CS3235 - Tutorial 1

Spring 2022

About your TA: Kareem Shehata

- Former Google SWE
- Canadian, lived in Brazil
- Just arrived in SG to start PhD
- Graduated EE at UWaterloo, Comp Eng Option
- Done everything from board design to ERP
- AMA during "open question" time!

Quiz 1 - **This Week!**

- Test of course prerequisites
- Should take << 1 hour to complete
- Must score at least 6/10 for success in this course
- Does not count towards grade
- **Please complete by Sunday night**

Course Overview

First Half: 11 Jan to 8 Mar 2022

- Network Attacks
- Cryptography / Secure Channels
- ~ Weekly Homework Assignments
- No class on 1 Feb or 22 Feb
- **Midterm: 8 Mar 2022 (in class)**

Second Half: 15 Mar to 12 Apr 2022

- Web Security
- Software Security
- Isolation and Sandboxing
- 2 Assignments / Projects
- **No Final Exam**

Grading Scheme

Cryptography Assignments	33%
Midterm (Compulsory)	34%
Web Security Assignment	33%
Software Security Assignment	33%

We will take the best 2 scores of the assignments.

Tutorials

- Tutorials are for **you!**
- Cover more practical / hands on material than the lectures
- Sometimes prepared material, sometimes a demo, sometimes just Q&A
- Please feel free to ask questions, especially about assignments
- Goal is to prepare and help you with the assignments

Academic Integrity

What are acceptable ways to get help / collaborate on assignments?

Academic Integrity

Acceptable:

- Asking questions on forum
- Asking questions in tutorials
- Looking up background materials on the web or textbooks
- Collaborating with colleagues to better understand the material before writing your own answers

Not Acceptable:

- Asking previous year students for solutions
- Copying and pasting code from the web as your solution
- Collaborating with colleagues to write a single solution that you each submit as your own answers

If in doubt, ask the TAs or Instructor what is acceptable!

How to Succeed in CS3235

- Do the homework
  - … and make sure you understand it!
- Come to tutorials
  - … and ask questions!
- Start early
  - … there is often setup that doesn't use lecture content.
- Play to your strengths
  - … don't try to do it all, be strategic!
- Be Prepared!

An Example for Discussion

Bank Security

You're in charge of security at a bank, and you've been tasked with ensuring that the safety deposit boxes are "secure".

What do you do?
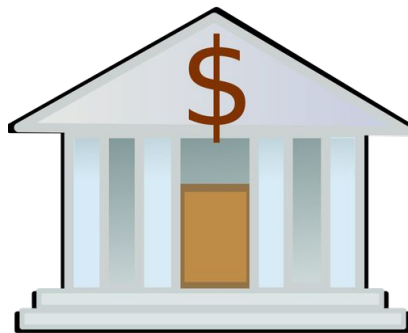
Bank Safety Deposit Boxes Threat Model

Can the attacker…

- Break a glass window?
- Cut through a wall?
- Incapacitate a security guard?
- Tunnel under the building?
- Impersonate another person?
- Forge government documents?
- Copy a user's key?

You can only determine security after you've defined a threat model