Syllabus

Course Info and Contact Information

- Course Name: CSE 548, Advanced Network Security
- Instructor: Jed Crandall
- Email: jedimaestro@asu.edu
- Meeting Times: Mondays and Wednesdays, 12:00pm to 1:15pm
- Meeting Location: Tempe - HLMK351
- Online Discussions: Canvas

Final exam date and info

The final will be in the university-designated final exam slot for the course, which is TBD.

Other exams

The course is divided into three roughly-4-week-long sections, and only the first section has in-person exams. The exam dates will be:

-February 5th

-February 10th

-February 12th

The exams will be in class in the regularly scheduled place and time, unless you make other accomodations through SAILS.

Office Hours

BYENG 574, 9am to 11:45am on Thursdays. I can be on Jitsi while I'm in office hours in case you can't make it physically, but you'll need to email me to remind me to log in.

TA and office hours

Your TA is TBD.

Course Description

"Comprehensive understanding of network security and corresponding solutions, including cryptography, access control, secure Web transactions, e-mail security, and viruses."

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.
- Students will gain an understanding of current research topics in measuring information controls on the Internet.

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 compare different Internet measurements and related experimental methodologies.

Enrollment Requirements

Prerequisite(s): Computer Engineering or Computer Science graduate student or Data Science, Analytics and Engineering PhD or Software Engineering MS OR Online Computer Science nondegree-seeking graduate student.

Grading Policies, Assignments, and Required Materials

There will be three in-person exams, six lab assignments, and a final exam. Your individual grade will be based on two out of the three exams (the first two), two of the lab assignments (the first in each section of three), and the final exam (if you're required to take it). The remaining exam and four lab assignments will contribute to your house's score (details below), which won't affect your grade but might get you a 100 on the final without needing to take it.

There will also be various digital artifact assignments, readings, and other commitments throughout the semester that are not turned in or graded. These non-graded assignments, your regular attendance, and all exams and lab assignments (whether they affect your own personal grade or not) are all part of your performance in the course.

The final is 25% of your individual grade (100 points).

The in-person exam that counts toward your individual grade for the cryptography section of the course are is 25% of your grade, or 100 points total.

The lab assignments that you do individually for the network intrusion detection and malware sections of the course are each 25% of your grade. I.e., 100 points each.

So, your final grade will be calculated out of 400 points total. Your grade is based on digital artifacts, homework, and exams (midterm and final), and will be your total points divided into the 400 possible. Grades are based on the following scale where x is the percentage: 97.0 <= x <= 100.0 is an A+, 93.0 <= x < 97.0 is an A, 90.0 <= x < 93.0 is an A-, 87.0 <= x < 90.0 is a B+, 83.0 <= x < 87.0 is a B, 80.0 <= x < 83.0 is a B-, 77.0 <= x < 80.0 is a C+, 70.0 <= x < 77.0 is a C, 60.0 <= x < 70.0 is a D, and x < 60.0 is an E.

There will be no adjustments to grades at the end of the semester. If you missed a certain grade by a small fraction of a percent, I can't do anything about that for two reasons: (1) fairness to the rest of the class; (2) my own sanity–If I give every student a bump of 0.5%, for example, then students who missed a grade by 0.1% are happy but the students who missed it by 0.6% start emailing me. It's just not tenable to adjust any scores in any way. Grades will not be curved in any way, either.

Attendance will not be recorded and will not be part of your grade, but regular attendance is expected of all students.

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.

Houses

The class will be divided into 4 houses at the beginning of the semester. Each section of the course will have a competition between the four houses as follows:

-In the cryptography section, the first in-person exam will have two parts: the first half of an RSA encryption and the first half of a Diffie-Hellman key exchange. In the second in-person exam, your answers will be passed to another student in your house and the whole house will be judged (it won't affect anyone's grade, just who has to take the final at the end of the semester) based upon correctly doing RSA and Diffie-Hellman end-to-end, in pairs. In the third in-person exam you'll try to break the encryption schemes of other houses for house points. The fist exam will contribute to your individual grade, the second and third will contribute to your house score. Before the first exam each of the four houses needs to let me know (in bits) how large they want the primes to be for their entire house.

-In the network intrusion detection section of the course, each student will submit code for obfuscating a network protocol to upload prime numbers to a Linux

server. This will be graded individually and will affect your individual grade. Then, each house will be allowed to upload a certain number of prime numbers to a server (this is one house lab), and then PCAPs of that will be provided to the whole class (this is the second house lab). Houses can gain points (not for grading, just for the competition) by uploading prime numbers undetected or by detecting the prime numbers of other houses. These points for the last two out of three labs in this section will contribute to your house score.

-In the malware section of the course, each student will submit a tar ball with a Makefile that compiles a Core War warrior. Each student will know something about the compilation environment that the rest of the class doesn't know, the goal being to hide your actual warrior. The entire class will get to see this first round of warriors and analyze them, and then each house can add a certain amount of additional warriors. This is the second lab for this course section and won't affect your individual grade. In the final lab, the warriors between houses will compete, randomly chosen in a pairwise fashion. Houses will be awarded points based on these competitions, to contribute to your house score.

All students who are members of the house with the highest house score at the end of the semester will get 100% on the final without having to take it.

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 lab 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%.

Excused absences for classes will be given without penalty to the grade in the case of (1) a university-sanctioned event ACD 304-02.; (2) religious holidays ACD 304-04.; a list of religious holidays can be found here https://eoss.asu.edu/cora/holidays; (3) work performed in the line-of-duty according SSM 201-18. Students who request an excused absences must follow the policy/procedure guidelines. Excused absences do not relieve students of responsibility for any part of the course work required during the period of absence.

Instructor recording of class sessions

Faculty may record class meetings to make an archived recording available to enrolled students, instructors, or support personnel. Creation of recordings for groups beyond these requires consent from students who are recorded.

Note that class sessions may be recorded, and recordings provided to enrolled students, instructors or instructional support personnel. If you have concerns about being recorded, please contact the course instructor.

Recordings of all class sessions will be posted in Canvas for all students to access for reviewing course materials.

Instruction Style

The course will be a combination of exams, labs, readings, lectures, and other materials. 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 then pinging me over email is fine.

All labs 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 labs 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.

All engineering students are expected to adhere to the ASU Student Honor Code

and the ASU academic integrity policy. Students are responsible for reviewing this policy and understanding each of the areas in which academic dishonesty can occur. If you have taken this course before, you may not reuse or submit any part of your previous assignments without the express written permission from the instructor. All student academic integrity violations are reported to the Fulton Schools of Engineering Academic Integrity Office (AIO). Withdrawing from this course will not absolve you of responsibility for an academic integrity violation and any sanctions that are applied. The AIO maintains a record of all violations and has access to academic integrity violations committed in all other ASU college/schools.

Generative AI

Generative AI is a technology that can often be useful in helping students learn the theories and concepts in this course. However, unless explicitly allowed by your instructor, the use of generative AI tools to complete any portion of a course assignment or exam will be considered academic dishonesty and a violation of the ASU Academic Integrity Policy. Students confirmed to be engaging in non-allowable use of generative AI will be sanctioned according to the academic integrity policy and FSE sanctioning guidelines.

Copyright stuff

You must refrain from uploading to this course shell, discussion board, website used by the course instructor or any other course forum, material that is not your own original work, unless you first comply with all applicable copyright laws. Course instructors reserve the right to delete materials from the course shell on the grounds of suspected copyright infringement.

The contents of this course, including lectures and other instructional materials, are copyrighted materials. Students may not share outside the class, including uploading, selling or distributing course content or notes taken during the conduct of the course. Any recording of class sessions is authorized only for the use of students enrolled in this course during their enrollment in this course. Recordings and excerpts of recordings may not be distributed to others. (see ACD 304–06, "Commercial Note Taking Services" and ABOR Policy 5-308 F.14 for more information).

Threatening behavior

Students, faculty, staff, and other individuals do not have an unqualified right of access to university grounds, property, or services (see SSM 104-02). 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.

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 -Quantum computing and its impact on cryptography -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 their individual exam and lab scores.

Lab Due Dates

Lab 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 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 of this course. -The violation will be reported to the AIO.

If you need more time to accomplish an 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.

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

Syllabus changes: Any information in this syllabus (other than grading and absence policies) may be subject to change with reasonable advance notice.

Photos

Arizona State University requires each enrolled student and university employee to have on file with ASU a current photo that meets ASU's requirements. ASU uses your Photo to identify you, as necessary, to provide you educational and related services as an enrolled student at ASU. If you do not have an acceptable Photo on file with ASU, or if you do not consent to the use of your photo, access to ASU resources, including access to course material or grades (online or in person) may be negatively affected, withheld or denied.

Waiting for an absent instructor

How Long Students Should Wait for an Absent Instructor: In the event the instructor fails to indicate a time obligation, the time obligation will be 15 minutes for class sessions lasting 90 minutes or less, and 30 minutes for class sessions lasting more than 90 minutes. Students may be directed to wait longer by someone from the academic unit if they know the instructor will arrive shortly.