DRAFT (Revised August 20, 2019)

CSCI 400 – Section 01 Cybersecurity Capstone I

Class Location: 06.64.02NB

Meeting Days/Time: Mon/Wed 10:50am-12:05pm (*sine tempore*)

INSTRUCTOR

Name: Prof. Dietrich

Email: sdietrich@jjay.cuny.edu

Phone: +1-212-393-6839

Office Hours: Mon/Wed 4:30pm-5:30pm, and by appointment

Office Location: 06.65.13NB

TEXTBOOKS

- Computer Security - Principles and Practice, by William Stallings, Lawrie Brown, 4th edition. Publisher: Addison Wesley Professional, 2017. ISBN-13: 978-0134794105 - Internet Denial of Service: Attack and Defense Mechanisms, by Jelena Mirković, Sven Dietrich, David Dittrich, and Peter Reiher, Publisher: Prentice Hall, 2004. ISBN-13: 978- 0131475731

- John Jay Textbookx link.

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. It is important to adhere to the proper course sequencing.

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.

REFERENCE MATERIAL

- DETER, based on the original Emulab, a virtual testing environment, is a resource for some of the labs. Students will be assigned individual accounts on DETER by the instructor.

- Hints for writing a research paper in Computer Science.

- Email etiquette and avoiding improper emails.

- Team management resources (Source: CMU)

    - Slides: Team Communications, Part I.

    - Videos: Team Communications, Part I (55 min), Part II (60 min).

- CUNY Institutional Review Board (IRB) overview.

- CUNY John Jay Office of Student Creativity and Research.

- Library resources: Workshops on using the library, finding research papers, and proper citation. Note that the proper citation style for Computer Science is typically either Chicago or Harvard (and not APA or MLA), as prescribed by the Springer LNCS, IEEE Transactions, or ACM Proceedings formats.

- LaTeX templates for the formats above as well as tutorials are available.

- Laptop loan center at CUNY John Jay.

- Your Fall 2019 academic calendar.

QUIZZES

There will be unannounced quizzes throughout the semester, typically 10 min in length. They will cover in-class material, assigned reading, and otherwise assigned material such as current research articles or material covering recent events. It is therefore imperative that students obtain lecture notes from their peers in a timely fashion in case of a missed lecture.

GROUP LABS

There will be group labs assigned every week, performed in groups of 3-4 students as appropriate, covering topics related to the lecture given that week. The groups will be reshuffled on a weekly basis, unless a static setting is needed for continuity of the lab sequence. It is strongly suggested that upon group formation students self-elect a lab group leader to coordinate the various tasks and keep on schedule.

Students may use any non-public means of communicating/messaging among themselves (e.g. email, Google Hangout, Slack, Skype, WhatsApp) that everyone in the group feels comfortable with. By default, John Jay email is the most acceptable one as all students have such an account. Students should consult the project/team management resources for help, and contact the instructor as early as possible in case of problems.

Group labs will be due the week following the assignment, unless otherwise specified.

PROJECTS

There will be group projects (groups of 3-4 students) in addition of the group labs for this class. Students should consult the writing reference material above to help with structuring the project reports. In general, programming sections (if appropriate) of a project should compile and run on Emulab, DETER, or the Unix lab (Math/CS infrastructure). For projects dealing with Windows/macOS, other OSes, or other infrastructures, students must get the permission of the instructor in writing.

These small project groups will include students with a variety of areas of expertise. A choice of semester projects will be

provided early in the semester, and students will be given an opportunity to indicate their preferences before projects are actually assigned. Students who have their own ideas for projects should discuss them with the instructor early in the semester.

Project proposal: The proposal should state the research questions; hypotheses or arguments (if any); general type of study, analysis (lab, online, interview, survey, etc.), or code/system development; overview of the tasks to be undertaken; quantitative metrics and/or qualitative analysis approach; in case of a subject study, the number and type of study participants the group is planning to recruit and the group will recruit them, and a study design (between subjects, within subjects); related work; equipment, software, other resources, and/or payments needed and preliminary budget. In case of needed funds, students should contact the John Jay Office of Student Research and Creativity and submit an application (e.g. for the Student Research/Creativity Support Fund) as soon as possible. In case of a human subject study, research involving personally identifiable information (PII) or directly/indirectly impacting humans and the local or global infrastructure, students will have to submit an IRB application (see IRB contact information above).

Midterm project report and presentation: This is in the form of a 5 to 8-page single-spaced paper (Springer LNCS, IEEE Transactions, or ACM Proceedings format required) summarizing the project findings, built upon the project proposal structure above, plus additional references appendices, and a 10-minute presentation of the key points of the project to the class, followed by 5 minutes of discussion.

Final project and presentation: A 15-page single-spaced paper (Springer LNCS, IEEE Transactions, or ACM Proceedings format required) summarizing the project findings, as an extension of the midterm report, plus references any appendices (e.g. code or data corpora), and a 15-minute presentation extending the midterm results, followed by 10 minutes of discussion. A poster (quad chart or tri-fold) may be substituted for the presentation, at the instructor's discretion.

Students are encouraged to submit a revised version of their final paper to a security conference, such as DIMVA 2019.

CLASS PARTICIPATION/PEER REVIEW

Students' active and constructive participation in the classroom is welcome and expected. Students are also expected to perform peer reviews on the in-class project presentations and posters, typically in the form of 2-3 constructive paragraphs per presentation.

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

POLICIES

Americans with Disabilities Act (ADA) Policies

Qualified students with disabilities will be provided reasonable academic accommodations if determined eligible by the Office of Accessibility Services (OAS). Prior to granting disability accommodations in this course, the instructor must receive written verification of a student's eligibility from the OAS which is located at L66 in the new building (212-237-8031). It is the student's responsibility to initiate contact with the office and to follow the established procedures for having the accommodation notice sent to the instructor.

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)

ADDITIONAL POLICIES

- No cell phones should be used in class. They should be off or on silent.
- No recording (photo, video, audio) is permitted during the lecture.
- Laptops, handhelds, or other electronic devices should NOT be used in class, unless explicitly required for the coursework.
- A make-up exam will be granted only if:
  - the instructor is notified BEFORE the exam
  - AND
  - there is serious illness or similarly important reason for missing that day. Students should notify the Dean of Students for such serious matters and have them inform the instructor.
- No make-up quizzes.
- For fairness to all students there will be no individual extra credit work.
- Assignments are due before the lecture begins. After that time, 25% will be deducted from the grade. For assignments late more than one (two) day(s), 50% (75%) will be deducted. No credit will be given for assignments that are more than 3 days late. Exceptions may be granted only if there is an important reason. Exceptions must be cleared with the instructor in advance. When assignments are due via CUNY Blackboard, the Blackboard timestamp is authoritative.
- Students may collaborate on projects with fellow students to a limited degree: students may discuss concept clarifications with other students, but the specific details of the projects must be their own work.
- Students must specify in writing any resources (web, books etc.) other than the textbook that that was used for completing the assignments.
- It is cheating to collaboratively work out a detailed solution, to copy a solution from another student or some other resource without specifying it, or to give away a solution. Plagiarism checkers such as SafeAssign and TurnItIn (text) or MOSS (source code) may be used by the instructor.
- Self-plagiarism is considered cheating.
- ALL parties involved in a case of cheating get an automatic grade of zero (0) in the assignment/exam. Repeated cases get an F in the course. Any case of cheating will be reported to the appropriate Dean.
- Most exercises/labs in this course are considered "red-team exercises" that could be harmful to production networks, including CUNY networks. They are for in-class use only! Do not apply these techniques outside of the experiment environment (such as DETER) without proper (and written) authorization. Violations will be reported to the Department of Information Technology and the appropriate Dean.
- All students are required to attend their midterm and final group project presentations.

COUNSELING AND REFERRAL SERVICES

Students should take care of themselves during the semester. In case of concern, students should know that their peers and themselves can find a complete range of counseling and referral services:

New Building L.68.00
Phone: +1-212-237-8111
Email: counseling@jjay.cuny.edu
Web: http://www.jjay.cuny.edu/counseling
Other resources: https://www.jjay.cuny.edu/wellness-resources

WEEKLY SCHEDULE

Week	Topic	Reading	Assignments
August 28, 2019	Crypto labs. Ciphers, steganography, and covert communications.	Stallings Ch 1, 2, App F	Lab 1 Reference materials (Lab 0 DETER warmup)
Sep 4 & 5, 2019	Crypto labs (avalanche, hash collisions, RSA, crypto MITM).	Stallings Ch 2, 20, 21, App B, D, E	Lab 2 Reference materials Project topics due Sep 14
Sep 9 & 11, 2019	Crypto attacks (dictionary attacks, space-time tradeoffs)	Stallings Ch 3	Lab 3 Project proposals due Sep 21
Sep 16 & 18, 2019	Enhanced-security operating systems labs (SELinux, OpenBSD)	Stallings Ch 4, 13	Lab 4
Sep 23 & Sep 25, 2019	Intrusion Detection Systems labs (Snort, Bro, honeyd, nessus, nmap)	Stallings Ch 8, App F	Lab 5
Oct 2 & 7, 2019	Firewall labs (building FWs, positioning, ruleset development)	Stallings Ch 9	Lab 6
Oct 16, 2019	Midterm project in-class presentations		Project reports/presentations due Oct 16
Oct 21 & 23, 2019	DoS labs (closed network experimentation with DoS, single, reflected, amplified, distributed)	Stallings Ch 7 Mirkovic Ch 1-6	Lab 7
Oct 28 & 30, 2019	Malware labs (closed network experimentation with attack tools)	Stallings Ch 6	Lab 8
Nov 4 & 6, 2019	Special topics		Research paper summary report due Nov 8
Nov 11 & 13, 2019	Exploits labs (buffer overflow, SQL Injection)	Stallings Ch 5, 10	Lab 9
Nov 18 & 20, 2019	Stack protection and sandboxing labs (automatic and interactive hardening)	Stallings Ch 11	Lab 10

Nov 25 & 27, 2019	OS-specific security (Windows/Unix), Cross-site scripting, Mail security (GPG)	Stallings Ch 12, 22	Lab 11
Dec 2 & 4, 2019	Wireless labs (WEP/WPA attacks: deauthentication, key extraction)	Stallings Ch 21, 23, 24, 802.11 standards	Lab 12 Draft presentations due Dec 5
Dec 9 & 11, 2019	Final project in-class presentations Poster session (at community hour on Dec 9)		Final project reports/presentations due Dec 10
Dec 18, 2019	Revised final report due		Revised project report due