

Syllabus

Course Info and Contact Information

- Course Name: CSE 468, Computer Network Security
- Instructor: Jed Crandall
- Email: jedimaestro@asu.edu
- Meeting Times: Tuesday and Thursday, 10:30am to 11:45am
- Meeting Location: Tempe - CDN68
- Online Discussions: Canvas

Office Hours

BYENG 574, 12pm to 1:30pm on Thursdays. I'll also be on Jitsi while I'm in office hours in case you can't make it physically. If you make it to the physical office or to the Jitsi room by 1:30pm I can stay until almost 2pm.

TA and office hours

You can contact the TA through Canvas. Her office hours are TBA.

Course Description

Practical network security exposure and hands-on experience about basic security concepts, case studies and useful tools.

Course Objectives

- Students will gain an understanding of both symmetric and asymmetric applied cryptography.
- Students will gain an understanding of Network Intrusion Detections Systems (NIDS) and techniques for evading NIDS.
- Students will gain an understanding of how NIDS is applied around the world by various nation states for information controls (e.g., Internet censorship).
- Students will gain an understanding of basic tools used for network security analysis.

Course Learning Outcomes

- Students will identify if a given cryptosystem is symmetric or asymmetric.
- Students will identify if a cryptosystem has perfect forward secrecy.
- Students will identify NIDS evasions within a packet capture using industry standard tools, including Wireshark.
- Students will compare the NIDS systems and related evasion techniques that various nation states around the world use for information controls.
- Students will identify different types of network vulnerabilities.

Enrollment Requirements

Prerequisite(s) with C or better: Computer Science BS, Computer Systems Engineering BSE, or Software Engineering BS major; CSE 365 OR Computer Science, Computer Engineering, or Software Engineering graduate student OR Visiting University Student.

Grading Policies, Assignments, and Required Materials

There will be three sets of homeworks (crypto, NIDS, and malware/side channels), each totalling up to 100 points for 300 total. Your grade is 100% based on your homework, and will be your total points divided into the 300 possible. Grades are based on the following scale where x is the percentage: $97.0 \leq x \leq 100.0$ is an A+, $93.0 \leq x < 97.0$ is an A, $90.0 \leq x < 93.0$ is an A-, $87.0 \leq x < 90.0$ is a B+, $83.0 \leq x < 87.0$ is a B, $80.0 \leq x < 83.0$ is a B-, $77.0 \leq x < 80.0$ is a C+, $70.0 \leq x < 77.0$ is a C, $60.0 \leq x < 70.0$ is a D, and $x < 60.0$ is an E.

There will also be 10 points per week, or 150 points total, for attendance and participation. Typically, this will be self reported and there will be no in-class quiz. At the end of each week, starting on the week of August 21st, you will submit a weekly report saying how many lectures you attended that week (some weeks, e.g., Thanksgiving week, have only one lecture—don't worry, you won't be marked down for this) and affirming that you did everything required to prepare for class. For each lecture I'll post in Canvas a video to watch, a paper to read, or some task that will require about an hour to prepare. If I suspect that students are not self-reporting accurately and honestly (e.g., because the head counts differ from the students claiming to have been in class, or blank stares when I ask about the preparation material), I reserve the right to give in-class, unannounced, 5-point quizzes that will count as half of your points for that week (the self reporting being reduced to 5 points out of 10 for the week in that case). Students with excused absences (you should email me before class when possible in such cases) will be allowed to make up the quiz over email.

There is no textbook for the course, neither required nor recommended. All materials used for the course lectures and assignments will be widely and publicly available and/or licensed open source.

Absence policies and the conditions under which assigned work can be made up

Everyone is entitled to the following course-specific late policy for every homework assignment, but cannot combine it with any other form of absence forgiveness (e.g., any of them from below): For every hour that an assignment is turned in late, you will lose 1% of the grade. Note that a little after four days late the assignment is worth 0%.

As an alternative to that policy, in every course you are entitled to: - Excused

absences related to religious observances/practices that are in accord with ACD 304-04. - Excused absences related to university sanctioned events/activities that are in accord with ACD 304-02. - Excused absences related to missed class due to military line-of-duty activities that are in accord with ACD 304-11.

Your attendance will be self-recorded in Canvas. Reporting yourself as present when you were actually absent will be considered a violation of academic integrity (same as cheating on an assignment).

Instruction Style

The course will be a combination of lectures and homework assignments. Attendance is required.

For questions and answers regarding course materials and homework please use Canvas or come to office hours, unless there is some compelling reason to use email. Use email for course administrativia (requesting an extension, you need a signature from me for some reason, etc.) Feel free to email me any time for anything, I won't shame you, but if you're asking questions about the homework or lectures you're much more likely to get a timely response in Canvas than via email. If I'm slow to reply in Canvas pinging me over email is fine.

All homeworks should be done in Linux. If you use other OSes you do so at your own risk, and with no guarantee of support from me. If you attempt to do the homeworks in Mac OS, it's probably possible but it's going to be painful and the amount of help I can offer is minimal. The same goes for any BSD-based OS. If your OS of choice is another UNIX, like Solaris, I also can't help you with OS-specific questions and... seriously? If you attempt to do the homework in OSes that don't have a native UNIX-like shell, such as Windows, you will most likely fail. There are exceptions, but unless you've been competing in CtFs with your OS of choice for years and already have an environment set up for dealing with raw files, common file formats, packet captures, encodings, etc., please just use a Linux virtual machine or install Linux somewhere.

You are responsible for your own file backups and time management. E.g., feel free to email me, or send as a private post in Canvas, the day before something is due, "I worked on it all day and then my VM crashed and I lost my file!" I won't shame you, but that's not grounds for an extension and I'm not going to be able to do anything about it to make sure you submit your homework on time. I recommend keeping your code and other work for this course in a *private* repository that you periodically commit to.

Classroom Behavior

Please refrain from anything that will distract you or others from fully engaging in the class. Disruptive behavior will be dealt with according to university policies. While classroom behavior (unlike attendance) is not explicitly part of the grade, you are hereby notified that both your attendance and classroom

behavior are considered as part of your overall performance in the course to the extent allowed by university policies.

You may not record lectures without permission.

Textbook

As stated above, no textbook is required for this course.

Course Topics

1. Cryptography and other foundations of network security, basic tools - Review of crypto basics, with case studies for WEP, WPA, WPA2, WPA3, TLS, GPG, OTR, Signal, Tor, and others -Asymmetric cryptography and semantic security -Basic information theory -Basic tool usage, including Wireshark, tshark, and tcpflow
2. Network Intrusion Detections Systems (NIDSs), firewalls, attacks, and evasion -Firewalls, port scans, and side channel attacks -NIDS and NIDS evasion techniques -Tool usage for NIDS and NIDS evasion, including Zeek and Scapy -Case studies, including NSA QUANTUM INSERT, Russia's TSPU, and China's Great Firewall -Tools for censorship evasion, privacy, and anonymity -Tool usage, including Tor and OONI
3. Malware and side channels -Port scans, tool usage (e.g., nmap and hping3) -Side channels, DNS security -Malware, including worms and viruses, targeted malware, etc.

Assessment

Students will be evaluated on (1) their performance on homework assignments and (2) attendance and participation. There will not be any exams.

Homework Due Dates

Homework due dates will be posted in advance in Canvas and announced in class. All times will be Mountain Standard Time, i.e., Arizona time. Late submissions will be accepted with a 1% reduction of score per hour, as described above.

Academic Integrity

Students in this class must adhere to ASU's academic integrity policy, which can be found at <https://provost.asu.edu/academic-integrity/policy>. Students are responsible for reviewing this policy and understanding each of the areas in which academic dishonesty can occur. In addition, all engineering students are expected to adhere to both the ASU Academic Integrity Honor Code and the Fulton Schools of Engineering Honor Code. All academic integrity violations will be reported to the Fulton Schools of Engineering Academic Integrity Office

(AIO). The AIO maintains record of all violations and has access to academic integrity violations committed in all other ASU college/schools.

Plagiarism and Cheating Policies Specific to This Course

This course has a zero-tolerance policy: -Any violation of the academic integrity policy (detailed below) will lead to a failure on this course. -The violation will be reported to the AIO.

If you need more time to accomplish a homework assignment, please tell the instructor and ask for an extension. Extensions will be considered for circumstances that are/were beyond your control. Do not attempt plagiarism.

For this course, you are allowed to use code snippets that you find on the Internet as long as you specify clearly in the comment of your source code where the code snippets come from, and the source snippets existed before the assignment was assigned. You are not allowed to upload any part of your solution online or show it to other students. Using other students' answers or code, past or present, with or without a citation is seen as a violation of the academic integrity policy. You will not turn in your source code for most assignments, and maybe not any assignment. But if I suspect cheating I reserve the right to require you to come to my office and show me your source code to get full points. All assignments are graded automatically by graders with anti-cheating mechanisms built-in. Do not cheat – it is not worth risking your grade and your academic profile.

Sexual Discrimination

Title IX is a federal law that provides that no person be excluded on the basis of sex from participation in, be denied benefits of, or be subjected to discrimination under any education program or activity. Both Title IX and university policy make clear that sexual violence and harassment based on sex is prohibited. An individual who believes they have been subjected to sexual violence or harassed on the basis of sex can seek support, including counseling and academic support, from the university. If you or someone you know has been harassed on the basis of sex or sexually assaulted, you can find information and resources at <https://sexualviolenceprevention.asu.edu/faqs>. As a mandated reporter, I am obligated to report any information I become aware of regarding alleged acts of sexual discrimination, including sexual violence and dating violence. ASU Counseling Services, <https://eoss.asu.edu/counseling> is available if you wish to discuss any concerns confidentially and privately. ASU online students may access 360 Life Services, <https://goto.asuonline.asu.edu/success/online-resources.html>.

Copyright

All course content and materials, including lectures (Zoom recorded lectures included), are copyrighted materials. You may not share outside the class, upload to online websites not approved by the instructor, sell, or distribute

course content or notes taken during the conduct of the course. See ACD 304-06, “Commercial Note Taking Services” and ABOR Policy 5-308 F.14 for more information.

You must refrain from uploading to any course shell, discussion board, or website used by the course instructor or other course forum, material that is not the student’s original work, unless the students first comply with all applicable copyright laws; faculty members reserve the right to delete materials on the grounds of suspected copyright infringement.

Policy Against Threatening Behavior

Students, faculty, staff, and other individuals do not have an unqualified right of access to university grounds, property, or services. Interfering with the peaceful conduct of university-related business or activities or remaining on campus grounds after a request to leave may be considered a crime. All incidents and allegations of violent or threatening conduct by an ASU student (whether on- or off-campus) must be reported to the ASU Police Department (ASU PD) and the Office of the Dean of Students.

Disability Accommodations

Suitable accommodations will be made for students having disabilities. Students needing accommodations must register with the ASU Disabilities Resource Center and provide documentation of that registration to the instructor. Students should communicate the need for an accommodation in sufficient time for it to be properly arranged. See ACD 304-08, Classroom and Testing Accommodations for Students with Disabilities.

Future Changes

Any information in this syllabus may be subject to change with reasonable advance notice.