Syllabus - UConn CSE 4402/5402 - Network Security
Fall 2023

This course introduces network security. This is a large topic; we cannot cover all of it in the allocated time, so we have to be selective. We focus on the most important and interesting aspects of Internet security. This includes 'classical' net-security (firewalls, scanning, IDS etc.), TCP/IP security (incl. ARP, DNS), inter-domain routing (BGP) security, web security and more. There is also a (natural?) bias towards topics that the lecturer has been doing research in, and/or finds more interesting and important.

The course is challenging, esp. since the lecture notes are not yet ready. But I hope that you will still learn a lot from it and also enjoy it.

0.1 Course information

Lecturer: Prof. Amir Herzberg. Office: ITE (Information Technologies Engineering) room 217. Office hours: schedule in Nexus ; if unavailable/inconvenient, coordinate by email (or after lecture if time permits). You can also contact by by email for questions or otherwise.

Attendance. Course is held Tuesdays and Thursdays, TuTh 9:30AM - 10:45AM, in AUST 164 (unless we move it, which seems likely, or if we need to do remotely). *Attendance is mandatory*, in person when class is held in person, since some assignments are done in class. However, if you have any issue, send, sufficiently in advance, email to inform of absence or to coordinate remote participation. Absence without such email, or excessive absences, may result in grade reduction.

Course Learning Objectives By the end of this course, you should understand and apply the basic (1) theoretical and (2) applied aspects of network security.

Prerequisites: Computer networking (3300) and introduction to cybersecurity (3400); this term we will experimentally allow taking these classes in parallel. Both courses are essential; a crypto course may be a reasonable substitute for 3400. Graduate students that learned the topics of these courses elsewhere can check with the lecturer, to confirm that their knowledge is sufficient.

Grad (5402) and undergrad (4402) versions. The two classes have the same requirements exactly. Undergrad students may consider switching to the 5402 course - this will allow the same credits to apply to a graduate degree if you will decide to pursue it, without any drawbacks afaik.

Honor conversions are possible.

Textbook, Labs and Reading materials The labs in the course are mostly based on the Seedlabs project, with few extensions in (most/all) specific labs and few labs not in SeedLabs or significantly modified. The students are referred to the SeedLabs website for the original labs, and to the corresponding (optional) textbook, 'Internet security', by Prof. Wenliang Du, also available in an edition covering also computer security [2], which is more cost-effective if you are interested in both topics. The book is not mandatory.

For deeper understanding and more advanced defenses and attacks, we will disuss beyond the contents in the book (and the labs). Some of that content will be available from lecture notes I will post in HuskyCT.

Additional optional sources for specific topics: *Network scanning* [5], *Firewalls* [1], *Web security* [6].

Communication All communication regarding the course will be via HuskyCT and Piazza; use signup link to Piazza. Please ensure you receive emails from HuskyCT so you get announcements.

Students are encouraged to ask questions in class, use the discussion board in Piazza or email. Piazza is preferred for non-personal issues (to provide help to others). You can ask and answers questions anonymously in Piazza, we hope this may make it easier to participate; but if you don't mind, share your name, this makes for even better cooperation.

0.2 Schedule, Requirements and Grades

Schedule. Table 1 contains the course schedule. Student presentations will be on different labs done by teams of 1-3 students. Some labs may be based on seedlabs, but extended as agreed with lecturer; other labs will be different, possibly based on code (and/or guidelines) from lecturer.

Course requirements will include about five homework assignments, which you may do in pairs. You are free to form these pairs and teams on your own. However, lab teams must be finalized by September 7, or you will have to do the lab alone, or in a team defined by the lecturer. You then must agree with the lecturer on the topic and scope of your lab, by October 3rd, and send a draft of your presentation and report to the lecturer by Nov. 20.

Assignments and grades. The course has four types of required grade components:

20% In-class quizzes (probably four).

25% A ('theory') final exam.

25% Home ('theory') assignments. Students are allowed 6 late days *in total for all of these assignments*, please write in *each* assignments how many late days do you use for it and how many did you use so far. I will ignore the lowest assignment grade (or ignore non-submission of one HW).

30% Lab preparation, report and presentation.

Mapping grades to letters. The numeric course grade will be mapped as in Table 2.

0.3 Ethics

Ethical research in security The material we learn in this course includes discussion of many vulnerabilities. You may be curious to check for this or other vulnerabilities in different systems. Please *consult with the lecturer* or another experienced researcher, before even attempting any test or experiment. Such experiments may cause unexpected damages in many ways, and may very well be illegal or break relevant codes of ethics.

One damage, which is relatively less severe, is the efforts spent by system-defenders (sysadmins, security experts, etc.), when an experiment is detected. Note that detection is likely, since security professionals invest many efforts in detecting what seems to be like attempts at exploring and detecting vulnerabilities. Beyond the waste of time and effort that this may cause, another possible result may be that you will find yourself under investigation or worse. Don't make this mistake, which has ruined the careers - and even lives - of talented individuals.

Finally *do not consider* to engage in unauthorized 'hacking', during or after the course. This activity is much less fun and glamorous than it appears in the media - and, regardless of any 'ethical/moral' restrictions you may try to place on your activities, hacking may result in damages to different individuals and organizations, in ways which are hard to determine in advance. Furthermore, there is a high risk of being caught by law-enforcing agencies - or being blackmailed or otherwise engaged with dangerous and criminal elements.

If you find yourself to be talented in this area of cybersecurity, do consider by all means continuing studies, research and work in this exciting area - but in a legitimate, supervised manner. If you are talented and hard working, there will be excellent financial rewards and interesting, exciting work.

Academic Honesty This course involves individual and team assignments. Individual assignments should be done by each student alone, consulting, when necessary, the course staff and *not* other students. However, students are allowed and even encouraged to send questions related to the material studied, even if these questions are also related to the assignments, as well as questions for clarifications of the assignments, to the course's shared forum (Piazza). You should *not* ask peer students about solutions, hints, directions and so on. Questions of this kind, i.e., about assignments and solutions, may be presented only to the course staff (in person, email or Piazza).

Team assignments should be done in fair cooperation among team members. If some team members are not contributing, contact the lecturer soon and we will

find a solution, typically, changing the membership of the team (giving smaller individual projects if necessary). Don't wait till it's too late to fix things!

On top of this, all students should act in accordance with the Guidelines for Academic Integrity at the University of Connecticut. If you have questions about academic integrity or intellectual property, you should consult with your instructor. Additionally, consult UConn's guidelines for academic integrity.

Violations of this policy will be considered violations of the academic integrity policy and will be reported to the Academic Integrity Hearing Board. Consequences may include (but are not limited to) failure of the class.

Student Conduct Code Students are expected to conduct themselves in accordance with UConn's Student Conduct Code.

Copyright My lectures, notes, handouts, and displays are protected by state common law and federal copyright law. They are my own original expression. Students may take notes. In addition, we will appreciate if you would be willing to release your created notes and solutions. Students will be consulted before using their solutions either with or without their name.

Students with Disabilities The University of Connecticut is committed to protecting the rights of individuals with disabilities and assuring that the learning environment is accessible. If you anticipate or experience physical or academic barriers based on disability or pregnancy, please let me know immediately so that we can discuss options. Students who require accommodations should contact the Center for Students with Disabilities, Wilbur Cross Building Room 204, (860) 486-2020, or `http://csd.uconn.edu/`.

Week of	Contents
Aug. 29	Overview, ethics, vulnerabilities, malware
Sept 5	Web security and privacy
Sept 12	Routing security 1
Sept 19	Routing security 2
Sept 26	Routing security 3, recitation
Oct 3	DNS security
Oct 10	Reconnaissance and Scanning
Oct 17	Basic Tools: Firewalls, Filters, ...
Oct 24	Recitation and makeup
Oct 31	Denial of Service (DoS) 1
Nov 7	Denial of Service (DoS) 2
Nov 14	IP and Transport security
Nov 21	Thanksgiving
Nov 28	Student presentations
Dec 5	Link security, recitation and makeup

Table 1: CSE4402 Network security course plan, spring'23.

Numeric course grade g	Assigned course grade	Grade Points
90+	A	4.0
86-89	A-	3.7
82-85	B+	3.3
79-81	B	3.0
77-79	B-	2.7
74-76	C+	2.3
71-73	C	2.0
68-70	C-	1.7
65-67	D+	1.3
62-64	D	1.0
59-61	D-	.7
0-58	F	0

Table 2: Grading Scale

Bibliography

[1] William R Cheswick, Steven M Bellovin, and Aviel D Rubin. *Firewalls and Internet security: repelling the wily hacker*. Addison-Wesley Longman Publishing Co., Inc., 2003. Available in safaribooksonline.com.

[2] Wenliang Du. *Computer and Internet Security*. `https://www.handsonsecurity.net/index.html`, 2019.

[3] Amir Herzberg. *Foundations of Cybersecurity: Applied Introduction to Cryptography*. World Scientific Publishing, 2021.

[4] James F Kurose and Keith W Ross. *Computer networking: a top-down approach*. Addison-Wesley Reading, 2010.

[5] Gordon Fyodor Lyon. *Nmap network scanning: The official Nmap project guide to network discovery and security scanning*. Insecure, 2009.

[6] Michal Zalewski. *The tangled Web: A guide to securing modern web applications*. No Starch Press, 2012. Available in safaribooksonline.com.