CUNY John Jay College of Criminal Justice
MATH AND COMPUTER SCIENCE

CSCI 411 Computer Security and Forensics
Credits: 3
Hybrid (face to face and online)

COURSE SYLLABUS

Instructor: Prof Aftab Ahmad
Office: NB 612
Telephone No. (212)393-6314
Email Address: aahmad@jjay.cuny.edu
Office Hours: By appointment

TEXT & REFERENCE MATERIAL

Text

Notes from instructor posted on Blackboard

NIST Special Publications SP 800-12r1, 800-53r4, 800-61r2, 800-86

References

Schneier, Bruce. *Applied Cryptography*, Second Edition, John Wiley & Sons, 1996. Other reference material as provided via the Blackboard

Pfleeger, C.P., Security in Computing 5th Edition, Prentice Hall, Copyright 2010ISBN 0-13-239077-9

CATALOG DESCRIPTION

This course concerns host-based security and forensics. The first part of the course explains how security is achieved by most modern operating systems, including authentication and access control at the level of processes, memory, and file systems. The second half of the course will cover methods for monitoring an operating system to detect when security has been breached, and for collecting forensic evidence from computers and other digital devices.

Course Outcomes

The student will be able to

CO1. Describe the various concepts in network defense.

CO2. Describe cyber defense tools, methods and components

CO3. Describe appropriate measures to be taken should a system compromise occur

CO4. List the first principles of security

CO5. Describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies

CO6. Analyze common security failures and identify specific design principles that have been violated

CO7. Identify the needed design principle when given a specific scenario

CO8. Identify the bad actors in cyberspace and compare and contrast their resources, capabilities/techniques, motivations, aversion to risk

CO9. Describe different types of attacks and their characteristics

MODULE	TOPICS	Assessment
Module 1 (CO1, CO8)	Computer security, where do we stand? Best practices Threats and Adversaries Adversaries and targets Motivations and Techniques The Adversary Model (resources, capabilities, intent, motivation, risk aversion, access) Password policies Authentications Methods Updates and patches Access Controls Logging and Auditing (for performance and security) Backup and Restoring Data Vulnerabilities and Risks Basic Risk Assessment	Assignment 1 Blackboard Discussion 1 Assignment 2 Blackboard Discussion 2
Module 2	Security Life-Cycle	Assignment 3

(CO4, CO5)	Security Models Access Control Models (MAC, DAC, RBAC) Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy Security Mechanisms (e.g., Identification/Authentication, Audit) **NIST SP 800-53r4** Two-factor authentication Identity theft in a social engineering scenario	Real-life scenario discussion on failure of authentication
Module 3 (CO2, CO7)	**Notes by instructor** Hashing and Signatures SHA-1, SHA-2, MD-5 and their strengths & weaknesses Digital Signatures and Message Authentication Code (MAC) Minimizing Exposure (Attack Surface and Vectors) Mission Assurance Confidentiality via encryption Secret key and two-key algorithms Advanced Encryption Algorithms (AES) and its principles Tools for Hash, Secure Hash, Digital Signature and Certificates of Authority	Assignment 4 Discuss tools for message authentication code and digital signatures
Module 4 (CO1, CO4, CO9)	**Notes by instructor** Mobile Devices and attacks on them Social Engineering Events that indicate an attack is/has happened Attack surfaces / vectors Attack trees Insider problem Threat Information Sources (e.g., CERT) Separation (of domains) Isolation Encapsulation Least Privilege	Assignment 5

	Simplicity (of design) Minimization (of implementation) Fail Safe Defaults / Fail Secure Modularity Layering Least Astonishment Open Design Usability	
Module 5	Revision and Midterm Examination	Midterm Examination
Module 6 (CO3, CO5, CO9)	**NIST SP 800-61r2 Preparation** *Patching OS and Application Updates Vulnerability Scanning Vulnerability Windows (0-day to patch availability)00 **NIST SP 800-61r2 Detection and Examination** Malicious activity detection / forms of attack Appropriate Countermeasures **NIST SP 800-86** Forensics Process Chain of Custody **(Instructor's notes)** Memory forensics and Volatility Framework	Assignment 6 Watch a video on Volatility Framework and Memory dump
Module 7 (CO2, CO3, CO9)	**Instructor's Notes / Reference** Types of Attacks Password guessing / cracking Backdoors / trojans / viruses / wireless attacks	Assignment 7 Discussion on attack tools, why we need them?

	Sniffing / spoofing / session hijacking Denial of service / distributed DOS / BOTs MAC spoofing / web app attacks / 0-day exploits Vulnerabilities that enable them Attack Timing (within x minutes of being attached to the net) Attack tools Port scanning NMAP and Nessus Password breaking tools Cain & Abel, Rainbow tables Packet sniffers and capture tools PCAP and TCPDump	
Module 8 (CO3, CO6)	NIST Special Publication SP 800-86 Attack detection and evidence collection Detection tools Evidence presentation Attack reporting Risk assessment	Assignment 8 Discussion on the balance between risk and security budget
Module 9	FINAL EXAMINATION	FINAL EXAMINATION