CMP4103 Computer Systems and Network Security

Period per Week			Contact Hour per Semester	Weighted Total Mark	Weighted Exam Mark	Weighted Continuous Assessment Mark	Credit Units
LH	PH	TH	CH	WTM	WEM	WCM	CU
30	30	00	45	100	60	40	3

Rationale

With the multiplication of tasks that are performed on computers and the advent of globalization of computing in general, the topic of computer security becomes more and more important. We see in this course what is computer security, especially as it relates to the protection of information stored on the computers and exchanged between computers The Computer Engineering student will be equipped with knowledge and skills in advanced cryptography, access control, distributed authentication, TCP/IP security, firewalls, IPSec, Virtual Private Networks, intrusion detection systems, and advanced topics such as wireless security, identity management.

Objectives

- To familiarize the student with the concept of system security analysis
- To introduce access control methods and various security models
- To equip the student with skills of identification and authentication in the security domain
- To introduce the various security concerns associated with the most popular operating systems - UNIX and Windows
- To introduce the concept of communication security
- To equip the student with various cryptography systems
- To introduce the student to the security concerns applicable to the internet
- To introduce the student to the various e-commerce security protocols

Course Content

1. ***Overview of Computer Security***
   - Threats, risks, vulnerabilities, safeguards, attacks, exploits
   - Information states
   - Security at the various states of information: processing, storage and transmission
   - Definition of security based on current state and reachable states
   - Comprehensive model of security
   - Confidentiality, integrity and availability
   - Risk management, corrective action, risk assessment
   - Physical security, including TEMPEST security
2. ***Access Control***
   - Access control matrix
   - Access control lists
   - Capabilities
   - Role-based access control
   - Application dependence
3. ***Security Policies***
   - Types of policies
   - Role of trust
   - Information states and procedures
   - Types of access control
   - Separation of duties
   - Application dependence
   - Importance for automated information systems (AIS)
   - Security planning
4. ***Confidentiality Policies***
   - Goals and definitions
   - Bell-LaPadula model
   - Multi-level security
5. ***Integrity Policies***
   - Goals and definitions

- Information states and procedures
- Operating system integrity
- Biba model
- Clark-Wilson model

6. ***Hybrid Policies***
- Chinese Wall model
- Role-Based Access Control

7. ***Basic Cryptography: user's viewpoint***
- Encryption : Classical cryptosystems, Public key cryptosystems
- Message digests and authentication codes
- Application to access control

8. ***Key Management***
- Key exchange
- Session and interchange keys
- Cryptographic key infrastructures
- Storing, revoking and destructing keys
- Digital signatures
- Application to access control

9. ***Cipher Techniques***
- Stream and block ciphers
- Block chaining

10. ***Authentication***
- Passwords
- Challenge-response
- Biometrics
- Location
- Combinations
- Application to access control/authorization

11. ***Design Principles***
- Least privilege
- Fail-safe defaults
- Economy of mechanism
- Complete mediation
- Open design
- Separation of privilege
- Least common mechanism
- Psychological acceptability

12. ***Information Flow***
- Information flow models and mechanisms
- Compiler-based and execution-based mechanisms
- Security policies on information flow
- Relevance of security policies to information security and operations security
- Interdependence between information security and operations security

13. ***Confinement Problem***
- Isolation
- Covert channels

14. ***Assurance and Software Engineering***

- Security aspects of the life cycle
- Software security mechanisms to protect information
- Assurance and trust
- Building trusted operating systems

15. ***Evaluating Systems***

- Historical perspective
- TCSEC
- Common criteria
- Rainbow series
- NSTISSAM COMPUSEC/1-99
- Security certification and accreditation of federal information systems

16. ***Malicious Logic***

- Trojan horses
- Computer viruses
- Computer worms
- Logic bombs
- Defenses and countermeasures

17. ***Vulnerability Analysis***

- Detailed description of threats, vulnerabilities and exploiting vulnerabilities

18. ***Auditing***

- Auditing mechanisms
- Auditing system design
- Privacy issues
- Trails and logs
- Access control issues
- Application dependence

19. ***Intrusion Detection***

- Principles
- Models
- Architecture
- Organization
- Intrusion response

20. ***Network Security***

- Policy development
- Network organization
- Firewalls
- Availability
- Access control issues
- Attacks anticipation
- Traffic analysis
- Public vs private

21. ***Program Security***

- Requirements and policy
- Common security-related programming problems
- Object reuse and access control

22. ***Virtual Machines***

- Virtual machine structure

- Virtual machine monitor

23. ***Security Administration and Training***

- Basic notions related to security administration: accountability, accreditation, security architecture, assessments, assurance, availability, integrity, confidentiality, authentication, non-repudiation, certification, configuration control, resource custidian, defense, domains, system security principles, information operations, records management, sensitivity, zoning, aggregation, end systems, operating systems and organizational security procedures, security tools, open systems interconnect, due care, facility support systems, media, alarms, signals, reports, non-repudiation, violations, modes of operation.
- Security countermeasures - education, training and awareness
- Surveillance
- Assessment
- Roles of various organizational personnel
- Personnel security practices and procedures
- Purposes of awareness, training and education
- Training of administrators and managers
- Protection of assets
- Security accreditation
- Administrative policies
- Password management and policies
- Assessment preparation
- Legal aspects
- Agency specific security policies, points of contact and control
- Security planning
- Contingency planning, disaster recovery
- Configuration management

24. ***Privacy in Databases***

- Publications of aggregate data from sensitive statistical databases
- Inference
- Privacy aspects of data mining

Learning Outcomes

On completing this course the student should be able to:

- Describe the functioning of various types of malicious code, such as viruses, worms, trapdoors.
- Enumerate set programming techniques that enhance security.
- Explain the various controls available for protection against internet attacks, including authentication, integrity check, firewalls, and intruder detection systems.
- Describe the different ways of providing authentication of a user or program.
- Describe the mechanisms used to provide security in programs, operating systems, databases and networks.
- Describe the background, history and properties of widely-used encryption algorithms such as DES, AES, and RSA.
- Describe legal, privacy and ethical issues in computer security.
- List and explain the typical set of tasks required of a system security administrator.

- Compare different access control, file protection or authentication mechanisms.
- Set up file protections in a UNIX or Windows file system to achieve a given purpose.
- Incorporate encryption, integrity check and/or authentication into a given program or algorithm.
- Distinguish between steganography and watermarking as document modification methods.
- Appraise a given code fragment for vulnerabilities.
- Appraise a given protocol for security flaws.
- Design a security protocol for a given application.
- Formulate a security plan for a given scenario, including risk analysis, organizational security policies, and planning for physical security and natural disasters.

Recommended and Reference Books

[1] *Matt Bishop, 2005,* Introduction to Computer Security, *Addison Wesley*

[2] *William Stallings, 2003,* Network Security Essentials, *2nd edition. Prentice Hall. ISBN: 0130351288*

[3] *William Stallings, 2004*, Data & Computer Communications, *7th Edition, Prentice Hall*

[4] Saadat Malik, 2002, *Network Security Principles and Practices (CCIE Professional Development)*. Pearson Education. ISBN: 1587050250

[5] Kaufman, Perlman, and Speciner, *Network Security*, 2nd edition, ISBN: 0130460192.

[6] Ross Anderson's, 2001, *Security Engineering*, 2nd edition. Wiley, ISBN 0470068523

[7] Charles P. Pfleeger, Shari Lawrence Pfleeger, 2003, *Security in Computing*, McGraw-Hill 3rd edition, Prentice Hall.