01. Course Introduction

Blase Ur and David Cash
January 4th, 2023
CMSC 23200 / 33250

THE UNIVERSITY OF
CHICAGO

Part 1: Course Logistics

Two Instructors

Blase Ur

David Cash

Seven TAs

Alex Hoover

Arthur Borém

Emma Peterson

Madison Pickering

Maggie Zhao

Maia Boyd

Zach Rothstein

Website / Syllabus

https://www.classes.cs.uchicago.edu/archive/2023/winter/23200-1/

Lectures

- Monday/Wednesday/Friday
  - 11:30am - 12:20pm (Section 1)
  - 1:30pm - 2:20pm (Section 2)
- Stuart Hall 105
  - Will **not** be recorded
  - Will generally **not** be livestreamed unless a student is ill and has requested a livestream

Textbook

- Paul van Oorschot, Computer Security and the Internet: Tools and Jewels (2nd Edition)
  - Free PDFs linked from the course website

Course Requirements (23200)

- 8 Reading Responses (8%)
  - Generally due Tuesdays 11:59pm
- 8 Assignments (60%)
  - Generally due Thursdays 11:59pm
  - First one due next Thursday (1/12)
- Midterm Exam (14%)
- Final Exam (18%)

Course Requirements (33250)

- 8 Reactions to Research Papers (4%)
  - Generally due Mondays 11:59pm
- Research project (22%)
- 8 Reading Responses (4%)
- 8 Assignments (48%)
- Midterm Exam (10%)
- Final Exam (12%)

Key Course Policies (1/2)

- Late submissions
  - Assignments and reading responses can be submitted 24 hours late for a 15 point penalty
  - 33250-specific 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

Communication

- **Canvas** for assignment distribution
- **Campuswire** for questions
  - ?s about assignments, course material, logistics
  - Extension requests (include post # in submission)
- Submit: **Canvas (code) / Gradescope (prose)**
- **Don't email us!** Use Campuswire!
  - We will add you in the next 24 hours
  - Not added? 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

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!

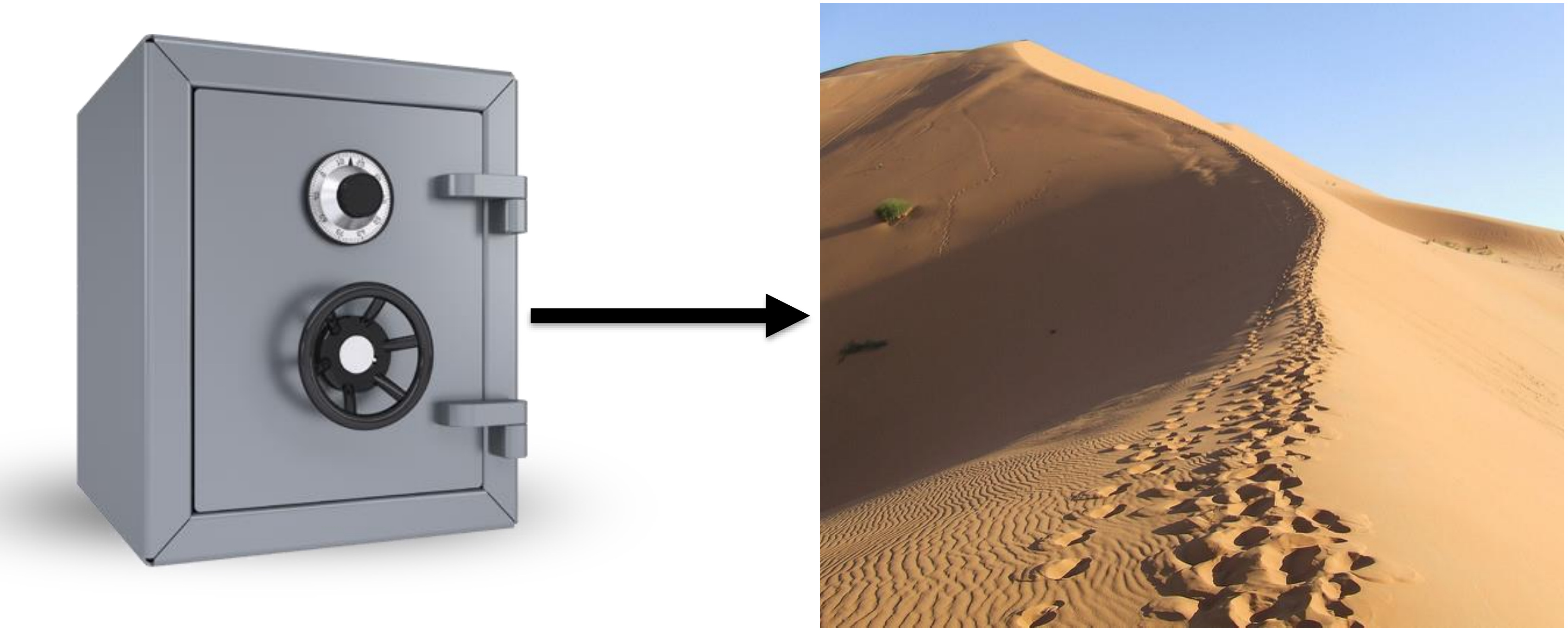
Are you not signed up yet?

- Currently 128 students registered
  - An additional 19 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!

Schedule of Topics By Week

1. Threat modeling
2. OS, memory vulnerabilities /protection
3. Authentication
4. Cryptography
5. Software security, network basics
6. Midterm, network attacks, web basics
7. Web security and privacy
8. Statistical data privacy, blockchain
9. Hardware/ML security, practical encryption

Tentative Assignments

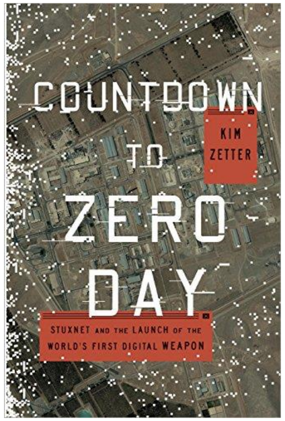
1. Threat modeling and TOCTOU attacks
2. Buffer overflows and memory attacks
3. Password cracking, auth systems
4. Attacking crypto implementations
5. Fuzzing, measuring X.509 cert usage
6. Side-channel analysis of network traffic
7. Web attacks, web tracking
8. Differential privacy implementation attack

Part 2: Some Famous/Instructive Security Incidents

The Morris Worm (1988)

- 99-line C program that exploited vulnerabilities in `sendmail` and `fingerd`, weak passwords, and other unsafe default settings
- Spread automatically over networks (the definition of a worm), reinfecting same machines many times (accidentally)
- 1000s of infected machines were knocked offline
  - Real costs to victims
- Morris convicted under the Computer Fraud Act
  - Sentenced to 3 years probation, 400 hours community service, plus fines.
- Led to a sea-change in computer security

Stuxnet (2005? Found 2010)



- Highly advanced attack created by US and Israeli governments to sabotage Iranian nuclear program.
- Included four zero days, each worth $$$ on gray market.
- Also used authenticate certificates (apparently) generated using keys stolen from two Certification Authorities (CAs).
- Attack targeted “air gapped” uranium enrichment systems, specifically to damage centrifuges. Malware would run centrifuges at rates that would cause them to fail often, but not too often; Behavior totally hidden from operators. (How did it jump the air gap?)
- Other advanced government threats subsequently discovered.

Dual EC and Juniper (2006? Discovered 2015)

Edward Snowden

- In 2013, Snowden documents strongly suggest that NSA tricked NIST into inserting a backdoor into a crypto standard called “Dual_EC” in 2006.
- In 2015, Juniper Networks announces that it found “unauthorized code" in ScreenOS, which is used widely on large routers. The patch suspiciously only changed a small portion of their binaries.
- Security researchers found Juniper had used Dual_EC, but tried to mitigate the possible backdoor in Dual_EC by changing some constants. The “unauthorized code” changed them back to the NSA-back-doored values. The patch changed them again.

Dual EC and Juniper (2006? Discovered 2015)

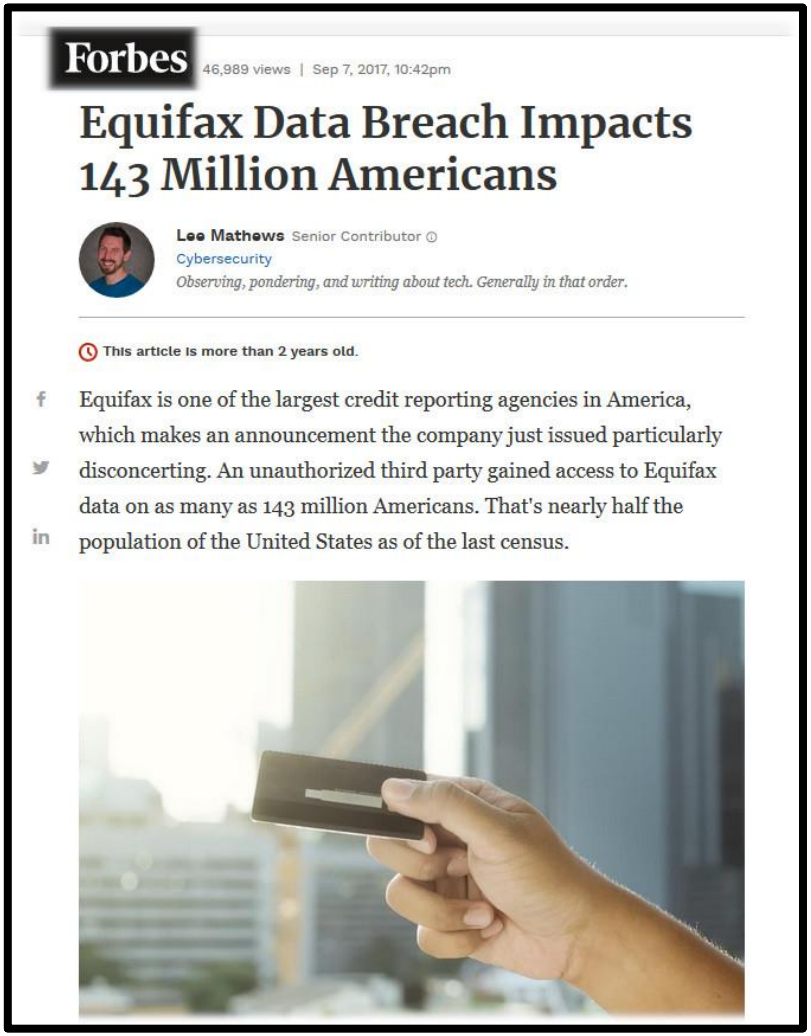
Edward Snowden

- Subsequently, a second(!) backdoor was found, unrelated to the first. This actor just created a hard-coded backdoor password. 😂
- Incident informs arguments over government backdoors today.
- Compare/contrast: Robert T. Morris vs NSA… 🤔

Target (2013)

- Millions of credit card and debit card numbers used at Target were stolen.
- Target’s technical infrastructure (including POS details) were posted as a Microsoft case study; it’s unclear if this was used by the attackers.
- Fazio Mechanical, an HVAC contractor, was compromised via a phishing email that installed the Citadel trojan.
  - Could have been detected by a modern antivirus.
- From the Target vendor portal, the attackers moved laterally to other systems.
- RAM-scraping malware was installed on POS terminals.

Equifax (2017)



Forbes

46,989 views | Sep 7, 2017, 10:42pm

Equifax Data Breach Impacts 143 Million Americans

Lee Mathews Senior Contributor

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

This article is more than 2 years old.

Equifax is one of the largest credit reporting agencies in America, which makes an announcement the company just issued particularly disconcerting. An unauthorized third party gained access to Equifax data on as many as 143 million Americans. That's nearly half the population of the United States as of the last census.

Equifax (2017)

- Apache Struts web-application framework had a vulnerability; a patch was released in March.
- Equifax engineers scanned their systems for vulnerable versions of Apache Struts and did not find any.
  - They forgot to use the recursive flag. *RIP.*
- Mid-May, attackers gained access via Struts and then moved laterally (enabled by poor access controls).
- Equifax took six weeks to announce the breach.
- Equifax's free credit reporting also suspect / vulnerable.
- Further issue: Equifax's Argentinian affiliate had a credit dispute website that used "admin/admin" credentials.
- Further issue: Are Social Security Numbers secure?

SolarWinds (2020)

- Widely used network-management software SolarWinds used by many major corporations and governments.
- By October 2019, attackers compromised the software build system used by SolarWinds.
- Malicious code was inserted into otherwise legitimate software updates for Orion.
- Malware stayed dormant for weeks, only operated on potentially high-value targets, and tried to mimic legitimate traffic.
- Command-and-control infrastructure was hosted on Amazon and Microsoft cloud systems.
- VMware exploit also seems to have been used.
- Data exfiltrated from governments and corporations.

Log4Shell (2021-2022)

- A zero-day vulnerability in the Log4j logging framework for JavaScript caused all sorts of problems last year.
- Affected 93% of cloud environments
- When logging, can request external resources via Lightweight Directory Access Protocol (LDAP)
- Attackers are able to execute arbitrary Java code on other people's servers by inserting a string that is logged in the log files (and then fetched and potentially run).
  - HTTP requests are often logged.