

CS 458 / 658

Computer Security and Privacy

Module 1
Introduction to Computer Security and Privacy

Winter 2014

Instructors

Ian Goldberg

- `iang@cs.uwaterloo.ca`
- `https://cs.uwaterloo.ca/~iang/`
- Office hours: M 3:00–4:00 pm in DC 3518 (or by appointment)

Urs Hengartner

- `urs.hengartner@cs.uwaterloo.ca`
- `https://cs.uwaterloo.ca/~uhengart/`
- Office hours: Th 10:00–11:00 am in DC 3526 (or by appointment)

Course website

- This course will use LEARN
 - Syllabus, calendar, lecture notes, additional materials, assignments, announcements, policies, etc.
 - Site will be updated regularly
 - It is your responsibility to ensure that you are authorized to access the site and to keep up with the information on that site.
- Feedback is encouraged!

Piazza

- Discussion related to the course will take place on Piazza (piazza.com)
 - General course questions, announcements
 - Assignment-related questions
 - Like LEARN, you are expected to keep up with the information on Piazza

Additional communication

- Some communication might be sent to your uWaterloo email address
 - Check your uWaterloo email account regularly or have email forwarded to your regular account
- Use discussion forums in Piazza for questions of general interest
- Always send course-related email from your uWaterloo email account

Course syllabus

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

Plagiarism and academic offenses

- We take academic offenses very seriously
 - Even (especially?) in fourth year
- Nice explanation of plagiarism online
 - <https://uwaterloo.ca/arts/current-undergraduates/student-support/ethical-behavior>
- 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 code or text**

Plagiarism (2)

- Common mistakes
 - Excess collaboration with other students
 - Share ideas, but no design or code!
 - Using solutions from other sources (like for previous offerings of this course, maybe written by yourself)
- 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

Grading scheme for CS 458

- Midterm (15%)
 - Tue, Feb 11, 2014, 7:00 – 8:20 pm in MC 4020,4021,4040
 - There is no alternate midterm.
- Final (30%)
 - You must pass the weighted exam mark in order to pass the course!
- Assignments ($3 \times 15\% = 45\%$)
 - Work alone
- Self-tests (5%)
- Blog task (5%)
- 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 3:00 PM**
- Late submissions will be accepted up to 48 hours after due date
- There will be no penalty for accepted late submissions
- Multiple assignments can be submitted late, including the last one
- **No assistance will be given after the due date**
- You must notify your instructor **before the due date** of any severe, long-lasting problems that prevent you from completing an assignment on time

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 for the availability and deadline information for each self-test
 - First test: available tomorrow, deadline one week
 - **No late self-tests will be accepted!**
 - You can attempt each self-test as often as you like during its availability period; your last grade on each self-test will be the one recorded
- Format: online (on LEARN), usually multiple-choice questions

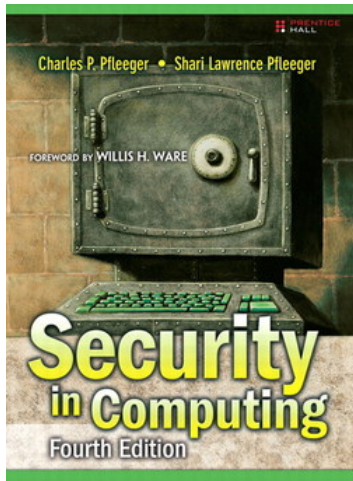
Blog task

- 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 forces you to keep up with these developments
- Each student has to write one blog post during an assigned timeslot
- You must also participate in the discussion of other students' blog posts **throughout the term**
- **Blog task is part of material covered in exams**
- See LEARN for sign-up and other instructions

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 uWaterloo policies
- See syllabus for more details

Required textbook



- **Security in Computing**, 4th edition, Charles P. Pfleeger and Shari Lawrence Pfleeger, Prentice-Hall, 2007.
- You are expected to know
 - entire textbook sections, as listed on course website
 - all the material presented in class

<http://proquest.safaribooksonline.com/9780132390774>

Other readings

- From time to time, there will be additional assigned readings
- They will be linked to from the modules page in LEARN
- 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 mechanics

- Teaching assistants: Sarah Harvey, Danish Mehmood, Sukhbir Singh, Yihang (Frank) Song, Vladimir Soukharev, Nikolas Unger, Jalaj Upadhyay
- **Come to class!** Not every bit of material will be on the slides or in the text
- You will need an account in the student.cs environment
 - **If you don't have a student.cs account for some reason, get one set up in MC 3017**

Module outline

- ① What is our goal in this course?
- ② What is security?
- ③ What is privacy?
- ④ Who are the adversaries?
- ⑤ Assets, vulnerabilities, threats, attacks, and controls
- ⑥ 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** (Should not be able to mod data)
 - When you ask for data, you get the “right” data
 - **Availability** DOS attacks
 - 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 C
 - ② Allow only authorized access or modifications to resources C,I
 - ③ Give you correct and meaningful results I
 - ④ Give you correct and meaningful results **when you want them** I,A

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 Be accountable
 - ② Identify the purpose of data collection
 - ③ Obtain consent
 - ④ Limit collection
 - ⑤ Limit use, disclosure and retention
 - ⑥ Be accurate
 - ⑦ Use appropriate safeguards
 - ⑧ Be open
 - ⑨ Give individuals access
 - ⑩ Provide recourse

Security vs. privacy

12:15PM 饿饿饿饿饿

- 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?

Bank account deny of random people...
Health record
Airport scanner

Who are the adversaries?

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

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 him, 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 (Cost for you)

Weakest link



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**

- Removing or reducing a vulnerability
- You **control** a **vulnerability** to prevent an **attack** and block 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
 - Deflect: Use “The Club”, have sticker mentioning car alarm, keep valuables out of sight
 - Detect: Car alarms, OnStar
 - Recover: Insurance

Defence of computer systems

- Remember we may want to protect any of our **assets**
 - Hardware, software, data
- Many ways to do this; for example:
- 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

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 his 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 changing 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