Syllabus

Course Info and Contact Information

- Course Name: CSE 548, Advanced Computer Network Security
- Instructor: Jed Crandall
- Email: jedimaestro@asu.edu
- Meeting Times: Tuesdays and Thursdays, 10:30am to 11:45am
- Meeting Location: Tempe - COORS 174
- Online Discussions: Canvas

Exam dates and info

There will be two in-semester exams, both in the regularly scheduled place and time:

- Thursday, March 5th, 2026
- Thursday, April 16th, 2026

If you miss an exam or are not happy with your score, you can make up or retake exactly one exam during the final exam slot for the course:

- Tuesday, May 5th from 9:50am to 11:40am

Please do not plan to travel away from Tempe before the final exam slot until you have received your scores for both of the two in-semester exams and you're happy with those scores. If you want to retake one of the two exams in the final exam slot, you must register with me and tell me which exam you want to make up or retake. I'll send out instructions about how to do this in Canvas in April. You cannot make up or retake both, exams, only one. You will receive the full time amount for the final exam slot, but I will only print one of the exams for you. If you somehow can't get the two exams done in the three allocated slots for the semester because of excused absences in two or more of those slots, you'll need to work with the Dean of students for other accommodations.

All exams, including the final exam slot, will be in the regular meeting room (COORS 174).

If you attend lectures, make an honest effort to understand what the lectures cover, do the assigned reading, and do your assignments then the exams should be very straightforward.

The exams will be closed book and closed notes, and no scratch paper is allowed. You can have nothing on your desk except for the exam itself, a pen or pencil, and an approved calculator. You will need a calculator. It is extremely foolish to attempt the exams without a calculator. The only calculator that is approved for the exams is a Casio fx-115ES PLUS. If I catch you with any other calculator out during the exam that will be treated as an academic integrity violation.

Office Hours

9am to 11am on Wednesdays. I will be on Jitsi (the word Jitsi is the link). I don't plan to hold physical office hours this semester (that might change).

TA and office hours

Your TA is Siddharth Ghule. You can contact him through Canvas. Don't contact him directly through email or other means other than Canvas. His office hours are Tuesdays and Thursdays 1pm to 3pm on Zoom (the word Zoom is the link).

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

This course basically has three threads that each form part of your grade:

- Mathematical and conceptual fundamentals, including frequency analysis, Fast Fourier Transform, birthday attacks, finite fields, fast modular exponentiation, information theory, ring theory, the Extended Euclidean Algorithm, the discrete logarithm, and IP fragmentation. This is assessed via the exams, with each exam being 25% of your grade, so 50% total.
- Practical tools and the analysis of digital artifacts. There will be approximately five to eight assignments, equally weighted, that together make up 30% of your grade.
- Research papers, both contemporary and classic. You will write a journal throughout the semester about your readings, videos, in-class discussions, etc. and turn it in at the end of the semester. It will be worth 20% of your grade. There may be several checkpoints throughout the semester where you submit your journal so far, those will not count towards the final grade.

The percentage for your grade is out of 100% (50% exams, 30% digital artifact assignments, 20% journal). Grades are based on the following scale where x is the overall percentage for your final grade: - A+ 100% to 97% - A $<$ 97% to 94% - A- $<$ 94% to 90% - B+ $<$ 90% to 87% - B $<$ 87% to 84% - B- $<$ 84% to 80% - C+ $<$ 80% to 76% - C $<$ 76% to 70% - D $<$ 70% to 60% - E $<$ 60% to 0%

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. It will be hard to put together a quality journal if you don't come to class.

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%.

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 lectures and assignments. Attendance is required.

For questions and answers regarding course materials and homework please use Canvas (private messages or the forum) or come to office hours, unless there is some compelling reason to use email. The same is true 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 in all cases 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 can't hurt.

All digital artifacts assignments 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 or the TA. If you attempt to do the assignments 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 assignments 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* git repository that you periodically commit to. (You can use GitHub, but the repo should be marked as private).

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.

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.

Course Topics

The class can be roughly divided into three parts, which are not covered in this order:

1. Confidentiality and cryptography

- Basic math of crypto (finite fields, modular exponentiation)
- Basic tool usage, including Wireshark, tshark, and tcpflow
- Physical, link, and routing layer security (case studies: ARP, BGP)
- Symmetric crypto (case studies: historical ciphers, DES, AES, RC4), including stream ciphers, block chain modes, and linear and differential cryptanalysis
- Wireless network security (case studies: WEP, WPA, WPA2, WPA3)
- Asymmetric crypto for key exchange (case study: Diffie-Hellman)
- Malleable encryption, perfect forward secrecy, future secrecy, and other advanced topics (case study: Signal messenger)
- Quantum computing and its impact on cryptography

2. Availability and socket security

- Information theory
- Basic tool usage, including nmap and Tor
- Firewalls
- Network Intrusion Detection (NIDS) and NIDS evasion
- Internet censorship and evasion (case studies: China's Great Firewall, Russia's TSPU, Tor)
- Analysis of encrypted traffic
- Port scans
- Denial of Service (DoS)
- Side channel attacks

3. Integrity and application-level security

- Fourier transforms and Haddamard transforms
- Ring theory
- Experimental design
- RSA, non-repudiation, and semantic security
- Secure hash functions and authentication

- Application security (case studies: TLS and SSH, including the xz backdoor)
- DNS security
- Malware and targeted attacks
- Software Defined Radio and attacks on radio communications

Assigned readings

For details and links for the assigned reading, please see the course website. The readings will include, but are not limited to...

- Short Chosen-Prefix Collisions for MD5 and the Creation of a Rogue CA Certificate, by Stevens et al.
- We Chat, They Watch How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus, by Knockel et al.
- The Final Nail in WEP's Coffin, by Bittau et al. (about WiFi security)
- AES proposal: rijndael, by Daemen and Rijmen (about the most common block encryption algorithm in use today)
- Fragmentation Considered Poisonous, by Herzberg and Shulman (about DNS cache poisoning)
- Off-The-Record Messaging, by Borisov et al. (about encryption for privacy)
- The classic Diffie-Hellman and RSA papers
- WireWatch: Measuring the security of proprietary network encryption in the global Android ecosystem, by Wang et al.
- The Essence of Command Injection Attacks in Web Applications, by Su and Wassermann
- The Halting Problems of Network Stack Insecurity, by Sassaman et al.
- ZMap, by Durumeric et al. (fast port scanning)
- A Taxonomy and Comparative Analysis of IPv4 Identifier Selection Correctness, Security, and Performance, by Daymude et al.
- Robust TCP Stream Reassembly In the Presence of Adversaries, by Dharmapurikar and Paxson (a classic paper about network intrusion detection)
- TSPU: Russia's Decentralized Censorship System, by Xue et al.
- OpenVPN is Open to VPN Fingerprinting, by Xue et al.
- Tor: The Second-Generation Onion Router, by Dingledine et al.
- Reflections on Trusting Trust, by Thompson (about Trojan Horses)
- Computer viruses: Theory and experiments, by Cohen
- Quantum Algorithms Revisited, by Cleve et al.

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 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 some assignments, 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. Some 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.

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.

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.

In other words, wait 15 minutes for me, then you're free to go.

Future changes

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