CS361S: Computer Security and Privacy

1. Course Contact

Dr. Shravan Narayan
Classes: 12:30pm to 2pm at JGB 2.218 on Tuesday, Thursday
Canvas: https://utexas.instructure.com/courses/1421761

Office Hours: At GDC 6.430, 2pm to 3pm on Wednesday and 2pm to 3pm on Thursday.
(Emailing to let me know you're coming helps. Also email me if you need alternate meeting times)
Email: shr@cs.utexas.edu (Expect a response within 48 hours)

TA: Darius Grassi dwg@utexas.edu (Always cc shr@cs.utexas.edu)
TA office hours: 1:00-2:00 pm every Friday (and Mondays on the weeks that have an assignment that is use), GDC room 6.416

Syllabus last updated: Nov 11th, 2025

2. Course overview, objectives, and requirements

This course focuses on computer security, covering a wide range of topics on both the defensive and offensive side of this field. Among these will be systems security and exploitation (e.g., buffer overflows and return-oriented programming), sandboxing and isolation, side channels, network security, JavaScript runtime security and more. The goal of the course is to provide an appreciation of how to think adversarially with respect to computer systems as well as an appreciation of how to reason about attacks and defenses.

The formal prerequisite for CS 361S is CS 439 (or 352 or 372) or CS 439H (or 352H or 372H).

At a minimum, students are expected to have knowledge of programming with C, compiling C applications, the memory layout of C applications including stack and heap, as well as standard terms and operations from programming and compilation such as how control flow (branches, indirect function calls) work, what a program counter does etc. Comfort with writing small Python and JavaScript programs and using Linux/UNIX tools, terminals, ssh, debugging tools is also expected. Finally, a basic understanding of computer architecture and at least one CPU ISA (x86, ARM, RISC-V) is expected.

3. Class attendance

The class will use a combination of slides, notes on whiteboard and live demonstrations. The slides will be made available, but you will have to take notes for whiteboard or live demonstrations. We may consider opening the collaborative class notes option on Canvas if there is enough interest for this.

If you are unable to attend some classes, it will be your responsibility to talk to your classmates to catch up with notes etc. You are always welcome to clarify your understanding of material you missed or haven't understood in the office hours.

If you have another class that conflicts with any part of this class, or if you think you cannot attend this class regularly, you should not take this class.

4. Lecture recordings

This class will not be recorded, so attending class regularly will be necessary to keep up with the material, as well as participate in the in-class written quizzes etc.

While there are no currently plans to record this class, this may change. Class recordings, if provided, are reserved only for students in this class for educational purposes and are protected under FERPA. The recordings should not be shared outside the class in any form. Violation of this restriction by a student could lead to Student Misconduct proceedings.

5. Grading

The grading scheme is as follows:

- Perusall readings – 10%
- Assignments (5 to 7) – 35%
- Midterm + Final = 55%. We will pick the higher of two scores computed below
    - Either: Midterm: 25%, Final: 30%
    - Or: Midterm: 15%, Final: 40%
- Course notes contribution bonus: 5% (Substantial contributions only)

Each of these are explained in the next sections.

Grading scheme (Final scores maybe curved by the instructor)

- A : 100% to 94%
- A- : 94% to 90%
- B+ : 90% to 87%
- B : 87% to 84%
- B- : 84% to 80%
- C+ : 80% to 77%
- C : 77% to 74%
- C- : 74% to 70%
- D+ : 70% to 67%
- D : 67% to 64%
- D- : 64% to 61%
- F : 61% to 0%

6. Perusall

We will be using perusal to assign class readings. This may be used to also ask you to comment on the readings or answer questions. There will be one or two readings every week. The expectation is that you will be able to commit time every week to do some of the readings.

7. Assignments

There will be between 5 to 7 assignments. The first assignment is easier and may not count as much as the other assignments towards the overall grade.

You have two late days that you may use to turn in work past the deadline over the entire semester. A late day is a contiguous 24-hour period starting at the assignment due time. Use of partial late days are always rounded up to the next full day. These late days are intended to cover your extension needs for usual circumstances: brief illness, busy with other classes, interviews, travel, extracurricular conflicts, and so on. You do not need to ask permission to use a late day

Assignments maybe assigned as individual assignments or for groups of 2. If you use late days on group assignments, both you and your partner will be charged for every late day that you use, and you both must have late days to use them.

8. Midterm and final exam

This course will have both a midterm and a final exam. There will be no makeup exams except for UT-authorized excuses. We may solely at the discretion of instructor re-weight other components of the grade to account for missed midterms for authorized reasons. See class schedule for dates.

9. Course notes contribution bonus

Canvas has a link the collaborative notes for the course that you can all contribute to and use for your preparations. There is a 5% bonus for substantial contributions to course notes.

What is a substantial contribution? Any contribution of notes for a large chapter, an entire class, or topic. Small typo fixes or adding a sentence here and there does not count as substantial contributions.

10. Policy on Academic Accommodations

The university is committed to creating an accessible and inclusive learning environment consistent with university policy and federal and state law. Please let me know if you experience any barriers to learning so I can work with you to ensure you have equal opportunity to participate fully in this course. If you are a student with a disability, or think you may have a disability, and need accommodation please contact Disability and Access (D&A). Please refer to D&A's website for contact and more information: http://diversity.utexas.edu/disability/. If you are already registered with D&A , please deliver your Accommodation Letter to me as early as possible in the semester so we can discuss your approved accommodation and needs in this course.

11. Academic Integrity

Recall the Student Honor Code: "As a student of The University of Texas at Austin, I shall abide by the core values of the University and uphold academic integrity."

Students who violate University rules on academic dishonesty are subject to disciplinary penalties, including the possibility of failure in the course and/or dismissal from the University. Since such dishonesty harms the individual, all students, and the integrity of the University, policies on academic

dishonesty will be strictly enforced. For further information, please visit the Student Conduct and Academic Integrity Website.

To detect instances of academic integrity violations in programming assignments we may use 3rd party software.

12. Artificial intelligence

The use of artificial intelligence tools (such as ChatGPT) as "assignments solvers" in this class is strictly prohibited. Any use of AI tools detected will always be reported as an attempt to cheat and an official violation of course policy. Use of AI tools as "search engines" is permitted.

13. Religious holy days

Religion (or lack thereof) is an important part of who we are. If a holy day observed by your religion falls during the semester and you require accommodation due to that, please let me know as soon as possible. Email is an acceptable form of communication. To guarantee accommodation around presentations or other big deadlines, I will need notice of at least two weeks. If you are unable (or forget!) to provide that notice, please contact me anyway in case I can still accommodate you.

University-required language: A student who is absent from an examination or cannot meet an assignment deadline due to the observance of a religious holy day may take the exam on an alternate day or submit the assignment up to 24 hours late without penalty, ONLY if proper notice of the planned absence has been given. Notice must be given at least 14 days prior to the classes which will be missed. For religious holy days that fall within the first two weeks of the semester, notice should be given on the first day of the semester. Notice must be personally delivered to the instructor and signed and dated by the instructor, or sent certified mail. Email notification will be accepted if received, but a student submitting email notification must receive email confirmation from the instructor.

14. Class Calendar

The course calendar is here to give you an idea. It is subject to change depending on how quickly we progress through the material. We may add, remove or replace material based on interest.

Note: Assignment start/end dates may also change. Perusall readings will be updated as we go. Pay attention to class announcements for calendar updates.

	Theme	Class Contents
Tue, Aug 26		**No class today**
Thu, Aug 28	Systems Security & Buffer overflows	**Contents** History of Systems Security. Buffer overflows. **Perusall reading 1 due on Sept 4th** Smashing the Stack for Fun and Profit - Aleph One (1996) – reformatted in 2017

		Extra resources Section 30.1 to Section 30.2.1 of Low-Level Software Security by Example - Úlfar Erlingsson, Yves Younan, and Frank Piessens (2010) E.H. Spafford: "The Internet Worm Program: An Analysis" (1988)
Tue, Sep 2	Shellcoding background. Revisiting GDB.	**Assignment 1 available (GDB).** **Contents** How to exploit buffer overflows Quick demo on GDB usage. **Extra resources** GDB documentation: Debugging with GDB
Thu, Sep 4	Shellcoding, other bugs, (Legacy) mitigations for memory safety	**Contents** Shellcoding Other bugs - Integer overflows, format string bugs Canaries, Data Execution Prevention, ASLR **Perusall reading 2 due on Sept 11th** V. van der Veen, N. dutt-Sharma, L. Cavallaro, and H. Bos: "Memory Errors: The Past, the Present, and the Future" (2012) **Extra resources** Exploiting Format String Vulnerabilities – scut (2001) T. de Raadt: "Exploit Mitigation Techniques: An Update after 10 Years" (2013)
Tue, Sep 9	Code reuse I	**Assignment 1 due. Assignment 2 available (Buffer overflow).** **Contents** Return-to-Libc, ROP **Perusall reading 3 due Sept 16th** R. Roemer, E. Buchanan, H. Shacham and S. Savage: "Return-Oriented Programming: Systems, Languages, and Applications" (2012) **Extra resources** Nergal, "The advanced return-into-lib(c) exploits: PaX case study" (2001)

		H. Shacham, The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86) (2007)
Thu, Sep 11	Code Reuse 2 (ROP), Control-flow integrity	**Contents** ROP, Control-flow graphs, control-flow integrity **Extra resources** M. Abadi, M. Budiu, Úlfar Erlingsson, and J. Ligatti: "Control-Flow Integrity: Principles, Implementations, and Applications" (2009)
Tue, Sep 16		**Contents** Control-flow integrity continued. Control-flow bending. **Extra resources** N. Carlini et al.: "Control-Flow Bending: On the Effectiveness of Control-Flow Integrity" (2015)
Thu, Sep 18	Other memory safety attacks. Isolation and secure design.	**Contents** Temporal safety and use after free. Secure application design using processes **Extra resources** Low-Level Software Security by Example - Úlfar Erlingsson, Yves Younan, and Frank Piessens (2010) A. Barth et al.: "The Security Architecture of the Chromium Browser" (2008) N. Provos, M. Friedl, P. Honeyman Preventing privilege escalation (2003)
Tue, Sep 23	Isolation in browsers	**Assignment 2 due.** **Contents** System calls subsets **Perusall reading 4 due Sept 30th** Adam Barth, Collin Jackson, Charles Reis, Google Chrome Team - The security architecture of the chromium browser (2009) **Extra resources** Maddie Stone (Project Zero): In-the-Wild Series: October 2020 0-day discovery (2021) T. Garfinkel: "Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools" (2003)

Thu, Sep 25	Software fault isolation (SFI) + Confused deputy attacks Part 1	**Contents** Classic SFI, RLBox **Assignment 3 available (Sandboxing)** **Extra resources** Chapters 1, 2, and 3 from G. Tan: "Principles and Implementation Techniques of Software-Based Fault Isolation" (2017)
Tue, Sep 30	Software fault isolation (SFI) + Confused deputy attacks Part 2	**Contents** RLBox continues, Wasm, Classic SFI vs. Wasm **Perusall reading 5 due Oct 7th** S. Narayan et al.: "Retrofitting Fine Grain Isolation in the Firefox Renderer" (2020)
Thu, Oct 2	Web introduction	**Contents** Overview, Browser Security Model, CSRF **Extra resources** J. Schwenk, M. Niemietz, and C. Mainka: "Same-Origin Policy: Evaluation in Modern Browsers" (2017) C. Reis, A. Moshchuk, and N. Oskov: "Site Isolation: Process Separation for Web Sites within the Browser" (2019)
Tue, Oct 7	Web intro cont., Web attacks	**Contents** CSRF, SQL Injection, XSS **Extra resources** php's SQL Injection OWASP XSS Cheat Sheet OWAP CSRF
Thu, Oct 9	Web attacks cont.	**Perusall reading 6 due Oct 16th** J. Schwenk, M. Niemietz, and C. Mainka: "Same-Origin Policy: Evaluation in Modern Browsers" (2017)
Tue, Oct 14	Web defenses	**Contents** CSP, Iframe sandbox, Clickjacking, CORS **Extra resources** Robust defenses for cross-site request forgery by Adam Barth Play safely in sandboxed IFrames by Mike West

		Content security policy by Joe Medley and Mike West Subresource integrity - W3C Working Draft **Assignment 3 due.**
Thu, Oct 16		**No class today.** Prepare for your midterm.
Tue, Oct 21		**Midterm exam at JGB 2.324 at 12:30pm to 2pm**
Thu, Oct 23	Network introduction	**Assignment 4 available (Web)** **Contents** Network Intro, Network Attacks: DNS and BGP **Extra resources** DNS root servers – Cloudflare S. Son and V. Shmatikov: "The Hitchhiker's Guide to DNS Cache Poisoning" (2010) Wikipedia: Autonomous System Wikipedia: OSPF routing Wikipedia: Border Gateway Protocol Wikipedia: User Datagram Protocol Wikipedia: Transmission Control Protocol Wikipedia: Domain Name System
Tue, Oct 28	Networks attacks	**Contents** IP, ARP Spoofing **Extra resources** Security problems in the TCP/IP protocol suite by Steven Bellovin. And a look back at this paper. Known instances of accidental/malicious BGP hijacking SAD DNS Explained by Marek Vavruša and Nick Sullivan NAT Slipstreaming by Samy Kamkar
Thu, Oct 30	Network defenses	**Contents** Firewalls, intrusion detection systems, honeypots

		Extra resources The Base Rate Fallacy and its implications for the difficulty of intrusion detection - Stefan Axelsson (1999) A DoS-Limiting Network Architecture - Yang, Wetherall, and Anderson (2005)
Tue, Nov 4	Network defenses cont.	
Thu, Nov 6	Basic side-channels	**Contents** Memory and timing side-channels **Assignment 4 due. Assignment 5 available (Side-channels)** **Extra resources** R. Branco and B. Lee: "Cache-Related Hardware Capabilities and Their Impact on Information Security (2022)
Tue, Nov 11	Microarchitecture Attacks	**Contents** Spectre attacks **Extra resources** D. Gruss: Introduction to Software-Based Microarchitectural Attacks (2017) J. Horn: "Reading Privileged Memory with a Side-Channel" (2018) L. Fiolhais and L. Sousa: "Transient-Execution Attacks: A Computer Architect Perspective" (2023)
Thu, Nov 13	Secure Channels	**Contents** TLS, Certs **Extra resources** A. Delignat-Lavaud and K. Bhargavan: "Network-based Origin Confusion Attacks against HTTPS Virtual Hosting" (2015)
Tue, Nov 18	(tentative plan which may be changed) Attacking browsers through JavaScript	**Contents** Introduction to JavaScript JavaScript interpreter internals
Thu, Nov 20		**Assignment 5 due. Assignment 6 available (TBD: Spectre or QuickJS)**

		Contents JavaScript interpreter exploitation **Extra resources** saelo: "The Art of Exploitation: Attacking JavaScript Engines" (2016/2021)
Tue, Nov 25		**No class today (Thanksgiving)**
Thu, Nov 27		**No class today (Thanksgiving)**
Tue, Dec 2	Recent developments; wrapping up	**Extra resources** P.A. Karger and R.R. Schell: "Multics Security Evaluation: Vulnerability Analysis" (1974)
Thu, Dec 4	Finals review	**Assignment 6 due.** **Contents** Finals review
Sat, Dec 13	**Final exam**	**Final exam 3:30 pm- 5:30 pm**