CUNY John Jay College of Criminal Justice
MATH AND COMPUTER SCIENCE

CSCI-400 Capstone Experience in Digital Forensics/Cybersecurity I
Credits: 3

COURSE SYLLABUS

CSCI 400 – section ##

Class Location: Meeting Days/Time:
Instructor Name: Email: Phone:
Office Hours: Office Location:

TEXT & REFERENCE MATERIAL

- Computer Security - Principles and Practice, by William Stallings, Lawrie Brown, 3rd edition. Publisher: Addison Wesley Professional, 2015. ISBN-13: 978-0133773927 - Internet Denial of Service: Attack and Defense Mechanisms, by Jelena Mirkovic, Sven Dietrich, David Dittrich, and Peter Reiher, Publisher: Prentice Hall, 2004. ISBN-13: 9780131475731

CATALOG DESCRIPTION

Theoretical foundations in cryptographic algorithms, cryptographic protocols, access control models, formal methods, security policy, etc. provide the necessary background to understand the real-world implications of cryptography and network security. This capstone course is designed to provide students with a hands-on experience based on the theoretical knowledge they have acquired by taking other security-oriented courses. This hands-on experience is of great importance for future jobs in industry. The course will accomplish its goals through a number of in-lab programming exercises. Topics covered include: basic cryptographic algorithms and protocols; authentication and authorization protocols; access control models; common network (wired and wireless) attacks; typical protection approaches including firewalls and intrusion detection systems; and operating systems and application vulnerabilities, exploits, and countermeasures.

COURSE REQUIREMENTS

Prerequisites: ENG 201, CSCI 373 (Data Structures)
This course is a required course for the Computer Science and Information Security major. It is also a prerequisite for the follow-on course CSCI 401.

COURSE OBJECTIVES

Students will be able to:

CO1. Explain the attacks on basic cryptographic algorithms and protocols in the context of networked computer systems.
CO2. Explain the security models, including the access control matrix and role-based access control.
CO3. Explain where cryptography cannot help with system security.

CO4. Explain the limits of intrusion detection (both signature-based and anomaly-based) and firewalls, in particular how do intrusion detection systems and firewalls fail. CO5. Explain exploits of systems and networks (including DDoS attacks, botnets), and why they still affect us today.
CO6. Explain some countermeasures to system and network attacks, including deceptive techniques.
CO7. Explain the intricacies of malware, including obfuscation techniques to defeat detection at both host and network levels.
CO8. Explain the use of both technical and non-technical means of securing a networked site.

Module Chapter Topics Assignments

1 Introduction, Cryptography Labs (CO1, CO3)
- basic security principles (Ch 1)
- applied cryptogaphy (Ch 2)
- basic networking (App F)

Assignment: Lab 1 (steganography, ciphers, covert communications)

2 Crypto labs (continued) (CO1, CO3)
- cryptographic tools (Ch 2)
- symmetric encryption and message confidentiality (Ch 20)
- public-key cryptography and authentication (Ch 21)
- some aspects of number theory (App B)
- random and pseudomrandom number generation (App D)
- message authentication codes based on block ciphers (App E)

Assignment: Lab 2 (hash collisions, RSA moduli, crypto MITM)

3 Crypto attacks (CO1, CO3)
- user authentication (Ch 3)

Assignment: Lab 3 (dictionary attacks, space-time tradeoffs, rainbow tables)

4 Enhanced-security operating systems (CO2)
- access control models and operating systems (Ch 4)
- trusted computing and multilevel security (Ch 13)

Assignment: Lab 4 (SELinux, OpenBSD, domain and type enforcement)

5 Intrusion detection systems (CO4, CO8, CO6)
- intrusion detection (Ch 8)
- networking protocols in IDS context (App F)

Assignment: Lab 5 (Snort, Bro, nessus, nmap, honeyd)

6 Firewalls (CO4, CO6, CO8)
- firewalls and intrusion prevention systems (Ch 9)

Assignment: Lab 6 (building firewalls, positioning, ruleset development)

Midterm presentation

7 Denial of Service (CO5)
- denial-of-service attacks (Ch 7, Mirkovic Ch 1-6)

Assignment: Lab 7 (closed network experimentation, direct, reflected, amplified, distributed attacks)

8 Malware (CO5, CO7)
- malicious software (Ch 6)

Assignment: Lab 8 (closed network experimentation with malware/attack tools)

9 Exploits (CO5, CO6)
- database (SQL) injection (Ch 5)
- buffer overflows, heap, stack (Ch 10)

Assignment: Lab 9 (buffer overflow generation, SQL injection)

10 Stack protection and sandboxing (CO6, CO7)
- software security (Ch 11)

Assignment: Lab 10 (sandboxing labs, automatic and interactive hardening)

11 OS-specific security, Cross-site scripting, Encrypted mail (CO6, CO8)
- Windows vs. Linux security (Ch 12)
- Internet security protocols and standards (Ch 22)

Assignment: Lab 11 (Securing your OS, XSS, GPG mail)

12 Wireless security (CO5, CO6, CO8)
- wireless security (Ch 24, 802.x standards)

Assignment: Lab 12 (attacks on WEP/WPA, in the form of a CTF exercise)

Final presentation

GRADING
Quizzes (unannounced): 20%
Labs: 20%
Midterm project/presentation: 20%
Final project/presentation: 30 %
Class participation/peer review: 10%

STUDENT INTEGRITY

Statement of the College Policy on Plagiarism

Plagiarism is the presentation of someone else's ideas, words, or artistic, scientific, or technical work as one's own creation. Using the ideas or work of another is permissible only when the original author is identified. Paraphrasing and summarizing, as well as direct quotations require citations to the original source. Plagiarism may be intentional or unintentional. Lack of dishonest intent does not necessarily absolve a student of responsibility for plagiarism. It is the student's responsibility to recognize the difference between statements that are common knowledge (which do not require documentation) and restatements of the ideas of others. Paraphrase, summary, and direct quotation are acceptable forms of restatement, as long as the source is cited. Students who are unsure how and when to provide documentation are advised to consult with their instructors. The Library has free guides designed to help students with problems of documentation. (John Jay College of Criminal Justice Undergraduate Bulletin, http://www.jjay.cuny.edu/academics/654.php, see Chapter IV Academic Standards)