESCRIPTION

Dept., Number	CSC 114	Course Title	Digital Evidence and Computer Crime
Semester hours	3	Course Coordinator	Isaac Ghansah
		URL (if any):	http://gaia.ecs.csus.edu/~ghansahi/

Catalog Description

Topics include technology and law, computer basics for digital investigations, network basics for digital investigations, investigation of computer crime and the handling of digital evidence.

Textbook

Mark Merkow and James Breithaupt, Information Security: Principles and Practices, Prentice-Hall, 2006.

References

C. Easton, Computer Security Fundamentals, Prentice Hall, 2006.

Cliff Stoll, The Cuckoo's Egg, Pocket Books, 1990.

C. Pfleeger and S. Pfleeger, Security in Computing, 3rd Ed., Prentice Hall, 2003.

Course Goals

1. To develop knowledge of information security and assurance best practices.
2. To develop understanding of the importance of securing information efficiently, the threats, risks, and vulnerabilities to information, and the controls available to address these threats.
3. To study management practices and proficiency in the use of selected software tools for securing systems.

Prerequisites by Topic

Thorough understanding of:

- Webpage design and layout including HTML tables and forms.

Basic understanding of:

- Fundamental properties of algorithms and programming.
- How to use Windows and/or Linux operating systems.

Exposure to:

- Elementary working knowledge of a commonly used applications programming language.
- Internet protocols such as HTTP and TCP/IP.

Major Topics Covered in the Course

1. Introduction to Information Assurance and Security, threats to information, importance of information security (3 hours).
2. Risk assessment and security management (3 hours).
3. How contemporary computer systems are organized (1 hour).
4. Access control techniques and models including 2-factor authentication, social engineering, and biometrics (3 hours).
5. Telecommunications, network security and network fundamentals: logical and physical topologies, introduction to TCP/IP, and hardware architecture (6 hours).
6. Cryptography including Advanced Encryption Standard (3 hours).
7. Security architecture and models (3 hours).
8. Operations security (3 hours).
9. Applications, system development, and database security (3 hours).
10. Business continuity planning – disaster recovery planning (3 hours).
11. Law, investigation, ethics, U.S. Patriot Act, Digital Millennium Copyright Act (DMCA), and recent rulings (3 hours).
12. Introduction to host-based perimeter detection and network-based perimeter detection, physical security (3 hours).
13. Methods of attacks, Honeypots and Honeynets, firewalls and perimeters, trap and trace tools such as Echelon (3 hours).
14. Government information assurance regulations (3 hours).
15. System security engineering, future threats and countermeasures (2 hours).

Outcomes

Thorough understanding of:

- Information Assurance and Security best practices.
- Threats, risks, and vulnerabilities to information systems; countermeasures available to address these threats.

Basic understanding of:

- Internet/web security.
- Host security.
- Tools for information security.

Exposure to:

- Cyber forensics.
- TCP/IP protocol suite.
- Career paths in information security.
- Ethical issues related to information security.
- Policy and administration of site security.

Laboratory Projects

1. Windows and Linux/Unix vulnerability analysis.
2. Internet research and reporting on security topics such as biometrics, computer system laws, certifications, security advisories, etc.
3. Linux and Windows security tools and techniques.
4. Security reporting, monitoring and auditing.
5. File system security and cryptography.
6. Use of hands-on hacking tools such as nmap.
7. Firewalls, personal and commercial grade.

Estimated Curriculum Category Content (Semester hours)

<i>Area</i>	<i>Core</i>	<i>Advanced</i>	<i>Area</i>	<i>Core</i>	<i>Advanced</i>
Algorithms			Data Structures		
Software Design			Prog. Languages		
Comp. Arch.					

Oral and Written Communications

Students will be required to write a term paper on information security issues.

Social and Ethical Issues

It will be made clear that the students should not use their knowledge and skills with any malicious intent against the university network, any other networks, physical computing resources, or humans. Students will be required to sign an agreement to observe a set of legal and ethical guidelines.

Theoretical Content

The course covers an overview of cryptographic algorithms and applies cryptography to secure communication applications. Access control principles are also covered.

Problem Analysis

A given configured system will be analyzed in a rigorous manner to determine to what extent it is secure.

Solution Design

Students will learn how to discover security weaknesses and mitigate the identified weakness in the system.