CSC 696I – Advanced Topics in Security

701 Gould-Simpson, MW 2:00-3:15 PM MST

Course Description

The goal of this graduate seminar is to learn more about research in the general field of computer security. We will review and critique research papers spanning current, important topics in security. Specific topics will be determined by the current literature and by instructor and student interest. Students will also strengthen research skills by conducting a research project on a security topic of their choice.

Instructor and Contact Information

Instructor: Prof. Quinn Burke

E-mail: qkb@arizona.edu

Office Hours: Monday 3:15-4:15 PM MST (or by appointment)

Instructor homepage: https://www.quinnburke.net/

Course homepage: https://d2l.arizona.edu/d2l/home/1800010

D2L information: 443-2264-1 CSC 696I 001

Course Format and Teaching Methods

This is a seminar course and will be based on in-class group discussion, paper presentations, and a semester-long project.

Course Objectives

Students will deeply engage with computer security research by reading published research articles, participating in simulated peer review, and conducting a research project in computer security. The readings will cover important areas in computer security research, such as software supply chain security, agentic/AI security, systems security, and web security.

Expected Learning Outcomes

After completing this course, students will be equipped to fluently understand advances in computer security research. They will also learn to formulate problems, critique methodologies, and conduct research independently.

Degree Learning Outcomes

This course is part of the Computer Science graduate degree learning outcomes assessment process. In this course, students will be assessed (by the instructor) on the following degree learning outcome(s):

- Analyze published research, explain scientific findings, and evaluate significance and impact as it relates to a stated research problem.
- Analyze published research, explain scientific findings, and evaluate significance and impact of the extent to which proposed solutions address problems.

Transferable Career Skills

National Association of Colleges and Employers (NACE) Career Readiness:

Career readiness is a foundation from which to demonstrate requisite core competencies that

broadly prepare the college-educated for success in the workplace and lifelong career management. For new college graduates, career readiness is key to ensuring successful entrance into the workforce.

There are eight career readiness competencies, each of which can be demonstrated in a variety of ways. (NACE, 2025)

- Career & Self Development
- Communication
- Critical Thinking
- Equity & Inclusion
- Leadership
- Professionalism
- Teamwork
- Technology

In this course, we will focus on the following competencies:

- Career & Self Development: The course content will focus on current and important topics in security research to help students learn the foundational problems and tools used in security research, allowing them to pursue security-related careers.
- Critical Thinking: Students will engage in technical discussions and critique modern security research to improve their critical thinking skills as scientists and engineers.
- Communication: The course includes presentations and student-led discussions, which will help students learn how to communicate effectively with technical teams.

Makeup Policy for Students Who Register Late

Students who register late may submit assignments due prior to enrollment for full credit.

Course Communications

Course communication will be done via D2L (and official UA email, as applicable).

Required Texts or Readings

No textbooks are required. Required course readings will be original published research articles as listed in the course schedule. Availability: Access to all digital articles is provided by the University library via NetID credentials.

Assignments and Examinations: Schedule/Due Dates

The is a seminar course and will be based on in-class group discussion, paper presentations, and a semester-long project. There are no exams.

Most lectures will be discussion-based, covering 1-2 research papers per class. Students must submit conference-style paper reviews before class (via D2L). Students are expected to come to class having read the papers and be prepared to discuss and critique them (scope, motivation, methodology, strengths, weaknesses, evaluation, etc.). The instructor will facilitate discussion and provide additional background context for each module. Other lectures may consist of alternative research-based activities (e.g., artifact evaluation) and guest lectures. **Note that this schedule may change** during the semester based on class interest, invited guest lectures, and instructor travel. All changes will be announced by email as early as possible.

A number of sessions are reserved for student-led discussion, where a student will present the paper then facilitate discussion (much like a conference Program Chair) of the paper. Each student will present **approximately twice** over the semester (the exact number depends on class size, and student will select which paper(s) they present).

Students will also complete a course project on a security topic of their choice, culminating in a final in-class presentation and a short conference-style research report (any paper template is fine) due at the end of the semester. A project idea proposal will be due by end of day October 7, 2026. A mid-semester project status update will be due by end of day November 2, 2026. The project can be a security idea you have always wanted to pursue, a security angle on your current research, a reproduction study of a published work, etc. The only requirement is that it must intersect with security. The instructor will provide suggestions and feedback on project ideas, and students are encouraged to discuss their ideas with the instructor early in the semester. Detailed requirements for each project milestone will be posted on D2L.

Final Examination

There will be no final exam. The final project report will be due by end of day on 12/14/2026.

Grading Scale and Policies

Component	Weight	Description
Paper reviews	**25%**	Grading based on paper reviews being submitted on time and containing structured critiques. The **three lowest review scores are dropped**, so no documentation is needed for a missed review. This applies to reviews only—in-class participation is graded separately, and you are still expected to attend and come prepared.
In-class participation	**25%**	Grading based on students coming to lectures prepared with questions and discussion points, and engaging with other student critiques.
Paper presentations	**20%**	Grading is based on student coverage of the assigned paper (motivation, scope, methodology, key results, and conclusions) and engagement with other students while leading the discussion.
Course project	**30%**	A proposal, a mid-semester status report, and a final presentation and report, which together should form a self-contained research artifact. Requirements and the weight of each milestone are posted on D2L.

This course will use Regular Grades. See the University policy regarding grades and grading systems: https://catalog.arizona.edu/policy/courses-credit/grading/grading-system. Reviews and project reports submitted late will be deducted 10% per day. Extra credit opportunities may be given at the discretion of the instructor in the form of additional paper reviews or paper presentations.

Incomplete (I) or Withdrawal (W):

Requests for incomplete (I) or withdrawal (W) must be made in accordance with University policies, which are available at https://catalog.arizona.edu/policy/courses-credit/grading/grading-system.

Dispute of Grade Policy:
Any disputes must be filed by end of day on the last lecture.

Class Participation Policies

The UA's policy concerning Class Attendance & Participation is available at: https://catalog.arizona.edu/policy/courses-credit/courses/class-attendance-participation. The course learning objectives are based on effective in-class discussion. As such, attendance and participation in discussion are expected at all lectures. Discussion will be evaluated on the quality

and frequency of student engagement with the material and other students through questions, answers, and critiques on the research papers covered in the lectures.

Class Absence Policies

The UA policy regarding absences for any sincerely held religious belief, observance or practice will be accommodated where reasonable: http://policy.arizona.edu/human-resources/religious-accommodation-policy. Absences pre-approved by the UA Dean of Students (or dean's designee) will be honored: https://deanofstudents.arizona.edu/policies/attendance-policies-and-practices.

Participating in this course, attending discussions and other course events are vital to the learning process. As such, attendance is expected at all lectures. Although absences may not affect a student's final course grade, if you anticipate being absent, are unexpectedly absent, or are unable to participate in class online activities, please contact me as soon as possible. To request a disability-related accommodation to this attendance policy, please contact the Disability Resource Center at (520) 621-3268 or drc-info@email.arizona.edu. If you are experiencing unexpected barriers to your success in your courses, the Dean of Students Office is a central support resource for all students and may be helpful. The Dean of Students Office is located in the Robert L. Nugent Building, Main Floor, Room 100, or call (520) 621-7057.

Scheduled Topic and Activities

Week			Notes
Introduction			
1	**Aug 24:** Class intro & syllabus; how to read a paper		Start thinking about project topics Optional reading: How to Read a Paper, Mitzenmacher on Reading
Software Supply Chain Security			
1		**Aug 26:** Supply Chain Attack Taxonomy	Optional reading: Reflections on Trusting Trust
2	**Aug 31:** in-toto	**Sep 2:** Reproducible Builds	Student presentation signup
3	***Sep 7: No class (Labor Day)***	**Sep 9:** Pushed by Accident	
4	**Sep 14:** Hypocrite Commits	**Sep 16:** Project brainstorming session	Bring a short written project idea (post to D2L the day before)
LLM & Agent Security			
5	**Sep 21:** Agentic AI Threat Landscape	**Sep 23:** Indirect Prompt Injection	
6	**Sep 28:** Jailbroken	**Sep 30:** LLM App Data Collection	
7	**Oct 5:** GCG Attack	**Oct 7:** StruQ	**Project proposal due** (Oct 9)

Week			Notes
8	**Oct 12:** AgentDojo	**Oct 14:** IsolateGPT	
9	**Oct 19:** Extracting Training Data	**Oct 21:** Poisoning Web-Scale Data	
Systems Security			
10	**Oct 26:** SoK: TEE Design	**Oct 28:** TDX Demystified	
11	**Nov 2:** SGX.Fail	**Nov 4:** Project development session	**Status report due** (Nov 2)
12	**Nov 9:** Nimble	***Nov 11: No class (Veterans Day)***	
13	**Nov 16:** syncfs Side Channels	**Nov 18:** Branch Shadowing	
Web Security			
14	**Nov 23:** SoK: Browser Security	**Nov 25:** Site Isolation	
15	**Nov 30:** CSP Is Dead	**Dec 2:** Silent Spring	
16	**Dec 7:** Cached and Confused	**Dec 9:** Final project presentations	
Finals			
17	**Dec 14:** No class meeting		**Final paper due** (Dec 14)

Classroom Behavior Policy

To foster a positive learning environment, students and instructors have a shared responsibility. We want a safe, welcoming, and inclusive environment where all of us feel comfortable with each other and where we can challenge ourselves to succeed. To that end, our focus is on the tasks at hand and not on extraneous activities (e.g., texting, chatting, reading a newspaper, making phone calls, web surfing, etc.).

Safety on Campus and in the Classroom

For a list of emergency procedures for all types of incidents, please visit the website of the Critical Incident Response Team (CIRT): https://cirt.arizona.edu/case-emergency/overview.

Also watch the video available at: https://arizona.sabacloud.com/Saba/Web_spf/NA7P1PRD161/app/me/ledetail;spf-url=common%2Flearningeventdetail%2Fcrtfy000000000003841.

University-wide Policies link

All students must familiarize themselves with the policies and resources at the following link: https://catalog.arizona.edu/syllabus-policies:

- Threatening Behavior Policy
- Student Code of Academic Integrity
- Nondiscrimination and Anti-Harassment Policy
- Disability Syllabus Statement
- Religious Accommodation Policy
- Absences pre-approved by the University Dean of Students (or dean's designee) will be honored.

Department-wide Syllabus Policies and Resources link

Links to the following departmental syllabus policies and resources are provided here, https://www.cs.arizona.edu/cs-course-syllabus-policies:

- Department Code of Conduct
- Illnesses and Emergencies
- Obtaining Help
- Confidentiality of Student Records
- Land Acknowledgement Statement

Subject to Change Statement

Information contained in the course syllabus, other than the grade and absence policy, may be subject to change with advance notice, as deemed appropriate by the instructor.

Ethics Statement

This course includes topics related to computer security. We may cover technologies whose abuse could infringe on the rights of others. As computer scientists, we rely on the ethical use of these technologies. Unethical use includes circumvention of any existing security mechanisms for any purpose, or the dissemination, promotion, or exploitation of vulnerabilities of these services. Any activity outside the letter or spirit of these guidelines will be reported to the proper authorities and may result in dismissal from the class and possibly more severe academic and legal sanctions.