LAGUARDIA COMMUNITY COLLEGE
CITY UNIVERSITY OF NEW YORK
MAC237: Computer Security
3 Credits, 4 hours (Lecture – 2 hours, Lab – 2hours)

Course Description

Computer Security course introduces students to different aspects of computer security. Topics include security fundamentals, user authentication mechanisms, access control, attacks, intrusion-detection, malicious software, malicious code and countermeasures, software security and its issues, writing safe program code, operating system security, human resources security, application security, browser attacks and security principles, database security, SQL injection, security risk assessment, cloud security.

Prerequisite – MAC227

Pre/Corequisite – MAC250

Textbooks

1. "Computer Security: Principles and Practice" by William Stallings, Lawrie Brown. Publisher: Pearson, 4th Edition. ISBN: 978-0134794105
2. "Web Application Security, A Beginner's Guide" by Bryan Sullivan, Vincent Liu. Publisher: McGraw Hill, 1st Edition. ISBN: 978-0071776165

Instructional Objectives

1. Reinforce students' knowledge of security fundamentals, security principles and strategy, cryptography basics, public-key and private-key cryptography, digital signatures, and hashing algorithms.
2. Introduce students to user authentication mechanisms, security issues for user authentication, access control, identity, credential and access management, trust frameworks.
3. Familiarize students with different types of attack - denial-of-service (DOS) attack, DDOS attack, flooding attack, defense mechanisms against DOS attacks, intrusion-detection, honeypots.
4. Provide the student with an understanding of malicious software, malicious code and countermeasures, software security and its issues, writing safe program code, interacting with system and other programs, operating system security.

5. Introduce students to application security, application security threats and vulnerabilities, session management fundamentals, browser and web attacks, browser security principles.
6. Reinforce students' knowledge of database and SQL basics. Introduce students to database security, stored procedure security, SQL injection and its effects, database encryption and data center security.
7. Introduce students to security development methodologies, IT security management, security policy and risk assessment, security controls.
8. Familiarize students with emerging topics and its security issues such as cloud computing, Internet of things, electronic voting, cyber warfare.

Performance Objectives

Upon completion of this course students should:

1. Illustrate in depth understanding of security fundamentals, security principles and strategy, cryptography basics, public-key and private-key cryptography, digital signatures, and hashing algorithms.
2. Describe different types of user authentication mechanisms, security issues for user authentication, access control, identity, credential and access management, trust frameworks.
3. Define different types of attack - denial-of-service (DOS) attack, DDOS attack, flooding attack, defense mechanisms against DOS attacks, intrusion-detection, honeypots.
4. Identify malicious software and malicious code. Explain software security and its issues, writing safe program code, interacting with system and other programs, operating system security.
5. Define application security, application security threats and vulnerabilities, session management fundamentals, browser and web attacks, browser security principles.
6. Analyze database security issues, SQL injection and its effects, database and data center security.
7. Illustrate security development methodologies, IT security management, policy and risk assessment.
8. Define emerging topics such as cloud computing, Internet of things, electronic voting, cyber warfare and its security issues.

Grading Guidelines

A-, A	90-100
B-, B, B+	80-89
C-, C, C+	70 – 79
D-, D, D+	60 – 69
F	Below 60
WU	Unofficial Withdrawal (Students who have stopped attending at any time before the final exam week, and did not officially withdraw will receive this grade)

Grading Standards

CATEGORY	PERCENTAGE
HomeWorks (3 @ 5% each)	15%
Labs (5@4% each)	20%
Midterm Exam	20%
Project	15%
Final Exam	30%
Total	**100%**

ACADEMIC INTEGRITY

This class will be conducted in compliance with LaGuardia Community College's academic integrity policy.

ATTENDANCE

The maximum number of unexcused absences allowed is 15% of the total class meetings (about 7 hours). Unexcused absences beyond this maximum will result in a grade of WU or F.

COMMENTS

The grading standards listed above, and the suggested homework problems listed in the course outline are both subject to modification by the instructor.

For more details about the academic requirements and grading policy, see the following link: https://www.laguardia.edu/uploadedFiles/Main_Site/Content/Academics/Catalog/PDFs/AcademicRequirementsAndPolicies.pdf

Weekly Topics

Week	Lecture Topics	Labs
1	Computer Security Overview – Security Concepts, Threats, Attacks and Assets, Fundamental Security Design Principles, Computer Security Strategy. Cryptographic Tools – Public Key and Private Key Encryption, Message Authentication and Hash Functions, Digital Signatures and Key Management.	Lab 1: Encryption of Stored Data.
2	User Authentication – Digital user authentication principles, different authentication mechanisms - password-based, token-based, biometric, and remote user. Security issues for user authentication. Access Control – access control principles, access rights. Discretionary, role-based and attributed-based access control. Identity, Credential and Access management. Trust Frameworks.	Lab 2: An Iris Biometric System, Security Problems for ATM systems, RBAC system for a bank. Project Discussion
3	Attacks-Denial-of-Service attacks, Flooding attacks, DDOS attacks, Application-Based Bandwidth attacks. Defenses against DOS attacks, responding to a DOS attack. Intrusion Detection – introduction; host-based, network-based, distributed or hybrid intrusion detection, intrusion detection exchange format, Honeypots.	Homework 1.
4	Malicious Software – Types of malicious software, advanced persistent threat. Propagation – Viruses, Worms, SPAM E-mail, Trojans. Payload – System corruption, Zombies, Bots, Keyloggers, Phishing, Spyware, Backdoors, Rootkits, Countermeasures. Nonmalicious programming oversights, Malicious Code – Malware, Countermeasures.	
5	Software Security – Buffer and Stack overflows, defending against buffer overflows, other forms of overflow attacks. Software security issues, handling program input, writing safe program code, interacting with the operating system and other programs.	Midterm Exam 1

6	Operating System Security – introduction, system security planning, security in the design of operating systems, application security, security maintenance, Linux/Unix and Windows security, Virtualization security, Rootkit. Human Resources Security – security awareness, practices and policies, e-mail and Internet use policies.	Homework 2
7	Application Security – introduction, Top 10 web application security threats (OWASP top 10), application security threats and vulnerabilities, Built-In HTTP authentication; Password best practices; securing password-based authentication. Session management fundamentals, SSL, HTTPS, SSH, Attacks against Session state, Securing Web Application Session Management.	Lab 3: Password based authentication illustration.
8	Browser attacks, Web attacks targeting users, obtaining user or website data, Browser Security Principles – Same-Origin policy and Cross-Site scripting fundamentals, Exceptions to Same Origin Policy and Cross-site request forgery.	Homework 3
9	Database and SQL, SP overview, need for database security, Database Management Systems, Relational Databases, SQL injection and its effects, Setting database permissions, Stored Procedure security, SQL injection in SP, Database access control, Inference, Database encryption, Data Center security.	Lab 4: Database security mechanisms
10	Security Development Methodologies – Approach to Application Security, Industry Standard Secure Development Models: Microsoft SDL, CLASP, SAMM, BSIMM.	Midterm Exam 2
11	IT Security Management, Security Policy, Security Risk Assessment, Security Risk Analysis. IT Security Management Implementation, Security Controls or Safeguards, IT Security Plan, Monitoring Risks.	Lab 5: Silver Star Mines. Project due.
12	Cloud Computing, Cloud Security Concepts, Cloud security Approaches, The Internet Of things (IoT), IoT security, Electronic Voting, Cyber Warfare.	Review
13	Final Exam	