01. Course Introduction

Blase Ur and David Cash
January 11th, 2021
CMSC 23200 / 33250

THE UNIVERSITY OF CHICAGO

Instructors

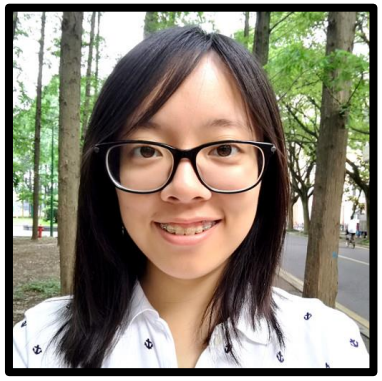
Blase Ur
blase@uchicago.edu

David Cash
davidcash@uchicago.edu

Four TAs

Alex Hoover

Julia Hanson



Weijia He

Will Brackenbury

Website / Syllabus

https://www.classes.cs.uchicago.edu/archive/2021/winter/23200-1/

Or https://bit.ly/35uvMOh

Live Lecture Recordings

- Monday/Wednesday/Friday 3:00-4:00pm
- Attendance at live lecture recordings is optional; they will be made available right after the lectures for asynchronous viewing

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
- 9 Assignments (91%)
  - Generally due Thursdays 11:59pm

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 (61%)
  - Generally due Thursdays 11:59pm
- Research project (30%)

Communication

- **Canvas** for assignment distribution
  - We manually added 33250 students
- **Campuswire** for discussion
  - Questions about assignments
  - Logistical requests
- **Gradescope** for submitting all work
- **Don't email us!** Use Campuswire!
  - Not on Campuswire? blase@uchicago.edu

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
  - This year has 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
- Remote interactions during lecture
  - Feel encouraged to add pronouns to name
  - Video is optional
  - Questions or answers? Raise hand or type (to all or whichever of David/Blase isn't teaching)

Academic Integrity Policy

- 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
- Detailed on syllabus

Office Hours

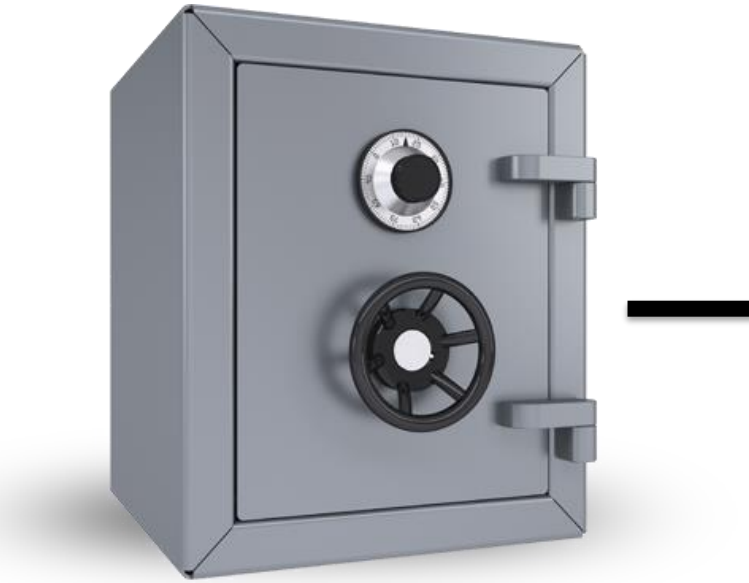
- Blase and David's office hours *(TBA)*
  - Talk about lectures / concepts in general
  - Get help with assignments
  - Get to know us!
- TA office hours *(TBA)*
  - Primary venue for help with assignments
  - Each assignment will have two TAs assigned
- All office hours will be held on Zoom

Are you not signed up yet?

- Currently 103 students enrolled
  - An additional 41 students on waiting list
- Want to switch from 23200 to 33250?
  - Submit an online consent request
- 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

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
- **Availability**: Information readily accessible
- **Authentication:** Principal/data is genuine
- **Accountability:** Responsible for past actions

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

Schedule of Topics (By Week)

1. Threat modeling and OS security
2. Memory vulnerabilities and protection
3. Software security and cryptography
4. Network and web basics
5. Web security
6. Web privacy and network security
7. Anonymity and authentication
8. Data privacy and database encryption
9. Hardware/ML/IoT security

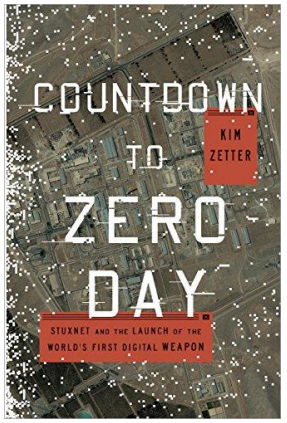
(Tentative) Assignments

1. Threat modeling *(written)*
2. Buffer overflows and memory attacks
3. Fuzzing, software analysis, crypto
4. Analysis of network traffic, X.509 certs
5. Web vulnerabilities
6. Implementing web tracking
7. Password cracking and attacks
8. Differential privacy / database encryption
9. Full-system analysis *(written)*

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 *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)

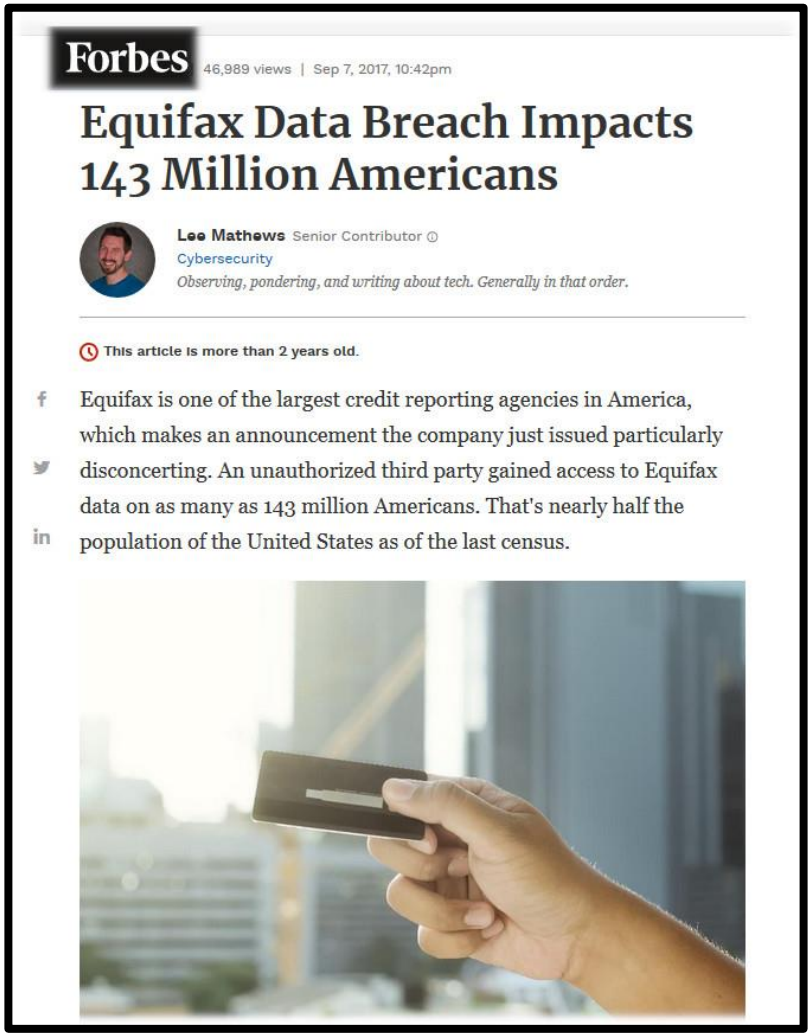
Edward Snowden

- 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

Parler (2021)

- This morning, a large archive of Parler posts (apparently including deleted private posts) was posted online
- Videos and photos included metadata
  - To support privacy, services should remove metadata when media files are uploaded
- The archive seems to be the result of a sequential crawl (and download) of all posts:
  - https://twitter.com/donk_enby/status/1348281459031814146