01. Course Introduction

Blase Ur and David Cash
January 6th, 2020
CMSC 23200 / 33250

THE UNIVERSITY OF
CHICAGO

Instructors

Blase Ur
JCL 363

David Cash
JCL 353

Website / Syllabus

https://www.classes.cs.uchicago.edu/archive/2020/winter/23200-1/

or

https://bit.ly/2sP9Wov

Textbook

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

Course Requirements (23200)

- 10 Reading Responses (10%)
  - Generally due Tuesdays 11:59pm
- 9 Assignments (76%)
  - Generally due Thursdays 11:59pm
- Closed-book final exam (11%)
- Class attendance / participation (3%)

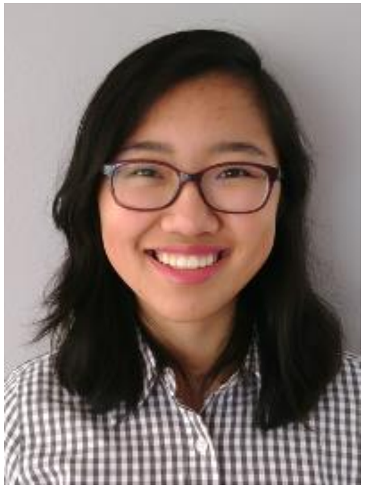
Course Requirements (33250)

- 8 Reactions to Research Papers (5%)
  - Generally due Mondays 11:59pm
- 10 Reading Responses (5%)
  - Generally due Tuesdays 11:59pm
- 9 Assignments (47%)
  - Generally due Thursdays 11:59pm
- Closed-book final exam (10%)
- Class attendance / participation (3%)
- Research project (30%)

Communication

- Canvas for submitting assignments and reading responses
  - We will manually add 33250 students
- Campuswire for discussion
  - Questions about assignments
  - Logistical requests
- (33250) Campuswire for submitting reactions to papers and project deliverables

Three TAs



Valerie
Zhao

Alex
Hoover

Rohan
Kumar

- Office hours TBA
  - Will be held in JCL 391

Additional policies

- Academic integrity
  - All work submitted must be your own
  - May speak in general terms about approach with others, but **document this** (see syllabus)
- Late submissions
  - Assignments and reading responses can be submitted 24 hours late for a 15 point penalty
  - No other late submissions are accepted
- Wellness

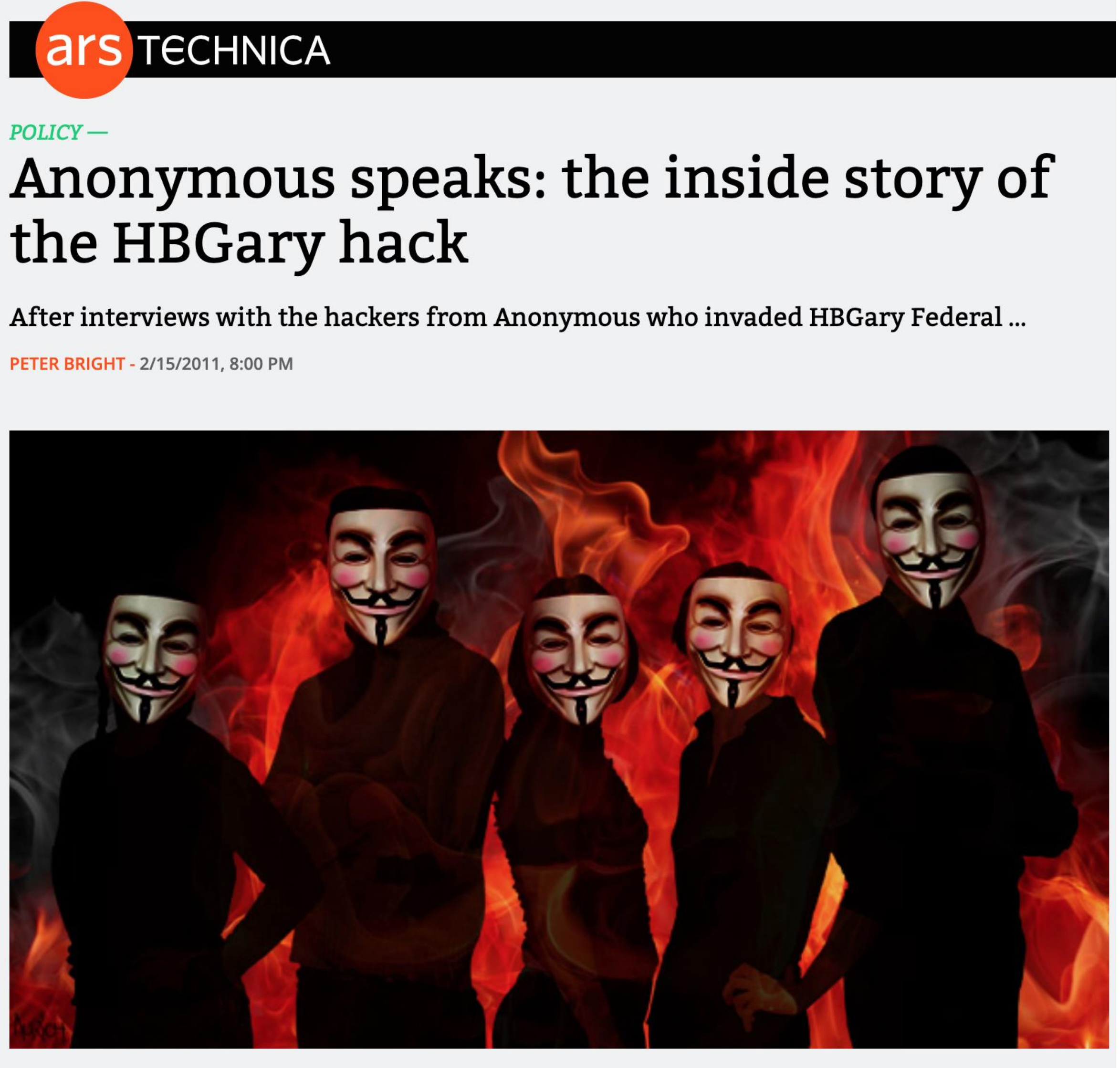
Are you not signed up yet?

- Currently 65 students enrolled
  - An additional 66 students on waiting list
- Want to switch from 23200 to 33250?
  - Submit a consent request
- Do you not have a seat at all?
  - If you have an urgent need to take the class this quarter, come speak to us after class.
  - Otherwise, try again next year.
- Email blase@uchicago.edu for Canvas

Schedule of Topics

1. Security mindset and cryptography
2. Cryptography and blockchain
3. How the Internet & networks work
4. Web security and privacy
5. Network security and anonymity
6. Authentication
7. Data privacy, database encryption
8. Systems and software security
9. Hardware security and current topics
10. Mobile, IoT, and security in practice

Historical incident: HB Gary



ars TECHNICA

POLICY —

Anonymous speaks: the inside story of the HBGary hack

After interviews with the hackers from Anonymous who invaded HBGary Federal ...

PETER BRIGHT - 2/15/2011, 8:00 PM

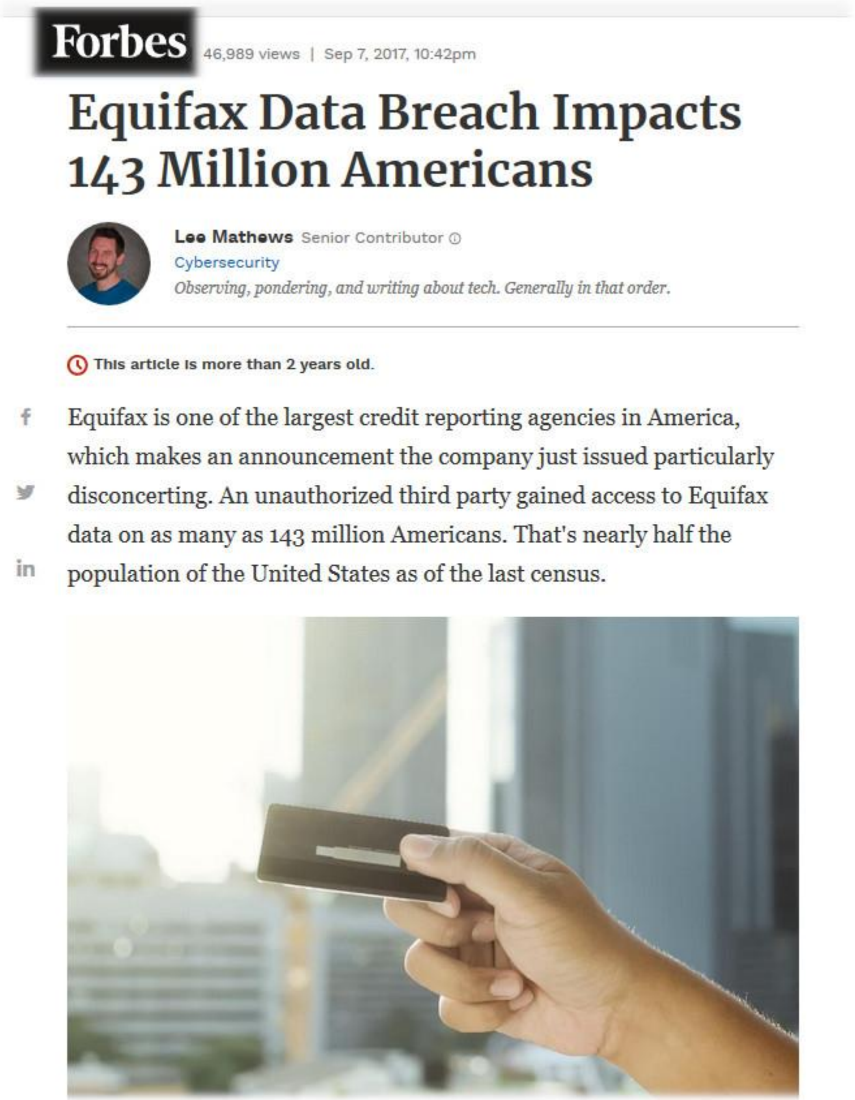
https://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

HB Gary incident

1. Security mindset and cryptography
2. Cryptography and blockchain
3. How the Internet & networks work
4. Web security and privacy
5. Network security and anonymity
6. Authentication
7. Data privacy, database encryption
8. Systems and software security
9. Hardware security and current topics
10. Mobile, IoT, and security in practice

Historical incident: Equifax

Historical incident: Equifax



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.

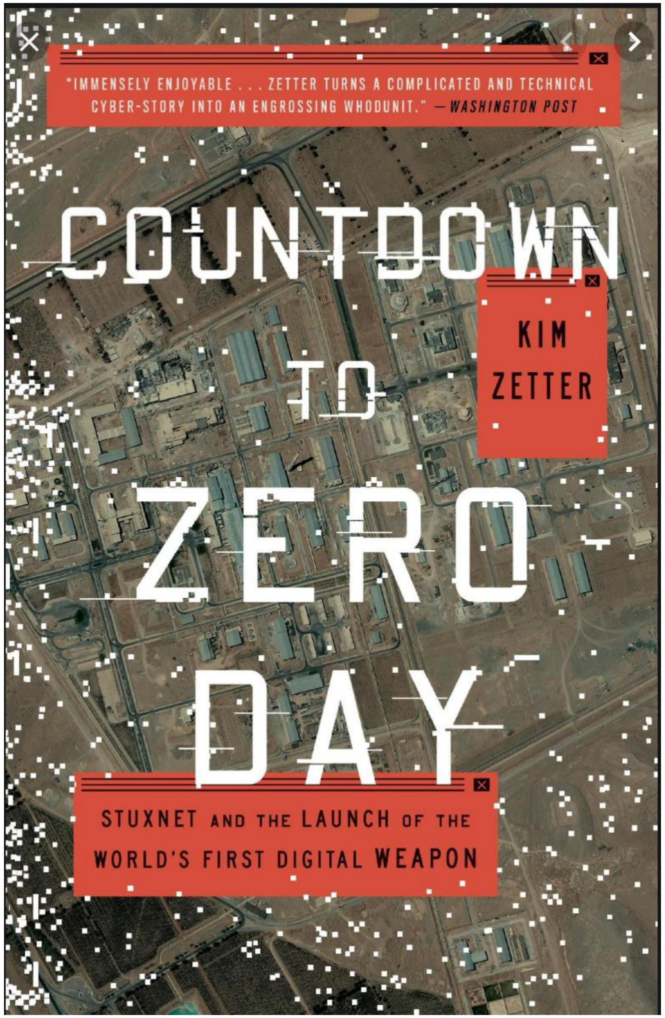
Equifax is one of the largest credit reporting agencies in America, which makes an announcement the company just issued particularly disconcerting. An unauthorized third party gained access to Equifax data on as many as 143 million Americans. That's nearly half the population of the United States as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

https://www.wired.com/story/how-to-stop-breaches-equifax/

Equifax incident

1. Security mindset and cryptography
2. Cryptography and blockchain
3. How the Internet & networks work
4. Web security and privacy
5. Network security and anonymity
6. Authentication
7. Data privacy, database encryption
8. Systems and software security
9. Hardware security and current topics
10. Mobile, IoT, and security in practice

Historical incident: Stuxnet


"IMMENSELY ENJOYABLE . . . ZETTER TURNS A COMPLICATED AND TECHNICAL CYBER-STORY INTO AN ENGROSSING WHODUNIT." — WASHINGTON POST
COUNTDOWN TO ZERO DAY
KIM ZETTER
STUXNET AND THE LAUNCH OF THE WORLD'S FIRST DIGITAL WEAPON

Stuxnet incident

1. Security mindset and cryptography
2. Cryptography and blockchain
3. How the Internet & networks work
4. Web security and privacy
5. Network security and anonymity
6. Authentication
7. Data privacy, database encryption
8. Systems and software security
9. Hardware security and current topics
10. Mobile, IoT, and security in practice

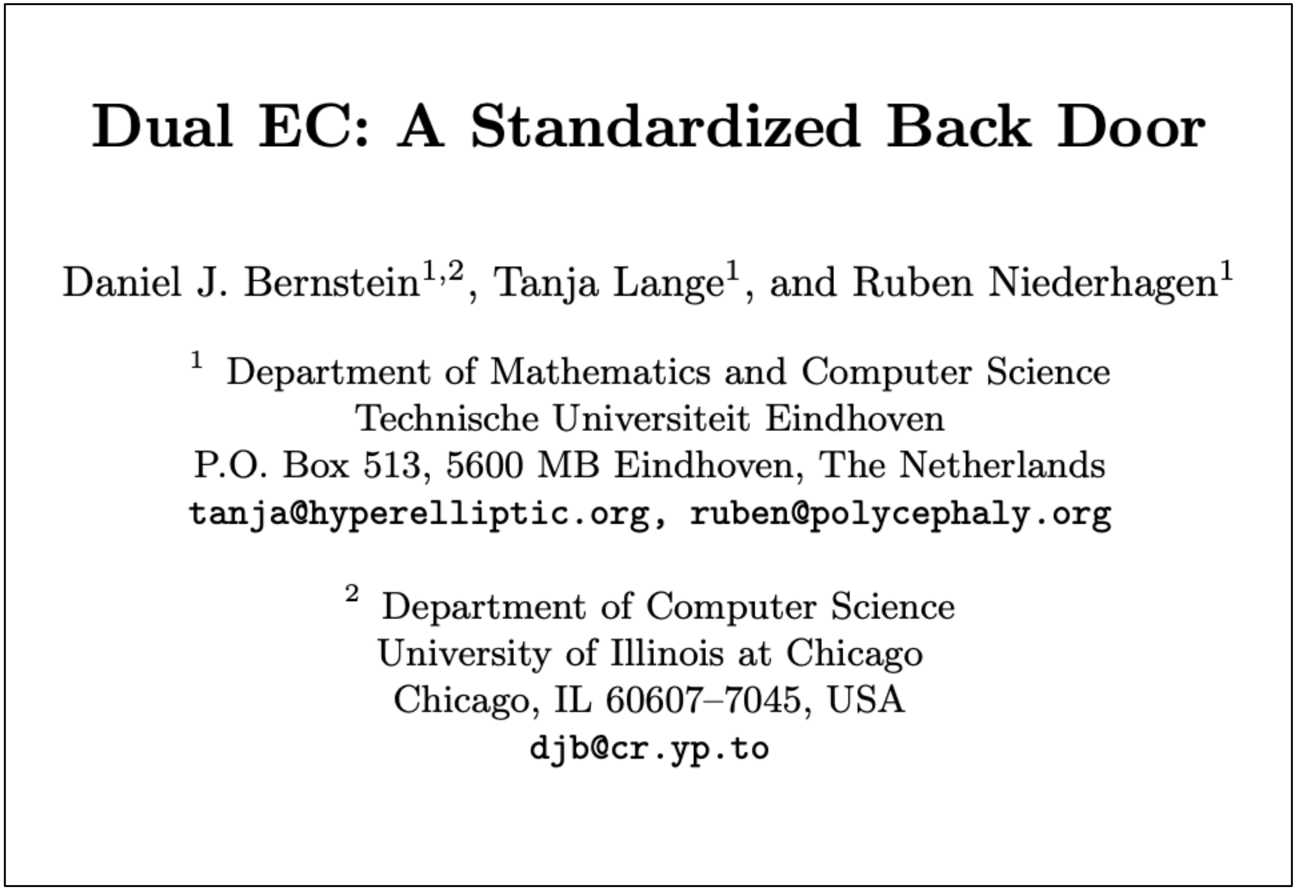
Historical incident: Target Breach

https://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

Target incident

1. Security mindset and cryptography
2. Cryptography and blockchain
3. How the Internet & networks work
4. Web security and privacy
5. Network security and anonymity
6. Authentication
7. Data privacy, database encryption
8. Systems and software security
9. Hardware security and current topics
10. Mobile, IoT, and security in practice

Historical incident: Dual EC



Dual EC: A Standardized Back Door

Daniel J. Bernstein[1,2], Tanja Lange[1], and Ruben Niederhagen[1]

[1] Department of Mathematics and Computer Science
Technische Universiteit Eindhoven
P.O. Box 513, 5600 MB Eindhoven, The Netherlands
`tanja@hyperelliptic.org, ruben@polycephaly.org`

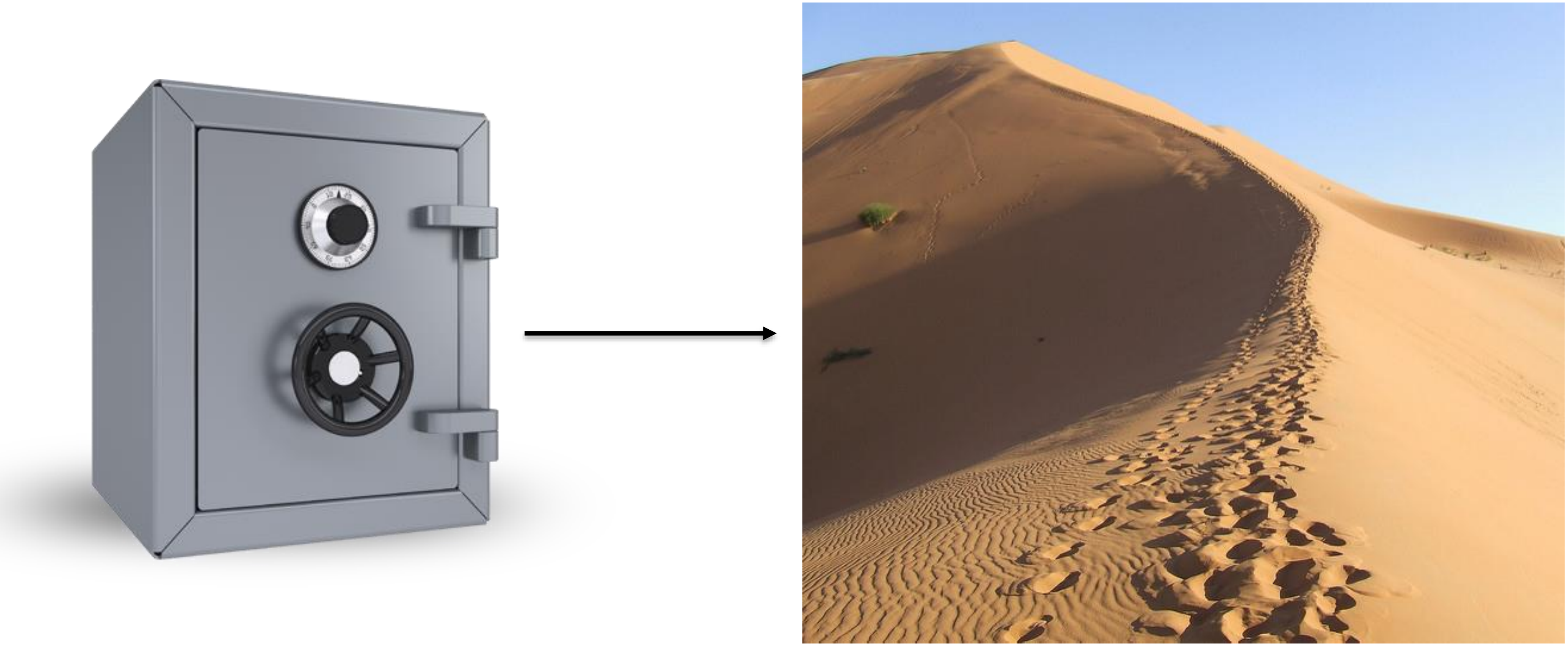
[2] Department of Computer Science
University of Illinois at Chicago
Chicago, IL 60607–7045, USA
`djb@cr.yp.to`

https://eprint.iacr.org/2015/767.pdf

Dual EC incident

1. Security mindset and cryptography
2. Cryptography and blockchain
3. How the Internet & networks work
4. Web security and privacy
5. Network security and anonymity
6. Authentication
7. Data privacy, database encryption
8. Systems and software security
9. Hardware security and current topics
10. Mobile, IoT, and security in practice

How can we keep something secure?



What properties do we want?

- **Confidentiality**: Non-public information accessible only to authorized parties
- **Integrity**: Information not secretly modified
- **Authorization:** Information is accessible only by authorized entities
- **Availability**: Information is readily accessible
- **Authentication:** Principal or data is genuine
- **Accountability:** Responsible for past actions