HUNTER
The City University of New York

CSCI 493-81-01 Introduction to Computer Security
Combined course:
CSCI 795-29-01 Introduction to Computer Security
Fall 2021
(Final draft syllabus as of Aug 26, 2021)

Thursday 5:35PM – 8:15PM, Online/synchronous

Instructor:	Dr. Sven Dietrich, Professor of Computer Science spock@hunter.cuny.edu, http://www.cs.hunter.cuny.edu/~spock
WWW:	Course-related material can be found on the **Blackboard** course page. Visit it regularly. Online lectures will take place on Blackboard or Zoom, as appropriate/needed and announced on Blackboard.
Office:	1009, Hunter North (for office hours, see below)
Tel:	(212) 772-4939 [office], (212) 772-5213 [CS department]
Office Hours:	Thursday 1-2pm (via online meetings only) or by appointment

Textbooks

Required: P.C van Oorschot, Computer Security and the Internet: Tools and Jewels, Springer Verlag, 2020.
ISBN: 978-3-030-33648-6 (hardcopy), 978-3-030-33649-3 (eBook)
Required: J. Mirkovic, S. Dietrich, D. Dittrich, and P. Reiher. Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall, 2004. ISBN-13: 978-0131475731 (hardcopy)

Course Content and Objectives

Security is key to understanding critical systems and one of the core requirements for their design. This introductory course will cover the introduction-level fundamental knowledge of computer security as well as applied cryptography. Students will learn the basic concepts in computer security, including applied cryptography, software vulnerability analysis and defense, networking, intrusion detection, and wireless security. Students will be able to understand the fundamentals for designing and analyzing security-critical systems.

Learning goals

As a computer security course, an area of Computer Science, this course is compliant with the Hunter Computer Science Learning Goals listed at http://www.hunter.cuny.edu/csci/for-students/learning-goals-for-hunter-college-students

Prerequisites

Undergraduate: CSCI 33500 Software Analysis and Design III;
MS-level: permission of department.

Succeeding in This Course

If you want to succeed in this course, then you must do *all* of the following:

- Do the assigned readings before the lecture, not after it.
- Make a list of questions before the class.
- Submit all assignments on time.
- Read additional papers listed at the end of each chapter.
- Study for exams/prepare for presentations.
- Do all assignments yourself or as a project group, as assigned! Various plagiarism checkers will be used. Expect severe penalties for plagiarism or misconduct.

Syllabus and Readings

At the end of this document you can see which parts of the textbook we will cover. You are responsible for everything in the listed chapters regardless of how much time we spend on them in class. As noted above, you should read ahead so that you can ask questions in class to clear up anything you find confusing.

Except for changes that substantially affect implementation of the evaluation (grading) statement, this syllabus is a guide for the course and is subject to change with advance notice. Any such change will be posted on Blackboard.

Assignments

No one can become proficient at computer and network security without working with it at the systems level, but one must also communicate results. There will be a semester-long group project during the semester, together with presentation assignments to fulfill the oral presentation goals. All assignments will be due on Blackboard.

Group projects

There will be group projects (groups of 3-4 students) for this class. Students should consult the writing reference material in the Resources section below 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 (Hunter CS Lab 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 via project proposals before projects are actually assigned. Students who have their own ideas for projects should discuss them with the instructor early in the semester, prior to the project proposal deadline.

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, if appropriate. There may be Hunter College funding available for undergraduate or graduate-level projects. 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 CUNY IRB contact information below). If you can't find a topic or project peers, those will be assigned to you.

Midterm project presentation: A 10-minute presentation of the key points of the project to the class, followed by 5 minutes of discussion. You should also include any code or project materials.

Midterm project report (MS-Level): 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 in a scientific manner, built upon the project proposal structure above, plus additional references appendices.

Final presentation: A 15-minute presentation extending the midterm results, followed by 10 minutes of discussion. A poster (quad chart or tri-fold) should be created as a companion for the presentation. . You should also include any updated code or project materials.

Final project report (MS-Level): 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, in a scientific manner, plus references and any appendices (e.g. code or data corpora).

MS-Level: students are encouraged to submit a research paper based on their final project report to a research conference with deadlines in Spring 2022. Please contact the instructor for details.

A division of labor statement is required for all group presentations and reports, both for undergraduate and MS-level.

Resources

- 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.
- Hints for reading Computer Science research papers.
- Email etiquette and avoiding improper emails.
- Team management resources (Source: CMU)
    - General resources: overview.
    - Videos: Team Communications, Part I (55 min), Part II (60 min).
- CUNY Institutional Review Board (IRB) overview.
- 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 software and tutorials are available.

Course Material and Communication

All course material (i.e. slides or other resources) will be uploaded on *Blackboard*. Assignments will be uploaded on *Blackboard*.

If you have a question about the class, topics covered, assignments etc. please first check the posts in the Q & A or discussion board section. If you did not find an answer, please post your question there. That will make it easier for all students to see answers. You can also answer questions of fellow students. Do not post any type of assignment solutions, as violations will be reported to the Office of Academic Integrity.

For questions involving personal matters you can email the instructor. All email communication is to use **CUNY email only**. Please make sure you add "CSCI 493" to the subject of your emails, and you read the email guidelines in the Resources section. Allow for reasonable time for email response, adjusting for business hours, and understand that replies won't be immediate.

Note on cameras: Please be aware that the instructor in this course will require that the camera and audio be on during certain class sessions, e.g. for presentations or discussions.

Grading

Undergraduate level: There will be one midterm exam and one final exam. The final exam is not comprehensive (i.e. it will only cover material taught after the midterm). Your final grade will be calculated as follows:

25% (midterm exam) + 35% (final exam) + 20% (2 project presentations) + 20% (project poster) = 100%

For MS-level the allocation is as follows: 15% (midterm project report) + 25% (final project report) + 20% (2 project presentations) + 20% (project poster) = 100%

Late submissions are subject to 10 points off an assignment worth 100 points for being late one day (24 hours), 20 points for the second day, and 30 points off for the third day. Submissions late more than three days will not be accepted and will result in a grade of zero for that assignment.

Make-up Policy

All exams must be taken on time. Failure to take an exam counts as a zero grade on that exam. The same applies to a project presentation. If you miss the midterm or final exam (or the presentations) for a legitimate, documented medical emergency, the instructor will find a way (if possible) to assist you.

Lecture Recording Policy

Students are **not allowed** to record the online lecture using any screen, audio, or video recording. Lecture notes/slides will be made available to the students to get access to the lecture materials. Violations will be reported to the Office of Student Conduct.

Student conduct

As a reminder, CUNY students are bound by the Henderson Rules of Conduct. Further details can be found on the web page of the Hunter College Office of Student Conduct: http://www.hunter.cuny.edu/studentaffairs/student-conduct

Academic Integrity

Hunter College regards acts of academic dishonesty (e.g., plagiarism, cheating on examinations, obtaining unfair advantage, and falsification of records and official documents) as serious offenses against the values of intellectual honesty. The college is committed to enforcing the CUNY Policy on Academic Integrity and will pursue cases of academic dishonesty according to the Hunter

College Academic Integrity Procedures. You can find a copy of this policy online, and by being a CUNY student you are held by it. Please take a moment to read it, if you have not done so already:

https://www.cuny.edu/about/administration/offices/legal-affairs/policies-procedures/academic-integrity-policy/

Note on Course Materials

Most techniques discussed 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, the appropriate Dean, or the proper law enforcement authorities.

Proctoring Software

Proctoring software, which may include the use of browser lock-downs and cameras, may be used for examinations in this course.

ADA Compliance

In compliance with the American Disability Act of 1990 (ADA) and with Section 504 of the Rehabilitation Act of 1973, Hunter College is committed to ensuring educational parity and accommodations for all students with documented disabilities and / or medical conditions. It is recommended that all students with documented disabilities (Emotional, Medical, Physical and / or Learning) consult the Office of AccessABILITY located in Room E1124 to secure necessary academic accommodations. For further information and assistance please call (212-772-4857)/TTY (212-650-3230).

Hunter College Policy on Sexual Misconduct

In compliance with the CUNY Policy on Sexual Misconduct, Hunter College reaffirms the prohibition of any sexual misconduct, which includes sexual violence, sexual harassment, and gender-based harassment retaliation against students, employees, or visitors, as well as certain intimate relationships. Students who have experienced any form of sexual violence on or off campus (including CUNY-sponsored trips and events) are entitled to the rights outlined in the Bill of Rights for Hunter College.
a. Sexual Violence: Students are strongly encouraged to immediately report the incident by calling 911, contacting NYPD Special Victims Division Hotline (646-610-7272) or their local police precinct, or contacting the College's Public Safety Office (212-772-4444).
b. All Other Forms of Sexual Misconduct: Students are also encouraged to contact the College's Title IX Campus Coordinator, Dean John Rose (jtrose@hunter.cuny.edu or 212-650-3262) or

Colleen Barry (colleen.barry@hunter.cuny.edu or 212-772-4534) and seek complimentary services through the Counseling and Wellness Services Office, Hunter East 1123. CUNY Policy on Sexual Misconduct Link:
http://www.cuny.edu/about/administration/offices/la/Policy-on-Sexual-Misconduct-12-1-14-with-links.pdf

Hunter College Counseling and Wellness 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 at the Hunter Counseling & Wellness Services:

personalcounseling@hunter.cuny.edu
Tel: 212.772.4931
Room 1119, East Building
http://www.hunter.cuny.edu/cws

Outline of lectures

Week 1 (August 26, 2021)

Basics: Introduction, Ethics, Course Overview

Reading:

- The Menlo Report, Ethical Principles Guiding Information and Communication Technology Research, US Department of Homeland Security, August 2012.
- Ken Thompson. Reflections on Trusting Trust, Communications of the ACM, August 1984 https://doi.org/10.1145/358198.358210.

Crypto: Introduction to Cryptography

In this lecture we will provide a high-level introduction to cryptography, including an overview of primitives and security models. We will touch on the rich power offered by modern cryptographic tools. Finally, we will discuss (in)secure sources of randomness. We will review the mathematics needed to understand modern cryptographic algorithms and discuss the basics of writing rigorous proofs.

Reading:

- Computer Security and the Internet (textbook), Chapter 2.1-2.2.
- Al Menezes, et al. Handbook of Applied Cryptography, Select chapters, 1996.

Assignments:

Review the syllabus materials, read DETER manuals, explore project topics.

Week 2 (September 2, 2021)

Crypto: Public-Key Cryptography

In this lecture we will cover the fundamentals of public key cryptography, focusing on RSA and Diffie-Hellman as examples.

Reading:

- Computer Security and the Internet (textbook), Chapter 2.3-2.9.
- Dan Boneh and David Brumley, Remote timing attacks are practical, In Proceedings of the 12th Usenix Security Symposium, 2003.

Security Principles: Threat Models and Trusted Computing Bases

Reading:

- Computer Security and the Internet (textbook), Chapter 1-1.8.
- Optional reading (MS-level): All of Chapter 1.

Week 3 (September 9, 2021)

Security Principles: Designing Secure Systems

Principles of designing secure systems, CIA Triad, three AUs (authentication, authorization, audit).

Reading:

- Computer Security and the Internet: Chapter 5.2-5.4, 5.7

Software Security: Execution Semantics and Buffer Overflows

This covers the compilation process, assembly-level considerations, control flow, memory models, and stack frames. This also discusses how to gain control of the instruction point in the context of buffer overflows.

Reading:

- Aleph1 (aka Elias Levy), Smashing the Stack for Fun and Profit, Phrack 49. Available at www.phrack.org/issues/49/14.html#article, November 1996.

Assignments:

Project proposals due.

Week 4 (September 16, 2021)

No classes.

Week 5 (September 23, 2021)

Software Security: Control-Flow Attacks and Defenses

This covers more advanced control-flow hijacking attacks, e.g. format-string exploits, integer overflows, and memory-allocation dynamics. Defenses discussed include canaries, W^X aka DEP, and randomization of library calls (ASLR). Here we also cover methods to bypass these defenses.

Reading:

- Paul Makowski, Smashing the stack in 2011. Available at https://paulmakowski.wordpress.com/2011/01/25/smashing-the-stack-in-2011/
- teso. Exploiting format string vulnerabilities. Phrack, September 2001.

Software Security: Return-Oriented Programming

This covers Return-Oriented Programming attacks.

Reading:

- Hovav Shacham, The Geometry of Innocent Flesh on the Bone: Return-into-libc without Calls (on the x86), Full version of ACM CCS 2007 Extended Abstract.
- Ropasaurusrex, A primer on return-oriented programming, 2013. Available at https://blog.skullsecurity.org/2013/ropasaurusrex-a-primer-on-return-oriented-programming

Week 6 (September 30, 2021)

Software Security: Looking at Memory Safety

This lecture focuses on retrofitting legacy C code, e.g. with Control Flow Integrity (CFI) by enforcing executions to follow the CFG.

Reading:

- Abadi et al., Control Flow Integrity Principles, Implementations, Applications, ACM Transactions on Information and System Security, November 2009, Article No.: 4 https://doi.org/10.1145/1609956.1609960.
- George Necula, et al., CCured: Type-Safe Retrofitting of Legacy Software, ACM Transactions on Programming Languages and Systems, Vol. 27, No. 3, May 2005, Pages 477–526.

Software Security: Type Systems and Verification

This covers programming language techniques to eliminate entire classes of vulnerabilities and prove strong properties of software.

Reading:

- K. Rustan Leino, Microsoft Research, Dafny: An Automatic Program Verifier for Functional Correctness.

Week 7 (October 7, 2021)

Software Security: Code Analysis and Isolation Techniques

This discusses techniques for analyzing code for memory vulnerabilities. Several techniques for protecting memory are covered: sandboxing, Software Fault Isolation (SFI), SMAC.

Reading:

- Computer Security and the Internet: Chapter 5.1
- Al Bessey et al., A few billion lines of code later: using static analysis to find bugs in the real world, Communications of the ACM, February 2010, https://doi.org/10.1145/1646353.1646374
- Google Native Client, https://developer.chrome.com/docs/native-client/

Systems Security: Modern Operating System Security and Trusted Computing

The focus is on modern operating system security, including access control and capabilities, and reasoning about authorization. This will also cover how to bootstrap trust in systems.

Reading:

- Martin Abadi et al., A calculus for access control in distributed systems, ACM Transactions on Programming Languages and Systems, September 1993, https://doi.org/10.1145/155183.155225
- Bryan Parno, Jonathan M. McCune, and Adrian Perrig. Bootstrapping Trust in Commodity Computers (SoK paper), 31st IEEE Symposium on Security and Privacy, S&P 2010, 16-19 May 2010, Berkeley/Oakland, California, USA.

Week 8 (October 14, 2021)

Midterm project presentations.

Assignments due: Midterm project presentations. MS-Level: Additionally draft midterm project reports due.

Week 9 (October 21, 2021)

Undergraduate level: Midterm exam. MS-Level: Midterm project reports due.

Week 10 (October 28, 2021)

Network Security: Protocol Design and Analysis

This lecture will give a broad overview of network security, including general principles, denial-of-service attacks, botnets, and intrusion detection (and prevention) systems. The latter will cover some basic detection theory, focusing on the base rate fallacy.

Reading:

- Computer Security and the Internet, Chapters 10.1 and 10.6
- Computer Security and the Internet, Ch. 11.1, 11.2, 11.4
- Internet Denial of Service: Attack and Defense Mechanisms, Ch. 1-6
- Stefan Axelsson, The base-rate fallacy and the difficulty of intrusion detection, ACM Transactions on Information and System Security, August 2000. https://doi.org/10.1145/357830.357849
- Steven M. Bellovin, Security problems in the TCP/IP protocol suite, ACM SIGCOMM Computer Communication ReviewApril 1989 https://doi.org/10.1145/378444.378449
- Steven M. Bellovin, "A look back at "security problems in the TCP/IP protocol suite," 20th Annual Computer Security Applications Conference, Tucson, AZ, USA, 2004, pp. 229-249, doi: 10.1109/CSAC.2004.3.

Week 11 (November 4, 2021)

Network Security: Protocol Design and Analysis

This lecture will cover design principles for secure protocols, common failures and defenses, and tools for analyzing protocol security. TLS will be used as a detailed case study.

Reading:

- Martin Abadi and Roger Needham, Prudent Engineering Practice for Designing Cryptographic Protocols, IEEE Transactions on Software Engineering 22, 1 (January 1996), 6-15.

- Cas Cremers et al., A Comprehensive Symbolic Analysis of TLS 1.3, CCS '17: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, October 2017, Pages 1773–1788 https://doi.org/10.1145/3133956.3134063

Web Security: Attacks and Defenses

This lecture will cover web security, including vulnerabilities such as injection attacks, XSS, and CSRF. This lecture will also cover web security with a focus on principles, such as authentication vs. authorization, and best practices for establishing security on the web.

Reading:

- Computer Security and the Internet: Chapter 9.
- Bennet Yee, et al., Native Client: A Sandbox for Portable, Untrusted x86 Native Code, 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, USA, 2009, pp. 79-93, doi: 10.1109/SP.2009.25.

Week 12 (November 11, 2021)

Wireless LAN Security: Attacks and Defenses

This covers wireless protocols and associated security mechanisms, as well as attacks.

Reading:

- P.C. van Oorschot. Computer Security and the Internet. Additional chapter 12 from 2021.

Week 13 (November 18, 2021)

Privacy: Introduction to Privacy

This lecture will cover general concepts and various mathematical definitions of privacy as well as how to achieve them. We will discuss and experiment with practical tools used to provide privacy today.

Reading:

- S. Spiekermann and L. F. Cranor, "Engineering Privacy," in IEEE Transactions on Software Engineering, vol. 35, no. 1, pp. 67-82, Jan.-Feb. 2009, doi: 10.1109/TSE.2008.88.

Usability: Making Security Usable

The most secure system in the world can be subverted if users can't employ it correctly (or if they themselves are subverted!). This lecture will cover usable design, with case studies drawn from security warnings, authentication, and phishing. We will also cover attacks and defenses based on social engineering.

Reading:

- Alma Whitten and J.D. Tygar, Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0, Proceedings of the 8th conference on USENIX Security Symposium - Volume 8, August 1999.

Week 14 (November 25, 2021)

No classes.

Week 15 (December 2, 2021)

Special topics: Blockchains, Cryptocurrencies, and Smart Contracts

We will cover the basics of blockchains (what they are, what they are and are not good for), cryptocurrencies and, time permitting, smart contracts. We will also discuss attacks on these.

Reading:

- P.C. van Oorschot. Computer Security and the Internet. Additional chapter 13 from 2021.
- Arvind Narayanan, et al., Bitcoin and Cryptocurrency Technologies, Chapters 3-21, Available at https://bitcoinbook.cs.princeton.edu

Special Topics: State-of-the-art Security Research (time permitting)

A sampling of recent security papers from the main security conferences.

Week 16 (December 9, 2021)

Final semester project presentations; MS-level: final draft of project report due

Week 17 (December 16, 2021)

Undergraduate level: Final exam (5:35pm-7:35pm); MS-level: final project reports due 5:35pm.

Credit where credit is due: Lujo Bauer, David Brumley, Mike Reiter.