Ira A. Fulton Schools of Engineering
Arizona State University

Course Syllabus - Spring A 2021

Software Security (CSE 545)

Course Description

This course will provide students with an understanding of the theories, tools, and techniques to identify, exploit, and mitigate software security vulnerabilities in the network, binary, and web levels. Students will study, in-depth, vulnerability classes to understand how to protect software and how to secure software. We will also cover the history of software security, and ethical considerations. This course will focus on a hands-on approach: In addition to understanding vulnerability classes, students will be required to identify and exploit vulnerabilities.

Specific topics covered include:

- History of Software Security
- Software Security Ethics
- Network Security
- Application Security
- Web Security

Technologies covered:

- C
- x86-64 Assembly
- HTTP
- HTML
- JavaScript
- SQL
- Scripting languages

Course Objectives

Learners will be able to:

- Identify the differences between bugs and vulnerabilities.
- Explain the difficulties inherent in software security.
- Discuss the adversarial mindset as an approach to software security.
- Determine the historical and modern necessity for software security.
- Propose ethical issues inherent in software security.
- Evaluate and apply adversarial mindset to setuid binaries and challenges.
- Analyze, design and prototype a web server backdoor.
- Differentiate between ethical and unethical behavior in regards to identifying and exploiting security vulnerabilities.

- Write a Makefile that creates an executable file from a C program.
- Write a Makefile that creates an executable file from a Python 3 program.
- Develop a network server in C.
- Analyze a complex technical specification.
- Implement a protocol from a technical specification.
- Develop a minimally compliant HTTP 1.1 server in C.
- Demonstrate local network-level security attacks.
- Develop a network program that sniffs all packets on a network interface.
- Apply the Address Resolution Protocol (ARP).
- Implement ARP to impersonate a host on a local network.
- Create a program that can send raw network packets.
- Read x86_64 assembly code.
- Analyze binary program behavior.
- Reverse engineer a password from analyzing a binary x86_64 program.
- Evaluate a local networking situation to determine appropriate attacks and the corresponding defenses.
- Reverse engineer an x86_64 binary application.
- Determine what an application should not be able to do.
- Read assembly language.
- Discuss the project's goal.
- Analyze team project progress and specific contributions of each team member.
- Outline remaining project needs and deliverables and the responsible team member(s).
- Ask probing and clarifying questions to gain specific feedback from the course team.
- Curate relevant resources and reference materials cited in IEEE format.
- Reverse engineer an x86_64 binary application.
- Analyze an x86_64 binary for vulnerabilities.
- Develop exploits that control the behavior of an x86_64 binary.
- Analyze a web application's behavior.
- Identify vulnerabilities in a web application.
- Exploit vulnerabilities in a web application to reveal secret data.
- Reverse engineer binaries and web applications.
- Analyze a binary or web application for vulnerabilities.
- Develop an exploit for a discovered vulnerability.
- Create a patch that fixes a vulnerability in a binary or web application.
- Design, engineer, and write project code.
- Apply professional writing and presentation techniques in a typed report.
- Analyze a web application's behavior.
- Identify vulnerabilities in a web application.
- Exploit vulnerabilities in a web application to reveal secret data.
- Describe project functionality.
- Explain specific connections with the project description and project code.
- Predict performance expectations for PCTF game play.
- Evaluate project performance and results of PCTF game play.
- Propose project improvements.
- Discuss peer contributions across project inception through competition.

Learning Outcomes

Learners completing this course will be able to:

- Explain the history of security vulnerabilities.
- Differentiate between ethical and unethical behavior in regards to identifying and exploiting security vulnerabilities.
- Demonstrate local network-level security attacks.
- Evaluate a local networking situation to determine appropriate attacks and the corresponding defenses.
- Analyze a binary application, describe its behavior, identify security vulnerabilities, and develop an exploit.
- Analyze a web application, describe its behavior, identify security vulnerabilities, and develop an exploit.

Estimated Workload/ Time Commitment Per Week

Average of 20 hours per week

Required Prior Knowledge and Skills

This course will be very challenging, and students are expected to learn the necessary technologies on their own time. If you are not already proficient in the following areas, consider expanding your skills in these areas and take this course at a later time.

- Clear understanding of theoretical and applied industry-relevant operating systems and computer networks (e.g., Ethernet, ARP, Routing, IP Addresses, Fragmentation, ICMP, UDP, TCP, and x86-64 assembly)
- Experience reading technical specifications and documentation.
- Network programming skills: creating raw packets, implementing network protocols, and other foundational networking skills.
- C/C++ Programming
- Scripting language programming (Something similar to Python, Ruby, or PHP)
- Computer Networking
    - Specifically Ethernet, ARP, Routing, IP Addresses, Fragmentation, ICMP, UDP, and TCP
- Compilers
    - Linkers
    - ELF
- Operating Systems
- Computer Architecture
    - Specifically x86-64 assembly
    - System calls
- Familiarity with these tools to understand network traffic, binaries and web applications for your coursework:
    - tcpdump
    - objdump

- gdb
- ltrace
- strace
- pwntools
- Ghidra
- Chrome Developer Tools
- Burp Proxy

Technology Requirements

Hardware

- Standard personal computer with major OS

Software and Other

- Reliable Internet connection with unrestricted access to key websites that are commonly used in software development activities (e.g., GitHub and StackOverflow)
- Linux Operating System, Ubuntu 18.04 64-bit with administrator capability (ability to install new software).
    - You can run this OS in a virtual machine, if it is not your main machine.
- SSH Client (PuTTY for Windows, built-in SSH client for MacOS or Linux)
- gcc compiler (build-essential package on Ubuntu).
- Access to external websites: overthewire.org, wikipedia, etc.
- Python 3 with a pip installation of swpag-client and the scapy module.
- Network traffic capture tools: tcpdump and wireshark.
- Reverse engineering tools such as objdump, Ghidra, or IDA Pro.
- VMware: can be downloaded for free for ASU students.
- A browser to access the web hacking server.
- Access to these tools for your coursework:
    - gcc
    - objdump
    - gdb
    - ltrace
    - strace
    - pwntools
    - Ghidra
    - Chrome Developer Tools
    - Burp Proxy

Textbook and Readings

At the graduate level, inquiry, research, and critical reading are part of the learning experience; however, this course does not have a required textbook. All content is available within the course.

Ira A. Fulton Schools of Engineering
Arizona State University

Course Content

Instruction

Video Lectures
Other Videos
Live Sessions (e.g. Live Events hosted by the faculty and Virtual Office Hours hosted by other members of the course team)

Assessments

In-Video Questions (individual, ungraded, auto-feedback)
Knowledge Check Questions (individual, ungraded, auto-feedback)
Practice Exams (individual, ungraded, auto-feedback)
Assignments (individual, graded, auto-graded)
Team Project Updates (group, ungraded, human feedback)
Team Project (group, graded, human-graded)
Midterm Exam and Final Exam (individual, graded, auto-graded, timed, proctored)

Details of the main instructional and assessment elements this course comprises follow:

Lecture videos: The concepts you need to know will be presented through a collection of video lectures. You may stream these videos for playback within the browser by clicking on their titles or download the videos. Each week has a media guide, which is designed to provide a snapshot description of media components, so you can plan your learning and quickly go back and review material to prepare for coursework and a variety of assessments. To help you develop your own notes, the media guides include some essential questions for students to think about and be able to answer after viewing. This is intended to model how to think about key concepts. To further support learning, all of the videos include transcripts and most include PDF lecture slides. Weekly overview videos, assignment videos, and project-related videos do not have PDF lecture slides because they are not lectures and have associated documents specific to them. The interview videos build context for the course and do not have PDF slides.

In-Video Questions and Knowledge Checks: Designed to support your learning, these are short, ungraded quizzes to test your knowledge of the concepts presented in the lecture videos. You may take your time, review your notes, and learn at your own pace because knowledge checks are untimed. You may retake these as often as you would like at any point in the course. You are encouraged to read the feedback, review your answer choices, and compare them to the correct answers. *With the feedback as your guide, you may use these as opportunities to study for other assessments and tasks in the course.*

Discussion Forums: Discussion forums are present each week in the course. This course has two types of discussion forums: the general weekly discussion forums and discussion forums specific to assignments and projects. Although the course team is engaged in these discussions, the forums are spaces to clarify, support, and enrich student-to-student communication and learning. *If you have specific*

questions that you would like to be considered to be addressed in the weekly Live Event hosted by the instructor, please indicate your request in your post.

Practice Exams: To help you prepare for the midterm exam and final exam, you will have practice exams. The practice exams were designed to simulate the exam experience. Since they are intended to be practice opportunities and to help you learn, they are untimed and ungraded and include feedback. You may engage with your peers in the discussion forums to address questions, share resources and strategies, and provide feedback to help one another learn. You are encouraged to submit questions in the discussion forum for the course team to address during live sessions. *Use the feedback to guide your learning and to study for the midterm and final exams. A study strategy designed for this course is included in the first week to help you prepare for the exams.*

Proctored Exams: You will have two (2) proctored exams. These consist of a midterm exam and a final exam. The midterm exam covers content from weeks 1, 2, 3, and 4 while the final exam is cumulative and covers content from weeks 1, 2, 3, 4, 5, 6, and 7.

You have 2 hours = 120 minutes to complete each exam and 15 minutes for proctoring to be set up. Once you open the exam, your testing session begins and you must complete it in a single session. You will be allowed one (1) attempt to take and complete each exam. *For academic integrity purposes, once grades are released, students will see their overall total scores. Answers to each question will not be provided. No late exams will be permitted.*

Midterm and Final Exam Allowances
Both exams are closed resource exams. No materials, resources, technologies, or communication is permitted during the exam.

- Hardcopy and/or digital books and/or reference materials: None
- Calculators: None
- Notes in any format of any kind: None
- Web: None
- Software: None - and all virtual machines must be closed prior to starting proctoring
- Other technologies and devices: None
- Scratch Paper: Students may have blank scratch paper and writing utensils (e.g. pens and/or pencils) and eraser(s) to use during the exams.
- Miscellaneous: Students are to take the exam in a single session without leaving the testing space (e.g. no bathroom breaks) to ensure proctoring of the entire testing session.

ProctorU is an online proctoring service that allows students to take exams online while ensuring the integrity of the exam for the institution. Additional information and instructions are provided in the *Welcome and Start Here* section of the course. You *must* set up your proctoring 72 hours prior to taking your exams, so complete this early.

Individual Assignments: There are six (6) individual assignments in this course that are part of your overall grade. There is one (1) optional assignment that does not count towards your grade. *There is an automatic 20% grade penalty for each day late past the deadline.*

- *Optional* Makefile Assignment - due at the end of Week 1 on Sunday, January 17th, 2021 at 11:59PM AZ Time.
- Bandit Assignment - due at the end of Week 1 on Sunday, January 17th, 2021 at 11:59PM AZ Time.
- Backdoor Web Server Assignment - due at the end of Week 2 on Sunday, January 24th, 2021 at 11:59PM AZ Time.
- Reflector Assignment - due at the end of Week 3 on Sunday, January 31st, 2021 at 11:59PM AZ Time.
- Crack the Password Assignment - due at the end of Week 3 on Sunday, January 31st, 2021 at 11:59PM AZ Time.
- Binary Hacking Assignment - due at the end of Week 5 on Sunday, February 14th, 2021 at 11:59PM AZ Time.
- Web Hacking Assignment - due at the end of Week 7 on Sunday, February 28th, 2021 at 11:59PM AZ Time.

Team Project: CSE 545: Software Security prepares students for a cybersecurity career by teaching ethical hacking concepts. The purpose of the project and the Project Capture the Flag (PCTF) is to reinforce these concepts with hands-on, team-based exercises, where students will demonstrate their cybersecurity knowledge and skills by first building a project (software) to help them win the PCTF. In the PCTF, in addition to their project, the students will use the skills that they have developed in the class of analyzing software for vulnerabilities and developing exploits. There are three (3) project components associated with this team project and live PCTF game play. The Final Team Report is what you will be using for the MCS Portfolio Submission (optional).

- PCTF Project Proposal (ungraded) - due at the end of Week 3 on Sunday, January 31st, 2021 at 11:59PM AZ Time.
- PCTF Status Update (ungraded) - due at the end of Week 4 on Sunday, February 7th, 2021 at 11:59PM AZ Time.
- PCTF Final Team Report (graded, 30% of your overall course grade) - due at the end of Week 7 on Sunday, February 28th, 2021 at 11:59PM AZ Time.*There is an automatic 20% grade penalty for each day late past the deadline.*

Course Grade Breakdown

Course Work	**Quantity**	**Percentage**

		of Grade
Individual Assignments	6	50%
Team Course Project*	1	30%
Midterm exam	1	10%
Final exam	1	10%

**The instructor reserves the right to adjust individual grades based on, but not limited to: workload imbalance, inappropriate behavior, lack of productivity, violations of academic integrity, etc.*

Grade Scale

Notes: You must earn a cumulative grade of 70% or above to earn a "C" in this course. You must earn at least a "C" to receive graduate credit. No graded course components will be dropped. Grades will not be rounded. The full list of cutoffs that will be used to generate your letter grade:

A+	99% - 100%
A	94% - 98.99%
A-	90% - 93.99%
B+	86% - 89.99%
B	83% - 85.99%
B-	80% - 82.99%
C+	76% - 79.99%
C	70% - 75.99%
E	<70%

Course Schedule

Week/Module	Begin Date	End Date

Week 1: Introduction to Software Security	Monday, January 11, 2021 at 12:01 AM AZ Time	Sunday, January 17, 2021 at 11:59 PM AZ Time
Week 2: Network Security Part 1	Monday, January 18, 2021 at 12:01 AM AZ Time	Sunday, January 24, 2021 at 11:59 PM AZ Time
Week 3: Network Security Part 2	Monday, January 25, 2021 at 12:01 AM AZ Time	Sunday, January 31, 2021 at 11:59 PM AZ Time
Week 4: Application Security Part 1	Monday, February 1, 2021 at 12:01 AM AZ Time	Sunday, February 7, 2021 at 11:59 PM AZ Time
Midterm Exam	Thursday, February 4, 2021 at 12:01 AM AZ time	Tuesday, February 9, 2021 at 11:59 PM AZ time
Week 5: Application Security Part 2	Monday, February 8, 2021 at 12:01 AM AZ Time	Sunday, February 14, 2021 at 11:59 PM AZ Time
Week 6: Web Security Part 1	Monday, February 15 2021 at 12:01 AM AZ Time	Sunday, February 21, 2021 at 11:59 PM AZ Time
Week 7: Web Security Part 2	Monday, February 22, 2021 at 12:01 AM AZ Time	Sunday, February 28, 2021 at 11:59 PM AZ time
Final Exam	Wednesday, February 24, 2021 at 12:01 AM AZ time	Wednesday, March 3, 2021 at 11:59 PM AZ time

**Grades are due March 5th, 2021 (Please see the ASU Academic Calendar for additional information.)*

Live Events

The list of Live Events for this course are located under the “Live Events” page in your Coursera course. The Live Event schedule will not be available until *after* the official course start date: Monday, January 11, 2021.

Live Sessions - Weekly

Live Sessions are a valuable part of the learning experience because students can meet with the course instructor and fellow classmates to learn more about course topics, special topics within the field, and discuss coursework. The official weekly schedule for these events will be announced once the course starts. If you are able to attend these Live Sessions, you are strongly encouraged to do so. If you have specific questions or topics of interest to be discussed during the live events, please indicate your request in your discussion forum post. Although it may not be possible to address all requests live, the instructor is interested in tailoring the live events to your questions and interests. The instructor will be following a set agenda, so please be mindful of that when engaging in the live session.

Live Sessions hosted by the faculty will be recorded and uploaded to the wrap-up section of each week.

Live Sessions Expectations

The environment should remain professional at all times. Inappropriate content/visuals, language, tone, feedback, etc. will not be tolerated, reported and subject to disciplinary action. Review the Policy Regarding Expected Classroom Behavior section of the syllabus and the Student Code of Conduct for more detailed information.

Virtual Office Hours - Weekly

Virtual Office Hours offer a chance for students to get their questions answered from the course team. The official weekly schedule for office hours will be announced once the course starts.

Virtual office hours are recorded, but not uploaded into the course.

Virtual Office Hour Expectations

Although the course team is responsive to trends in the discussion forums and mcsonline@asu.edu emails, these sessions focus on addressing students' specific questions related to content: clarifications, reteaching, assessment review, etc. These sessions are not intended to address program or course design questions or feedback. Teaching assistants do not have the authority to weigh in or make decisions regarding those items, so please do not include those at this time. These sessions are specific to helping students learn materials and understand various course assessments. Feedback of that nature is best addressed in the communication channel: mcsonline@asu.edu and please include it in your course survey.

The environment should remain professional at all times. Inappropriate content/visuals, language, tone, feedback, etc. will not be tolerated, reported and subject to disciplinary action. Review the Policy Regarding Expected Classroom Behavior section of the syllabus and the Student Code of Conduct for more detailed information.

Assignment Deadlines

Unless otherwise noted (e.g., in a course announcement), all graded work is due on Sundays at 11:59 PM Arizona time. *A late penalty of 20% for each day late will be applied for work submitted after the scheduled due date and time.*

Course Outline with Assignments

Week 1: Introduction to Software Security

Content

- ❏ Introduction to Software Security
- ❏ History of Software Security
- ❏ Ethics of Software Security

Assignments

- ❏ Bandit Assignment

- ❏ Makefile Assignment (optional)
- ❏ Team Formation Survey due by January 16th

Week 2: Network Security Part 1

Content

- ❏ Local Area Network Attacks

Assignments

- ❏ C Backdoor Web Server Assignment

Week 3: Network Security Part 2

Content

- ❏ Wide Area Network Attacks

Assignments

- ❏ Reflector Assignment
- ❏ Crack the Password Assignment
- ❏ PCTF Team Project Proposal

Week 4: Application Security Part 1

Content

- ❏ Overview of Application Security
- ❏ UNIX Security
- ❏ Reverse Engineering

Assignments

- ❏ PCTF Team Status Update

Midterm Exam

Content

- ❏ Covers content from weeks 1, 2, 3, and 4.

Assignments

- ❏ Midterm Exam - Proctored, Timed
  Available Thursday, February 4th, 2021 at 12:01 AM AZ Time - Tuesday, February 9th, 2021 at 11:59 PM AZ time

Week 5: Application Security Part 2

Content

- ❏ Application Vulnerabilities

Assignments

- ❏ Binary Hacking Assignment

Week 6: Web Security Part 1

Content

- ❏ Design of the Web
- ❏ Web Applications

Assignments

- ❏ PCTF Competition (Game Play)

Week 7: Web Security Part 2

Content

- ❏ Web Applications

Assignments

- ❏ Web Hacking Assignment
- ❏ PCTF Team Final Report
- ❏ Course Survey (*strongly encouraged, appreciated, and used by the course team, but optional*)
- ❏ Request for Faculty Review: MCS Project Portfolio Submission (*optional*)

Final Exam

Content

- ❏ Covers content from weeks 1, 2, 3, 4, 5, 6, and 7 (cumulative).

Assignments

- ❏ Final Exam - Proctored, Timed
  Available Wednesday, February 24th, 2021 at 12:01 AM AZ Time- Wednesday, March 3rd, 2021 at 11:59 PM AZ time

Policies

All ASU and Coursera policies will be enforced during this course. For policy details, please consult the MCS Graduate Handbook 2020-2021 and the MCS Onboarding Course.

Absence Policies

There are no required or mandatory attendance events in this online course. Live Events, both Live Sessions hosted by the faculty and Virtual Office Hours hosted by the course team do not take attendance. Absence from teamwork and group work are not tolerated: it is expected that every group member will participate in the group work. The instructor reserves the right to adjust individual grades based on, but not limited to: workload imbalance, inappropriate behavior, lack of productivity, etc.

Students are to complete all graded coursework (e.g., assignments, projects and exams). If exceptions for graded coursework deadlines need to be made for excused absences, please reach out to the course team by using the mcsonline@asu.edu email address (these need to be built into the course). Review the exam availability windows and schedule accordingly. The exam availability windows allow for your own flexibility and you are expected to plan ahead. Personal travel does not qualify as an excused absence and does not guarantee an exception.

Review the resources for what qualifies as an excused absence and review the late penalties in the Assignment Deadlines section of the syllabus and the course:

a. Excused absences related to religious observances/practices that are in accord with ACD 304–04, “Accommodation for Religious Practices”
b. Excused absences related to university sanctioned events/activities that are in accord with ACD 304–02, “Missed Classes Due to University-Sanctioned Activities”
c. Excused absences related to missed class due to military line-of-duty activities that are in accord with ACD 304–11, “Missed Class Due to Military Line-of-Duty Activities,” and SSM 201–18, “Accommodating Active Duty Military”

Policy Regarding Expected Classroom Behavior

The aim of education is the intellectual, personal, social, and ethical development of the individual. The educational process is ideally conducted in an environment that encourages reasoned discourse, intellectual honesty, openness to constructive change, and respect for the rights of all individuals. Self-discipline and a respect for the rights of others in the university community are necessary for the fulfillment of such goals. An instructor may withdraw a student from a course with a mark of “W” or “E” or employ other interventions when the student’s behavior disrupts the educational process. For more information, review SSM 201–10.

If you identify something as unacceptable classroom behavior on the class platform (e.g., Coursera discussion forum) or communication channels (e.g., Zoom, virtual live session, virtual office hours, Slack, etc.), please notify the course team using the mcsonline@asu.edu email. In the discussion forums, you can also flag the post for our attention. For more specifics on appropriate participation, please review our Netiquette infographic in the course.

Our classroom community rules are to:

- Be professional
- Be positive
- Be polite
- Be proactive

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 a record of all violations and has access to academic integrity violations committed in all other ASU colleges/schools.

Plagiarism and Cheating

Plagiarism or any form of cheating in assignments, projects, or exams is subject to serious academic penalty. To understand your responsibilities as a student read: ASU Student Code of Conduct and ASU Student Academic Integrity Policy.

You are allowed to use code snippets that you find online (StackOverflow or otherwise) provided that you provide, as part of a comment in your source code, the source of the code. These snippets should not constitute a significant part of your code. Using another student's code, past or present, even with a citation is a violation of the academic integrity policy.

There is a zero tolerance policy in this class: any violation of the academic integrity policies will result in a zero on the assignment and the violation will be reported.

Examples of academic integrity violations include (*but are not limited to*):

- Sharing code with a fellow student (even if it is only a few lines).
- Collaborating on code with a fellow student.
- Submitting another student's and/or other students' code as your own.
- Submitting a prior student's code and/or other students' code as your own.

Posting your projects online is expressly forbidden, and will be considered a violation of the academic integrity policy. Note that this includes working out of a public Github repo. The Github Student Developer Pack provides unlimited private repositories while you are a student. If you want to impress employers with your coding abilities, create an open-source project that is done outside of class.

Copyright

All course content and materials, including lectures (Zoom recorded lectures included), are copyrighted materials and students 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 nadam "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 (SSM 104-02)

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 Student Accessibility and Inclusive Learning Services (SAILS). Students should communicate the need for an accommodation at the beginning of each course so there is sufficient time for it to be properly arranged. These requests should be submitted through Connect. See ACD 304-08 Classroom and Testing Accommodations for Students with Disabilities. ASU Student Accessibility and Inclusive Learning Services will send the instructor of record a notification of approved accommodations and students are copied on these letters. It is recommended that students reply to the faculty notification letters, introduce themselves to their instructor, and share anything they might want to disclose.

Harassment and Sexual Discrimination

Arizona State University is committed to providing an environment free of discrimination, harassment, or retaliation for the entire university community, including all students, faculty members, staff employees, and guests. ASU expressly prohibits discrimination, harassment, and retaliation by employees, students, contractors, or agents of the university based on any protected status: race, color, religion, sex, national origin, age, disability, veteran status, sexual orientation, gender identity, and genetic information.

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.

Mandated sexual harassment reporter: 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.

Disclaimer

Information in the syllabus may be subject to change without advance notice.

Course Faculty

Dr. Adam Doupé created this course.

Adam Doupé, Ph.D.

Dr. Adam Doupé is an Associate Professor in the School of Computing, Informatics, and Decision Systems Engineering (CIDSE) at Arizona State University (ASU) and is the Associate Director of the Center for Cybersecurity and Digital Forensics in the Global Security Initiate at ASU. Dr. Doupé was awarded the Top 5% Faculty Teaching Award for the Fulton Schools of Engineering at ASU for 2016, the Fulton Schools of Engineering Best Teacher Award in 2017 and 2018, the Fulton Schools of Engineering Outstanding Assistant Professor Award in 2017, and the NSF CAREER award in 2017. Dr. Doupé has co-authored over 30 peer-reviewed scholarly publications and served on program committees of well-known international security conferences. As a founding member of the Order of the Overflow, Dr. Doupé has organized the DEF CON Capture The Flag competition since 2018.