642: Introduction to Computer Security

This Google Doc will have the most up to date information about the course materials, topics, and schedule.
Canvas: COMPSCI642: Introduction to Information Security (001) SP23 (wisc.edu)
Piazza: https://piazza.com/class/ld4rre7xb0d27r
Homeworks/assignments: Canvas

Instructor: Prof. Rahul Chatterjee (he/him)
Mode: In-person. **Time**: Tue, Thu (9:30 am -10:45 am CT) **Location**: BARDEEN 140 (Google Map)

The team

TAs:

- Ben Jacobsen (he/him)
- Nick Ceccio (they/them)

Grader:

- Suhas Hebbar

Office hours:

- Rahul: Thursday 2-3 pm – CS 7373
- Ben: Tuesday 1:30-2:30 pm – CS 3205
- Nick: Friday 10-11 am – CS 3233

OH Zoom link:
https://uwmadison.zoom.us/j/99363539417?pwd=bXhYVG83NGs1WitTQ1VNcVBENm01QT09
(Zoom can only be used if you send a note via Piazza at least a day early.)

Class discussions: Piazza

Textbooks:

There is **no required textbook** for this course. Here are some reference textbooks that might help. We might use some portions from these textbooks, and the relevant PDFs will be attached in the course doc or on Canvas.

1. Introduction to Computer Security, Matt Bishop
2. Network Security: Private Communication in a Public World
3. Cryptography Engineering
4. Foundations of Security - What Every Programmer Needs to Know.pdf

Assignments and Midterms:

There will be **one** midterms and **no final**. Midterm will be in class. There will be **five** homework assignments, and **three in-class / take-home quizzes**. Each homework assignment is to be completed by a group of **two** students. You may perform up to 2 assignments with the same partner, but after that you must form a group with someone else. You must pick your groups before each assignment is released. Students who cannot find a group will be assigned to a group randomly **on the day assignment is released**. (It will be very difficult to reassign after you are assigned to a group. Please do not change groups after the assignment is released.)

The course will also have **a project** component on a security topic of your choice. You will have to write a **4 page report**, and give an **8-min presentation**. The project can be done in groups of 3-4 students (groups will be automatically assigned).

If you cannot take the exam on the below-mentioned dates, you have to take it earlier. Please let me know **at least 3 weeks in advance**. (Exceptions are possible, but only in exceptional circumstances.)

Late submission policy for homeworks:

- Everyone gets 2 late days without penalty, spread out over the semester. So, you can turn in one assignment 2 days late, or two assignments 1 day late.
- One-fourth of the obtained points will be deducted for every additional late day (rounded up).
- Homeworks submitted **after four late days will not be graded** (unless you notify me early with a proper justification).

Grades

Course grade will be determined based on these components

- Homework assignments: **40%** (5 assignments) [see below for Dates]
- Midterm: **25%** - midterm
- Quizzes: **15%** (3 quizzes) [see below for Dates]
    - 3 take-home/in-class quizzes (30-45 min each) distributed through Canvas.
- Project: **15% [2%** (proposal) **+ 6%** (presentation) **+ 7%** (report) **]**
    - Proposal
    - Presentation
    - Report
    - More details are posted on Canvas: Project details
- Class participation: **5%** *

* Class participation includes attending the lectures, interacting in the class, with instructor/TAs, and on Piazza on a regular basis. I am going to take attendance *on 5 random days*, and if you are present you get the pont.

The grade cutoffs are:

Letter grades will be assigned by rounding your final score to the next integer.

- A: 91-100
- AB: 84-90
- B: 77-83
- BC: 70-76
- C: 61-69
- D: 51-60
- F: 0-50

The grading would be absolute --- if you meet the cutoff you get the grade.
For graduate students each grade cutoff is increased by 2 points. That means if you are a graduate student you have to get at least 93 to get an A, and so on.

Academic misconduct

Academic misconduct is taken very seriously in this course. You are encouraged to collaborate with your peers by helping them understand topics, sharing study materials, and helping them set up computing environments for assignments. However, you are NOT allowed to share answers, solutions, or any specifics about them for any assignments and midterms.

You are also allowed to search on the Internet about security related topics we discuss in the class or of your interest. If you are using an online resource that helps you solve an assignment, please cite the resource. But you are NOT allowed to search for solutions about the assignments or midterm questions online or elsewhere. There are incorrect answers posted online, and if your answer matches with an (incorrect) solution on the Internet, you will be reported to the university for academic misconduct and might obtain an F in the whole course. Please refer to https://conduct.students.wisc.edu/academic-misconduct/ for more information.

Diversity and inclusion

Diversity is a source of strength, creativity, and innovation for UW-Madison. We value the contributions of each person and respect the profound ways their identity, culture, background, experience, status, abilities, and opinion enrich the university community and this class. We commit ourselves to the pursuit of excellence in teaching, research, outreach, and diversity as inextricably linked goals. The University of Wisconsin-Madison fulfills its public mission by creating a welcoming and inclusive community for people from every background – people who as students, faculty, and staff serve Wisconsin and the world.

If you need to miss any exam due to religious observance, please get in touch with me in advance and we will find an alternate date for the make-up exam.

Tentative day-by-day lesson plan

This is a **tentative lesson plan**/syllabus. The readings and the topics for each day might change as we proceed through the semester. Some reading materials are required, others are optional. As we progress through the course, [required] tags will be added to the readings that are required.

Homeworks will be **released at the beginning of the day (12:01 am CT)** on the day mentioned, and similarly they will be **due at the end of the day (11:59pm CT)** they are due.

Week	Date	Topics	Readings	HW/Exam?
1	Jan 24 (TUE)	**Introduction and Logistics** ● Security mindset ● Threat modeling CS642-Introduction.pptx	● Reflections on Trusting Trust ● Saltzer and Schroeder, The Protection of Information in Computer Systems ● Gray hat hacking: Ethical Hacker's Handbook	
1	Jan 26 (THU)	**Operating system security** ● UNIX and Multics security ● File system vulnerabilities ● Access control CS642-OSSec.pptx	● Multics Security Evaluation: Vulnerability Analysis ● TOCTTOU Vulnerabilities in UNIX-Style File Systems	
2	Jan 31 (TUE)	**Android security** ● Android permission model CS642-Android_Security.p…	● The Android Platform Security Model	

2	Feb 2 (THU)	**Low-level software security 1** ● X86 basics ● VM Setup CS642-SoftwareSecurity.p…	● A Crash Course in x86 Assembly for Reverse Engineers ● [required] Smashing the stack for fun and profit ● Low-level Software Security by Example	**HW 1 released** (Software exploits)
3	Feb 7 (TUE)	**Low-level software security 2** ● Buffer overflow ● Demo CS642-SoftwareSecurity.pptx	● Basic integer overflows ● Improving Integer Security for Systems with KINT ● Format string vulnerabilities	
3	Feb 9 (THU)	**Low-level software security 3** ● Heap overflow ● Integer overflow ● Format-string vulnerabilities ● Detecting vulnerabilities CS642-SoftwareSecurity.pptx	● Real-world fuzzing ● Syzkaller	
4	Feb 14 (TUE)	**Memory protection and attacks** ● Stack canary ● ASLR ● W^X ● Software Fault Isolations CS642-SoftwareSecurity.pptx	● Address Sanitizer ● The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86) ● StackGuard ● On the Effectiveness of Address-Space Randomization ● Adapting Software Fault Isolation to Contemporary CPU Architectures - David Sehr, Robert Muth, Cliff Biffle, Victor Khimenko	
4	Feb 16 (THU)	**Symmetric-key encryption** ● Symmetric encryption, ● Block ciphers, different block cipher modes of operations CS642-Cryptography.pptx	● [required] Cryptography Engineering -- Ch: 2.6, 4.1-4.3, 4.5 (Requires UW netid/password) ● Try to read before class (**6 pages in total**, must read after class!)	**Feb 15-16** **Quiz - 1 (take home)** - Software security - OS security - Android
5	Feb 21 (TUE)	● Hashing, MAC ● AEAD Encryption scheme CS642-Cryptography.pptx		
5	Feb 23 (THU)	**Asymmetric Key Crypto** - Brief background on number theory, Discrete log - RSA, Why Textbook RSA is not secure - Sharing keys - Diffie Hellman	● [reference] Number theory primer ● (Reference) Cryptography Engineering (Ch: 11-12) ● [required] Cryptography (Cryptography)Engineering -- Ch: 12.3-12.6 (Requires UW netid/password)	**HW1 due** / **HW2 released -** Cryptography

		- Source of randomness CS642-Cryptography.pptx	- Twenty Years of Attacks on the RSA Cryptosystem	
6	Feb 28 (TUE)	**User authentication** - Passwords and PINs - Entropy, Guessing attacks - Leaked passwords, HIBP - Biometrics CS642-UserAuthentication…	- The password thicket: technical and market failures in human authentication on the web - Biometrics: A Grand Challenge	
6	Mar 2 (THU)	**Web security 1** - Browser security - Same-origin policy, cookies, isolation CS642-WebSecurity.pptx Rahul OH from 1:30 pm - 3pm.	- [Interesting] Securing Frame Communication in Browsers, Barth et al. - Browser Security: Lessons from Google Chrome,	**Mar 2-5** **Quiz - 2 (take home)** - Cryptography - User auth - 45 min (Released at noon on Mar 2, take by 11:59pm on Mar 5)
7	Mar 7 (TUE)	**Web security 2** - SQL Injection - Cross-site scripting and request forgery - Clickjacking - Defenses CS642-WebSecurity.pptx	- Cross Site Scripting Explained - Robust Defenses for Cross-Site Request Forgery, Barth et al. - Clickjacking Vulnerability and Countermeasures - Advanced SQL Injection In SQL Server Applications	
7	Mar 09 (THU)	No Class. Rahul OH from 10-11 on Fri on Zoom.	No class - Rahul is traveling	**HW2 due /** **HW3 released** (Web security)
8	Mar 11 Mar 19	Spring Break - No Classes		
9	Mar 21 (TUE)	**[Special topics] Cryptocurrency** **IntroToBlockchains.pdf**	- DigiCash: Blind Signature for untraceable payment - A Peer-to-Peer Electronic Cash System - Ethereum White Paper	Guest lecture by Max Zinkus
9	Mar 23 (THU)	**Network security 1: TLS** - Trust in the Internet - How do certificate authorities work? - Certificate issuance and revocation CS642-NetworkSecurity-tl…	- [required] Networking 101: Transport Layer Security (TLS)	**HW3 return /** **HW4 released** (Network security)
10	Mar 28 (TUE)	**Network Security 2: DNS, Mac** - DNS, DNSsec - SYN flood	- [required] DNS cache poisoning, by Steve Friedl	

		● ~~Wireless security~~, ● Wireshark, Firewall, IDS CS642-NetworkSecurity-s…	● A survey of BGP security, Butler et al. ● Wireshark tool (for reference) ● Nmap tutorial ● Insertion, Evasion, and Denial of Service	
10	Mar 30 (THU)	**Censorship, Anonymity network, Tor** **CS642-Censorship_and_T…**	● Tor: The Second-Generation Onion Router, by Dingledine et al. ● Ignoring the Great Firewall of China, by Clayton et al.	**Quiz 3 (take home)** - Web auth - Cryptocurrency - TLS, N/w sec
11	Apr 4 (TUE)	**No agenda. Review content, Q&A**		
11	Apr 6 (THU)	**No lecture. Midterm exam [Format: Online on Canvas, released on Apr 6, 9am, take by April 7, 11:59pm]**	Include OS Security, Software Security, Cryptography, User authentication, and Web security, n/w security.	
12	Apr 11 (TUE)	**Hardware security** ● TEE, TPM, SGX, Bitlocker ● Flush+Reload, Prime+probe CS642-Hardware_Security…	● Intel Trusted Execution Technology ● Introduction to the TPM ● Attestation and Trusted Computing	**Return HW 4**
12	Apr 13 (THU)	**IoT Security** CS642-iot_security.pptx	● SoK: Security Evaluation of Home-Based IoT Deployments	**HW5 released -** IoT Security
13	Apr 18 (TUE)	**No class Agenda: Project check-in**	Project check in over Zoom **(9am - 12 noon)**	**Project proposal due.**
13	Apr 20 (THU)	**[Special topics] Machine Learning Security & Privacy** **642_Guest_Lecture.pptx (sharepoint.com)**	A Taxonomy and Terminology of Adversarial Machine Learning SoK: On the Impossible Security of Very Large Foundation Models	Guest lecture by Ben Jacobsen
14	Apr 25 (TUE)	**Special topics Human Aspects of security** ● Reimagine security as safety ● Case studies ● Principal of secure design CS642-FinalLecture.pptx	● Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q) ● Computer security impaired by legitimate users	
14	Apr 27 (THU)	**Special topics** -		**Project presentation due April 30.**
15	May 02 (TUE)	Project Q&A	18-20 groups (3 min each)	

15	May 04 (THU)	No class	Rahul is traveling	**HW5 due**

Final project report due: May 8, 2023.
Grades released: May 12, 2023

More readings (optional)

- Cryptography
- User authentication
  - https://www.cl.cam.ac.uk/~fms27/papers/2012-BonneauHerOorSta-password--oakland.pdf
  -
- Web security
  -
- Network security
  - DNS cache poisoning, by Steve Friedl
  - A survey of BGP security, Butler et al.
  - Address Resolution Protocol Spoofing and Man-in-the-Middle Attacks, by B. Wagner and J. Bryner
  - A look back at Security Problems in the TCP/IP Protocol Suite, by S. Bellovin
  - Tor: The Second-Generation Onion Router, by Dingledine et al.
  - Ignoring the Great Firewall of China, by Clayton et al.
- Software security
  - A Crash Course in x86 Assembly for Reverse Engineers
  - Smashing the stack for fun and profit
  - Low-level Software Security by Example
  - The Hacker's Strategy, Dave Aitel
  - Bypassing Browser Memory Protections
  - Basic integer overflows
  - Improving Integer Security for Systems with KINT
  - Format string vulnerabilities
  - Real-world fuzzing
  - Syzkaller
  - Address Sanitizer
  - The Geometry of Innocent Flesh on the Bone: Return-into-libc without Function Calls (on the x86)
    - Extended version: Return-Oriented Programming:Systems, Languages, and Applications
  - StackGuard
  - On the Effectiveness of Address-Space Randomization
  - Adapting Software Fault Isolation to Contemporary CPU Architectures
  - On the Effectiveness of Address-Space Randomization
  - Adapting Software Fault Isolation to Contemporary CPU Architectures
- OS security
  - Multics Security Evaluation: Vulnerability Analysis

    - TOCTTOU Vulnerabilities in UNIX-Style File Systems: An Anatomical Study
- Hardware security
    - Intel Trusted Execution Technology
    - Introduction to the TPM
    - Attestation and Trusted Computing
    - A Trusted Open Platform
    - Using Innovative Instructions to Create Trustworthy Software Solutions
    - Intel® Software Guard Extensions(Intel® SGX) slides
    - Intel SGX Explained very long...
    - Bitlocker
- Miscellaneous topics
    - **Sandboxing** & **Virtualization Security**
    - Virtualization, VM-escape, Cloud security
    - Traps and Pitfalls: Practical Problems in System Call Interposition Based Security Tools, T. Garfinkel
    - Efficient Software-Based Fault Isolation, Robert Wahbe, et al.
    - [interesting] A Note on the Confinement Problem, by Lampson
    - When Virtual is Harder than Real: Security Challenges in Virtual Machine Based Computing Environments , by Garfinkel and Rosenblum
    - Compatibility is Not Transparency: VMM Detection Myths and Realities, Garfinkel et al., HotOS 2007