01. Course Introduction

Blase Ur and David Cash
January 10th, 2022
CMSC 23200 / 33250

THE UNIVERSITY OF CHICAGO

Part 1: Course Logistics

Instructors

Blase Ur

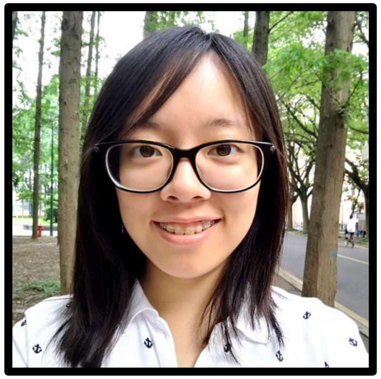
David Cash

Five TAs

Ally Nisenoff

Arthur Borém

Emma Peterson



Weijia He

Will Brackenbury

Website / Syllabus

https://www.classes.cs.uchicago.edu/archive/2022/winter/23200-1/

or shorturl.at/myLR9

Lectures

- Monday/Wednesday/Friday
  - 2:30pm - 3:20pm (Section 1)
  - 3:30pm - 4:20pm (Section 2)
- First two weeks: Zoom
  - Will be recorded
- Subsequently (we really hope): Ryerson 251
  - Will generally **not** be recorded

Textbook

- Paul van Oorschot, Computer Security and the Internet: Tools and Jewels
  - Free PDFs linked from the course website

Course Requirements (23200)

- 9 Reading Responses (9%)
  - Generally due Tuesdays 11:59pm
  - First one due **this Wednesday (1/12)**
- 9 Assignments (91%)
  - Generally due Thursdays 11:59pm
  - First one due next Thursday (1/20)

Course Requirements (33250)

- 8 Reactions to Research Papers (4.5%)
  - Generally due Mondays 11:59pm
- 9 Reading Responses (4.5%)
  - Generally due Tuesdays 11:59pm
- 9 Assignments (66%)
  - Generally due Thursdays 11:59pm
- Research project (25%)

Communication

- **Canvas** for assignment distribution
- **Campuswire** for questions
  - Questions about assignments, course material
  - Extension requests (include post # in submission)
  - Questions about logistics
- **Canvas / Gradescope** for submissions
- **Don’t email us!** Use Campuswire!
  - Not on Campuswire? blase@uchicago.edu

Communication on Campuswire

- See course website for guidelines about asking questions on Campuswire
- Private posts (visible to instructors) for:
  - Logistics, extensions, wellness, etc.
  - Questions about assignments that include code or specific insights about your solution
- Public posts for general ?s / clarifications
- Feel encouraged to answer questions

Key Course Policies (1/2)

- Late submissions
  - Assignments and reading responses can be submitted 24 hours late for a 15 point penalty
  - 33250-only work not accepted late
- Wellness
  - These years have been particularly hard for many of us, including the course staff!
  - Reach out to the course staff in a private (instructor-only) post on Campuswire

Key Course Policies (2/2)

- P/F grading
  - C- or higher = Pass
  - Request on Campuswire
  - Probably won’t count for your major
- Remote interactions during Zoom lectures
  - Video is optional
  - Feel encouraged to add pronouns to name
  - Questions or answers? Raise hand or type (to all or whichever of David/Blase isn’t teaching)

Academic Integrity Policy (1/2)

- Detailed on syllabus
- All work submitted must be your own
- May speak in general terms about approach
- You’re encouraged to talk to classmates
- At the top of each assignment, you **must document everyone in the class you spoke to, as well as every major resource you consulted** other than what we provide

Academic Integrity Policy (2/2)

- Example for the top of your submission:
  - "I discussed the whole assignment with Jane Smith. We also discussed Part 3 with John Doe. I consulted *https://www.helpfuldomain.com/helpfulpage.html* to understand the fetch() API and I used two lines of code from *https://www.other.com/page.html* in Part 3."
- Code reuse only allowed if **all** of the following:
  - Around 4 lines of code or fewer
  - Doesn't solve a whole sub-part of the assignment
  - Documented at top (see above) or as comment

Office Hours

- All office hours will be held on Zoom
- "TA" / "instructor" assignment office hours
  - Primary venue for help with assignments
  - Each assignment will have two TAs assigned
- Blase and David's office hours
  - Talk about lectures / concepts in general
  - Maybe get help with assignments
  - Get to know us!

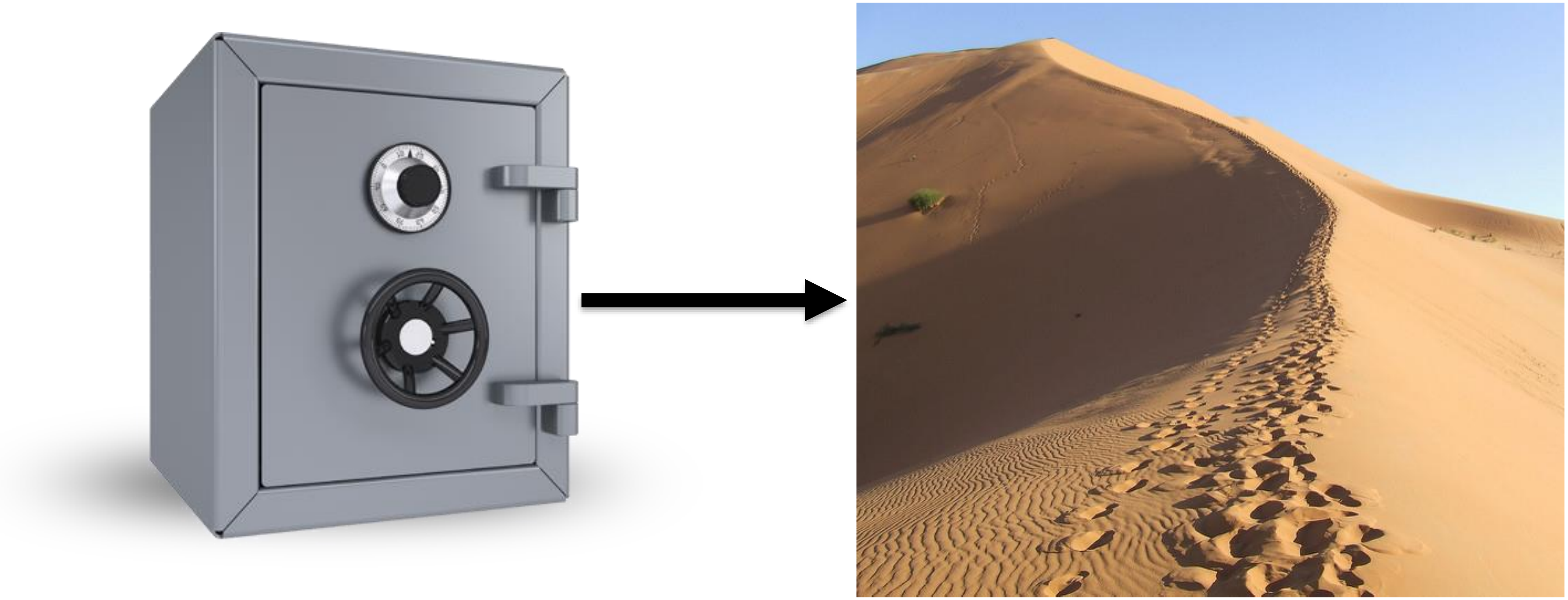
Are you not signed up yet?

- Currently 130 students enrolled
  - An additional 28 students on waiting list
- Want to switch from 23200 to 33250 or switch from Section 1 to Section 2?
  - Email Jess Garza to ask; cc Blase & David
- Are you not registered at all?
  - If you have a very urgent need to take the class this quarter, email us and explain
  - Otherwise, try again next year

Part 2: The Security Mindset

How can we keep something secure?

How can we keep something secure?



What properties do we want?

- **Confidentiality**: Information kept private
- **Integrity**: Information not secretly modified
- **Authorization:** Information accessible only by authorized entities

What properties do we want?

- **Confidentiality**: Information kept private
- **Integrity**: Information not secretly modified
- **Authorization:** Information accessible only by authorized entities
- **Authentication:** Principal/data is genuine
- **Accountability:** Responsible for past actions
- **Availability**: Information readily accessible

Course Learning Objectives

- The security mindset

Course Learning Objectives

- The security mindset
- Core security principles/properties

Course Learning Objectives

- The security mindset
- Core security principles/properties
- Computer security attacks

Course Learning Objectives

- The security mindset
- Core security principles/properties
- Computer security attacks
- Computer security defenses

Course Learning Objectives

- The security mindset
- Core security principles/properties
- Computer security attacks
- Computer security defenses
- The magic of houseplants
  - Plant Talk!
  - This Wednesday @ 4:30pm

Schedule of Topics By Week

1. Threat modeling and OS security
2. Memory vulnerabilities and protection
3. Software security and cryptography
4. Authentication
5. Network and web basics
6. Web security
7. Web privacy and network security
8. Statistical data privacy and current topics
9. Current topics

Tentative Assignments

1. Threat modeling and command line basics
2. Buffer overflows and memory attacks
3. Attacking crypto implementations
4. Password cracking, fuzzing auth systems
5. Analysis of network traffic
6. Web attacks, measuring X.509 cert usage
7. Web tracking, network defenses
8. Differential privacy / database encryption
9. Take-home final exam (written)