

CS 458 / 658
Computer Security and Privacy

Module 1
Introduction to Computer Security and Privacy

Spring 2023

Module outline

- ① Administrativa
- ② Course Overview

Instructors

Diogo Barradas

- diogo.barradas@uwaterloo.ca
- <https://cs.uwaterloo.ca/~dbarrada/>
- Office hours: Tuesdays 10:00–11:00 am (or by appointment), DC 2631

Adithya Vadapalli

- adithya.vadapalli@uwaterloo.ca
- <https://avadapal.github.io/>
- Office hours: Wednesdays 10:00–11:00 am (or by appointment), DC 2131

Section 1: Tue,Thu 04:00–05:20pm in MC 2034

Section 2: Tue,Thu 01:00–02:20pm in MC 2017

Teaching Assistants

TAs:

- Adrian Cruzat La Rosa
- Shreya Arun Naik
- Ru Ji
- Hossam ElAtali
- Sara Sarfaraz
- Solomon Levi Davidson

(Office hours link on LEARN)

Where to find information

- **Campus and CS VPNs**: remote working
- **student.cs account**: code submission
 - **If you don't have a student.cs account for some reason, ask cscfhelp@uwaterloo.ca for help**
- **LEARN**: Bongo livestream classroom, recordings, tests, assignments, etc.
- **Piazza**: Q&A, general discussions
- **BigBlueButton (BBB)**: TA office hours, in case we host them online (no need to make an account!)
- **Course website**: syllabus, slides, public materials
- **infodist**: individual information (scores, comments) final assessment

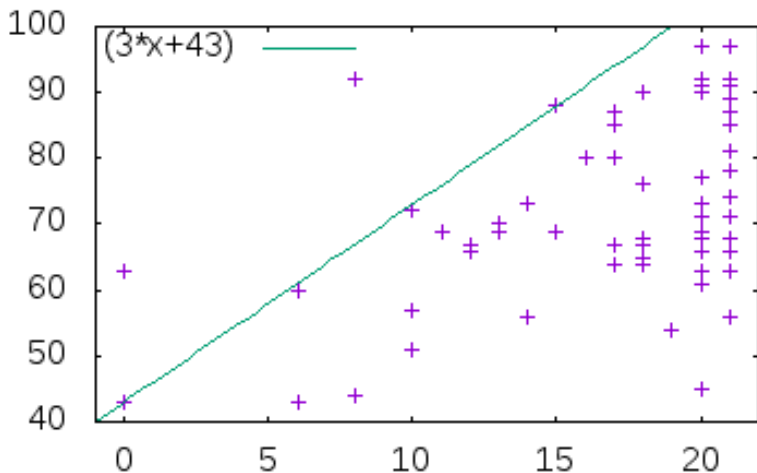
Teaching with COVID-19 Considerations

- Because we cannot predict what COVID will do and how the university will react, we are committing to making the course *mostly* available remotely the whole term.
- Lecture content will be both livestreamed and recorded.
- There will be an **in-person** final exam.

Teaching with COVID-19 Considerations

- If we're in a place where courses are offered remotely again, then that will be the only delivery mechanism; otherwise, we'll be livestreaming the course in Bongo from the classroom.
- If you are participating online, we encourage you to participate synchronously (joining the Bongo room live, as opposed to watching the recordings later).

Attend the (Online) Lectures!



Communication Channels

- Important course announcements will be made on Piazza.
 - Please keep up with the information there.
- Use discussion forums in Piazza for all communication
 - Use a private question for questions not of general interest
- Use email only as a last resort and then it must be from your uwaterloo.ca email address
- Some communication might be sent to your uWaterloo email address
 - Check your uWaterloo email account regularly or have email forwarded to your regular account

Per-student information

- Per-student information will be distributed using Infodist:

<https://crysp.uwaterloo.ca/courses/cs458/infodist/>

- Assignment marks and comments
- Blog task sign-up
- Login accounts for assignment machines

Course Syllabus

- You are expected to be familiar with the contents of the course syllabus
- Available on the course website and LEARN
- If you haven't read it, read it after this lecture

Grading Scheme

- Assignments ($3 \times 22\% = 66\%$)
 - contain written and programming portions
 - work alone
- Self-tests (5%)
- Blog task (7%)
- Final assessment (22%)
- Additional research survey paper for CS 658
 - See syllabus for more details
- See syllabus for late and reappraisal policies, academic integrity policy, and other details

Assignments

- Assignments will be due **at 3pm** Waterloo time.
- Late submissions will be accepted up to 48 hours after due date
 - No doctor's note or supporting documents required
 - No penalty will be given
 - Applicable to Assignments 1, 2, 3 only
- BUT
 - No assistance will be given after due date
 - No assignments will be accepted after the 48-hour grace period
 - Only assignments submitted with the official submission system will be accepted

Late Policy

- The purpose of the late policy is to deal with temporary problems occurring **before** the assignment due date
- If the problem occurs only during the 48 hours after the due date, you are out of luck
 - Submit early and submit often
- You must notify your instructor **well before the due date** of any severe, long-lasting problem preventing you from completing an assignment on time
- **No lates** are accepted for self-tests, blog task (sign-up, posts, or comments), and CS 658 proposal and survey paper

Plagiarism and Academic Offenses

- We take academic offenses very seriously
 - Even (especially?) in fourth year
- Nice explanation of plagiarism online
 - <https://uwaterloo.ca/math/academic-matters/academic-integrity>
- Read this and understand it
 - Ignorance is no excuse!
 - Questions should be brought to instructor
- Plagiarism applies to both text and code.
- You are free (even encouraged) to exchange ideas, but **no sharing of code or text.**

Plagiarism (2)

- Common mistakes
 - Excess collaboration with other students
 - Share ideas, but no design or code!
 - Using solutions from other sources
 - Asking public questions containing (partial) solutions
 - Posting (partial) solutions to websites (e.g., github)
- Possible penalties
 - First offense (for assignments; exams are harsher)
 - 0% for that assignment, -5% on final grade
 - Second offense
 - More severe penalties, including suspension
- Penalties for graduate students are more severe
- More information linked to from course syllabus

Self-tests

- The self-tests are worth 5% of your grade
- They're meant to help you keep up with the material, and gauge your grasp of it on an ongoing basis
- Check calendar in LEARN and course website for the release and deadline for each self-test
 - First test: available tomorrow, deadline one week.
 - **Late self-tests cannot be made up for any reason, including students signing up for the class late**
 - You can (re)do each self-test multiple times before its deadline; your last grade is the one recorded.
- Format: online (on LEARN), usually multiple-choice questions

Blog Task

- Many of the security and privacy problems that we will discuss in this course will (unfortunately) occur in the real world during the next four months.
- The blog task encourages you to keep up with these developments.
- Each student has to write one blog post during an assigned timeslot (a week).
- You must also participate in the discussion of other students' blog posts **throughout the term**.
- See LEARN for sign-up and other instructions.

Final Assessment

- Covers the entire syllabus
- Must pass ($\geq 50\%$) to pass course
- **In-person during exam season** - Time and place TBD
- You will have 2.5 hours to complete the assessment

A Note on Security

- In this course, you will be exposed to information about security problems and vulnerabilities with computing systems and networks.
- To be clear, **you are not to use this or any other similar information to test the security of, break into, compromise, or otherwise attack, any system or network** without the express consent of the owner
- In particular, you will comply with all applicable laws and University policies.
- See syllabus for more details.

CPI Award

- The [Cybersecurity and Privacy Institute](#) (CPI) Undergraduate Award is one award, valued at \$1 000, to be provided to a full-time student enrolled in CS458.
- You must be a full-time undergraduate student enrolled in CS458 for the S23 term.
- Awarded to a (the?) top student:
 - minimum 90% overall;
 - minimum 80% in each individual course component;
 - **and** the most useful comments on Piazza throughout the term.
- Graduate students will *not* be considered as contenders.

Recommended Textbooks

- **Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin (2nd Edition)**, Paul van Oorschot, Springer, 2021.
- **Security in Computing**, 5th edition, Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies, Prentice-Hall, 2015.
- Digital copies are available via the library website (linked from LEARN)
- You are expected to know all the material presented in class, even if it's not in the textbooks.

Other readings

- From time to time, there will be additional assigned readings
- Links will be provided from the modules page in LEARN in sync with the course website
- There will be both mandatory and optional readings
- You must read the mandatory ones **before** the class in which we will discuss them.
 - There is such a reading for the next lecture

Course Modules

- ① Introduction to Security and Privacy
- ② Program Security
- ③ Operating System Security
- ④ Network Security
- ⑤ Internet Application Security and Privacy
- ⑥ Data Security and Privacy
- ⑦ Non-Technical Aspects of Security and Privacy

Module outline

① Administrativa

- Course personnel
- Course mechanics
- Syllabus
- Readings

② Course Overview

- What is our goal in this course?
- What is security?
- What is privacy?
- Who are the adversaries?
- Assets, vulnerabilities, threats, attacks, and defences
- Methods of defence

What is our goal in this course?

- Our primary goal is to be able to **identify security and privacy issues** in various aspects of computing, including:
 - Programs
 - Operating systems
 - Networks
 - Internet applications
 - Databases
- Secondly, to be able to use this ability to **design systems that are more protective of security and privacy.**

What is security?

- In the context of computers, **security** generally means three things:
 - **Confidentiality**
 - Access to systems or data is limited to authorized parties
 - **Integrity**
 - When you receive data, you get the “right” data
 - **Availability**
 - The system or data is there when you want it
- A computing system is said to be secure if it has all three properties
 - Well, usually

Security and reliability

- Security has a lot to do with “reliability”
- A secure system is one you can rely on to (for example):
 - ① Keep your personal data confidential
 - ② Allow only authorized access or modifications to resources
 - ③ Ensure that any produced results are correct
 - ④ Give you correct and meaningful results **whenever you want them**

What is privacy?

- There are many definitions of privacy
- A useful one: “**informational self-determination**”
 - This means that **you** get to **control** information **about you**
 - “**Control**” means many things:
 - Who gets to see it
 - Who gets to use it
 - What they can use it for
 - Who they can give it to
 - etc.

Example: PIPEDA

- PIPEDA (Personal Information Protection and Electronic Documents Act) is Canada's private-sector privacy legislation
- Lists ten Fair Information Principles companies need to abide by:
 - ① Identify the purpose of data collection
 - ② Obtain consent
 - ③ Limit collection
 - ④ Limit use, disclosure and retention
 - ⑤ Use appropriate safeguards
 - ⑥ Give individuals access
 - ⑦ Be accurate
 - ⑧ Be open
 - ⑨ Be accountable
 - ⑩ Provide recourse

(Read more: https://www.priv.gc.ca/leg_c/p_principle_e.asp)

Consumer Privacy Protection Act

- Forthcoming legislation to regulate private sector use of personal information.
- Modernizing protection: meaningful consent, right to erasure, etc.
- Stronger provisions for enforcement.
- Private right of action.

Security vs. privacy

- Sometimes people place security and privacy as if they're opposing forces.
- Are they really? Do we have to give up one to get the other?

Who are the adversaries?

- Who's trying to mess with us?
- Various groups:
 - Murphy
 - Amateurs
 - "Script kiddies"
 - Crackers
 - Organised crime
 - Government "cyberwarriors"
 - Terrorists
- Which of these is the most serious threat today?

Some terminology

- **Assets**
 - Things we might want to protect, such as:
 - Hardware
 - Software
 - Data
- **Vulnerabilities**
 - Weaknesses in a system that may be able to be **exploited** in order to cause loss or harm
 - e.g., a file server that doesn't authenticate its users

Some terminology

- **Threats**
 - A loss or harm that might befall a system
 - e.g., users' personal files may be revealed to the public
 - There are four major categories of threats:
 - ① Interception
 - ② Interruption
 - ③ Modification
 - ④ Fabrication
 - When designing a system, we need to state the **threat model**
 - Set of threats we are undertaking to defend against
 - **Whom** do we want to prevent from doing **what**?

Some terminology

- **Attack**
 - An action which **exploits** a **vulnerability** to **execute** a **threat**
 - e.g., telling the file server you are a different user in an attempt to read or modify their files
- **Control/Defence**
 - Removing or reducing a vulnerability
 - You **control** a **vulnerability** to prevent an **attack** and defend against a **threat**.
 - How would you control the file server vulnerability?
 - Our goal: control vulnerabilities

Methods of defence

- How can we defend against a threat?
 - **Prevent it:** prevent the attack
 - **Deter it:** make the attack harder or more expensive
 - **Deflect it:** make yourself less attractive to attacker
 - **Detect it:** notice that attack is occurring (or has occurred)
 - **Recover from it:** mitigate the effects of the attack
- Often, we'll want to do many things to defend against the same threat
 - **"Defence in depth"**

Example of defence

- Threat: your car may get stolen
- How to defend?
 - Prevent: Immobilizer? Is it possible to absolutely prevent?
 - Deter: Store your car in a secure parking facility, use "The Club"
 - Deflect: Have sticker mentioning car alarm, keep valuables out of sight
 - Detect: Car alarms, OnStar
 - Recover: Insurance

How secure should we make it?

- Principle of Easiest Penetration
 - “A system is only as strong as its weakest link”
 - The attacker will go after whatever part of the system is easiest for them, not most convenient for you.
 - In order to build secure systems, we need to **learn how to think like an attacker!**
 - How would you get private information from the US Social Security Administration database?
- Principle of Adequate Protection
 - “Security is economics”
 - Don't spend \$100,000 to protect a system that can only cause \$1,000 in damage

Weakest link



Defence of computer systems

- Remember we may want to protect any of our **assets**
 - Hardware, software, data
- Many ways to do this
 - Cryptography
 - Software Controls
 - Hardware Controls
 - Physical Controls
 - Policies and Procedures

Defence of computer systems

- Cryptography
 - Protecting data by making it unreadable to an attacker
 - Authenticating users with digital signatures
 - Authenticating transactions with cryptographic protocols
 - Ensuring the integrity of stored data
 - Aid customers' privacy by having their personal information automatically become unreadable after a certain length of time

Defence of computer systems

- Software controls
 - Passwords and other forms of access control
 - Operating systems separate users' actions from each other
 - Virus scanners watch for some kinds of malware
 - Development controls enforce quality measures on the original source code
 - Personal firewalls that run on your desktop

Defence of computer systems

- Hardware controls
 - Not usually protection of the hardware itself, but rather using separate hardware to protect the system as a whole
 - Fingerprint readers
 - Smart tokens
 - Firewalls, intrusion detection systems
 - Trusted Execution Environments (TEEs)

Defence of computer systems

- Physical controls
 - Protection of the hardware itself, as well as physical access to the console, storage media, etc.
 - Locks
 - Guards
 - Off-site backups
 - Don't put your data centre on a fault line in California
 - Don't put your nuclear power plant in a tsunami zone

Defence of computer systems

- Policies and procedures
 - Non-technical means can be used to protect against some classes of attack
 - If an employee connects their own Wi-Fi access point to the internal company network, that can accidentally open the network to outside attack
 - So don't allow the employee to do that!
 - Rules about choosing passwords
 - Training in best security practices

Recap

- What is our goal in this course?
 - Identify security and privacy issues
 - Design systems that are more protective of security and privacy
- What is security?
 - Confidentiality, Integrity, Availability
- What is privacy?
 - Informational self-determination

Recap

- Who are the adversaries?
 - Learn to think like an attacker
- Assets, vulnerabilities, threats, attacks and controls
 - You **control** a **vulnerability** to prevent an **attack** and block a **threat**
- Methods of defence
 - Cryptography, software controls, hardware controls, physical controls, policies and procedures