Lessons Not Learned: We Still Can't Even Get the Basics Right

...OF CS 116 INTRODUCTION TO SECURITY, FALL 2023

Before We Begin, Let's Talk About Dirty Secrets About This Class
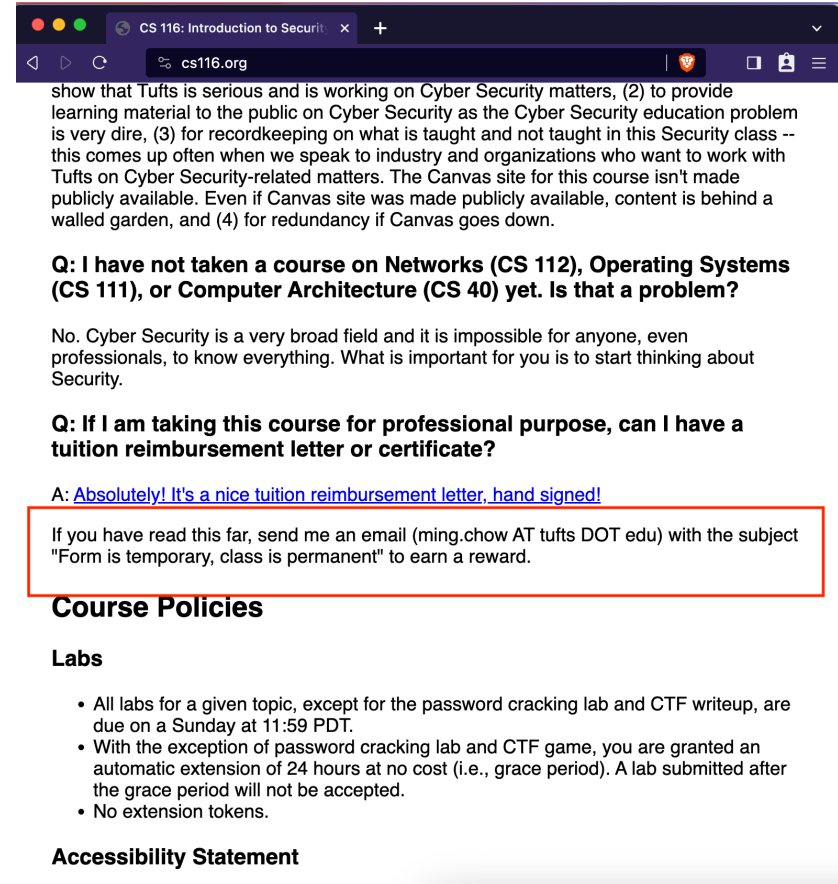
Dirty Secret 1: Only 22 students read the syllabus

100 students enrolled in CS 116 (Tuesday-Thursday section)

24 students enrolled in CS 116 (Online Masters Wednesday section)

Total: 124 students

17.7% of students read the syllabus

Emails ranged from August 28th to December 1st

show that Tufts is serious and is working on Cyber Security matters, (2) to provide learning material to the public on Cyber Security as the Cyber Security education problem is very dire, (3) for recordkeeping on what is taught and not taught in this Security class -- this comes up often when we speak to industry and organizations who want to work with Tufts on Cyber Security-related matters. The Canvas site for this course isn't made publicly available. Even if Canvas site was made publicly available, content is behind a walled garden, and (4) for redundancy if Canvas goes down.

Q: I have not taken a course on Networks (CS 112), Operating Systems (CS 111), or Computer Architecture (CS 40) yet. Is that a problem?

No. Cyber Security is a very broad field and it is impossible for anyone, even professionals, to know everything. What is important for you is to start thinking about Security.

Q: If I am taking this course for professional purpose, can I have a tuition reimbursement letter or certificate?

A: Absolutely! It's a nice tuition reimbursement letter, hand signed!

If you have read this far, send me an email (ming.chow AT tufts DOT edu) with the subject "Form is temporary, class is permanent" to earn a reward.

Course Policies

Labs

- All labs for a given topic, except for the password cracking lab and CTF writeup, are due on a Sunday at 11:59 PDT.
- With the exception of password cracking lab and CTF game, you are granted an automatic extension of 24 hours at no cost (i.e., grace period). A lab submitted after the grace period will not be accepted.
- No extension tokens.

Accessibility Statement

Dirty Secret 1: The Honor Roll

Benn, Yan, Siara, Ethan, Grayson, Valerie, Sam, Nathaniel, Ian, Kenny, Rafael, Jack, Gizem, Chris, Frederick, Simon, Angela, Maya, Idil, Anya, Gavin, Helena

Dirty Secret 2: The NSA er... Canvas Puzzle

25 students (or 20.1% of students) decoded the Base64 string

"Don't Dream It's Over"

Emails ranged from August 29th to November 30th

Puzzle solving and intellectual curiosity are critical skills in Security

Fall 2023

Fa23-CS-0116-01-Introduction to Security   ✏ Edit   ⋮

Home

Assignments

Piazza

Quizzes

People

Grades

Announcements   🚫

Rubrics   🚫

Discussions   🚫

Pages   🚫

Syllabus   🚫

Files   🚫

Public Course Website: https://cs116.org/ ⤢

Q29uZ3JhdHVsYXRpb25zIGRlY29kaW5nIHRoaXMuIE5vdyBlbWFpbCBtZSBhdCBtaW5nLmNob3dAdHVmdHMuZWR1IHdpdGggdGhlIHN1YmplY3QgbGluZTogRG9uJ3QgRHJlYW0gSXQncyBPdmVy

Dirty Secret 2 : The Honor Roll

Benn, Simon, Nasir, Yan, Wei, Danesia, Declan, Matt, Andres, Samay, Lucas, Grayson, Valerie, Mira **, Yunxuan, Weiwei, Daniel, Dale, David, Sam, Basak **

(** Both Mira and Basak "finished the job" and knew exactly what to do)

Dirty Secret 3: Special Congrats

…to Simon, Samay, and Gavin

..you know what you did!

#LeChampion #JerichoAppreciationSociety #AEW

Dirty Secret 4: About Lab 9, The Technical Risk Analysis Lab

You received either a 6 or a 10 / 10

The point being: it's not okay to have hardcoded passwords in this day in age. You can't make those mistakes.

And Now For The Feature Presentation

Motivation

- A list of bright shiny objects seen in security products and startups (or buzzword hell)
  - APTs
  - Machine Learning
  - Comprehensive cybersecurity
  - Real-time monitoring
  - Behavioral analysis
  - Next-gen <FILL IN THE BLANKS> (thanks Russell Butturini)
  - Xgen
  - Cloud-enabled

Motivation (continued)

- ¯_(ツ)_/¯
  - ["Top US Undergraduate Computer Science Programs Skip Cybersecurity Classes"](#)
  - ["Here are the 61 passwords that powered the Mirai IoT botnet"](#)
  - ["One of the Largest Hacks Yet Exposes Data on Hundreds of Thousands of Kids"](#)
  - ["Yahoo Says Hackers Stole Data on 500 Million Users in 2014"](#)

Motivation (continued)

Source:
https://twitter.com/jeremiahg/status/866783974311444480

The Gist

- Those motivating slides were from a presentation I gave in 2017
- I could give the same exact talk from 2017 now, without any changes, and get away with it
- In 2013, Veracode gave a presentation "We See the Future and it's Not Pretty". The predictions were accurate.
- While a lot of things have changed, a lot have stayed the same...

VERACODE

Key Findings:

- 70% of applications failed to comply with enterprise security policies on first submission.
- SQL injection prevalence has plateaued, affecting approximately 32% of web applications.
- Eradicating SQL injection in web applications remains a challenge as organizations make tradeoffs around what to remediate first.
- Cryptographic issues affect a sizeable portion of Android (64%) and iOS (58%) applications.

Predictions:

- Average CISO Tenure Continues to Decline.
- The Rise of the Everyday Hacker
- Decreased Job Satisfaction/ Higher Turn-over for Security Professionals.
- Default Encryption, Not "Opt-in," Will Become the Norm.

Let's Start With Education...

- Colleges and universities now offering Cyber Security programs
- Plethora of free Cyber Security programs offered online

...however (with regards to education)

- The Cyber Security programs offered at colleges and universities are mostly graduate-level programs
- By end of undergraduate computing science or engineering program, most graduating still have no knowledge of Security
- Most students don't know about the opportunities online to learn
- Few K-12 opportunities or requirements

Application Architecture

- Boils down to one word: cloud (a.k.a., someone else's computer)

...however (with regards to application architecture)

- Same mistakes from decades ago still being made
  - Open FTP servers => open AWS S3 buckets, open ElasticSearch instances
  - Open [insert favorite service here]

Data Privacy

- Alphabet soup of U.S. data privacy laws, federal and state level
- At the international level, there is now the General Data Protection Regulation (GDPR)

...however (with regards to data privacy)

- But what's the point when companies and institutions collect so much data --and then they all get broken into? (too many companies and institutions to name)
- Plethora of vulnerable voter databases via SQL injection
- Open databases and buckets there for the taking (see previous slide on application architecture)
- Leaky application programming interfaces (APIs)
- Data sold on forums for cheap

Are We Still Facing These Problems?

- Phishing and social engineering
- Password reuse
- Weak passwords
- Distributed Denial of Service (DDoS)

Geopolitical Changes

- Full-blown international crisis
- Infrastructure now being attacked: hospitals, schools, utilities
- Almost impossible to read an article about an incident without a country being named

Options We Now Have

1. (really easy) no changes, business as usual
2. (really hard and really expensive) draconian changes including requiring Cyber Security education at K-12 level
   a. Example: Cybersecurity Maturity Model Certification (CMMC)

Solutions

- Immediate: password managers, multi-factor authentication, input sanitization
- Intermediate term: "Don't call it a comeback" --invest in old-school, no/non-tech, and radical (thanks Matt)
  - Example: the U.S. Navy is resurrecting celestial navigation
- Long term: invest in Cyber Security education early
- Continuing:
  - Connecting and communicating with non-technical folks and the policymakers (policy)
  - Simplicity
- Last resort: the heavy hand of legislation

But For Now and For the Future

- Crime will continue to pay --and pay well
- We will still be talking about a Cyber Security skills shortage
    - I've been monitoring how long we've been playing this game for
      https://gist.github.com/mchow01/9569350f3b975ce84dad68f0d95c4579
- There will be another Executive Order on Improving the Nation's (United States) Cybersecurity
- In five years, someone will still be giving a presentation on what SQL injection is, what DDoS is
- In five years, I can give this presentation again without any changes, and get away with it

References

1. https://comp116.org/readings/predicting_the_future_veracode.pdf
2. https://www.csoonline.com/article/3535797/the-cybersecurity-maturity-model-certification-explained-what-defense-contractors-need-to-know.html
3. https://threatpost.com/sql-injection-attack-is-tied-to-election-commission-breach/122571/
4. https://abc7chicago.com/politics/how-the-russians-penetrated-illinois-election-computers/3778816/
5. https://www.popularmechanics.com/military/research/a36078957/celestial-navigation/

My Final Thoughts

The Ultimate Goal of This Course: For You To Be A Good Citizen

- We are still battling the same vulnerabilities, having the same debates, for the last 2+ decades

- Your job: talk to others, especially non-tech folks.
  - Example 1: inform developers it is really bad to use C functions like strcpy()
  - Example 2: engage in constructive debates, uncomfortable conversations

- If I still teach this course in 20 years with the same message, then something is terribly wrong

- December 8, 2015: "Congress puts terrorism and tech in the spotlight (CNN)"
  https://money.cnn.com/2015/12/08/technology/encryption-congress-commission/