CS 410/510: Web Security
Motivation

- Security issues are having a real impact
Motivation

07  Tech Firm Ubiquiti Suffers $46M Cyberheist
AUG 15

Networking firm Ubiquiti Networks Inc. disclosed this week that cyber thieves recently stole $46.7 million using an increasingly common scam in which crooks spoof communications from executives at the victim firm in a bid to initiate unauthorized international wire transfers.
Motivation

Look familiar? China finally unveils its J-20 stealth fighter jet, thought to be based on US war plane plans 'stolen' by hackers

By RYAN O'HARE FOR MAILONLINE and AFP
Motivation

How a hacker's typo helped stop a billion dollar bank heist

Unknown hackers still managed to get away with about $80 million, one of the largest known bank thefts in history.
Motivation

- Security issues are having a real impact

"STUXNET VIRUS SET BACK IRAN’S NUCLEAR PROGRAM BY 2 YEARS"

BY YAakov KATZ / DECEMBER 15, 2010 05:15

Top German computer consultant tells 'Post' virus was as effective as military strike, a huge success; expert speculates IDF creator of virus.
Motivation

• Russian 2016 election hacking
  • Influence election via fake news and exposing secrets
  • Destroy confidence in the US election system
    • Slow down voting systems used in strategic local election offices
    • Compromise machines used to count votes and register voters
    • Sow the seeds of distrust in the system

• Fake news or not?
  • Either way, successful in sowing the seeds of distrust in the system
Future elections

- What should we focus on for 2018?
- Election systems only considered critical infrastructure recently
- Gen. John Allen
  - [https://www.lawfareblog.com/lawfare-podcast-brookings-panel-cybersecurity-us-elections](https://www.lawfareblog.com/lawfare-podcast-brookings-panel-cybersecurity-us-elections)

“As a guy who has spent a lot of time overseas dealing with threats to America, I now recognize at the speed of light, the very heartland of America is under threat today. The enemy has moved beyond my reach. The first line of defense of American democracy and the last line of defense are in our states and counties.”
2016 Cybersecurity Skills Gap

Too Many Threats

$1 BILLION: PERSONALLY IDENTIFIABLE INFORMATION (PII) RECORDS STOLEN IN 2014

97% BELIEVE APTS REPRESENT CREDIBLE THREAT TO NATIONAL SECURITY AND ECONOMIC STABILITY

MORE THAN 1 IN 4 ORGANIZATIONS HAVE EXPERIENCED AN APT ATTACK

$150 MILLION: AVERAGE COST OF A DATA BREACH BY 2020

1 IN 2 BELIEVE THE IT DEPARTMENT IS UNAWARE OF ALL OF ORGANIZATION'S INTERNET OF THINGS (IOT) DEVICES

74% BELIEVE LIKELIHOOD OF ORGANIZATION BEING HACKED THROUGH IOT DEVICES IS HIGH OR MEDIUM

Too Few Professionals

2 MILLION: GLOBAL SHORTAGE OF CYBERSECURITY PROFESSIONALS BY 2019

3X RATE OF CYBERSECURITY JOB GROWTH VS. IT JOBS OVERALL, 2010-14

84% ORGANIZATIONS BELIEVE HALF OR FEWER OF APPLICANTS FOR OPEN SECURITY JOBS ARE QUALIFIED

53% OF ORGANIZATIONS EXPERIENCE DELAYS AS LONG AS 6 MONTHS TO FIND QUALIFIED SECURITY CANDIDATES

77% OF WOMEN SAID THAT NO HIGH SCHOOL TEACHER OR GUIDANCE COUNSELOR MENTIONED CYBERSECURITY AS CAREER

89% OF U.S. CONSUMERS BELIEVE IT IS IMPORTANT FOR ORGANIZATIONS TO HAVE CYBERSECURITY-CERTIFIED EMPLOYEES

Cyberattacks are growing, but the talent pool of defenders is not keeping pace.

Although attacks are growing in frequency and sophistication, the availability of sufficiently skilled cybersecurity professionals is falling behind. Cybersecurity Nexus (CSX) is addressing this gap by creating a skilled global cybersecurity workforce. From the Cybersecurity Fundamentals Certificate for university students to CSXP, the first vendor-neutral, performance-based cybersecurity certification, CSX is attracting and enabling cybersecurity professionals at every stage of their careers.

Why web security?

- Most new apps offered via web
  - Web as a “carrier” protocol for Internet apps
- Exploitation via the web now a common vector
  - SQL injection
  - Cross-site requests
  - Session hijacking
  - Click-jacking
This course

- A quick primer on the web and how it works
- A look at common classes of web vulnerabilities
- Hands-on practice exploiting web vulnerabilities
  - Exercises to demonstrate the overall vulnerability class
  - Help train an adversarial mindset
- Prevention techniques
- Will hopefully be useful at some point in your career
Based all on CTFs

- “Capture-the-Flag”
  - Sets of challenges used in security competitions
  - Understand and apply specific security concepts to find a hidden flag
  - Used to train a variety of skills (reverse-engineering, exploitation, cryptography etc.)
  - Focus on skill development
  - Puts valuable content in a fun format
- Many CTFs focused on web security due to its importance
- Why build a course on CTFs?
  - Extracurricular CTF not working
  - CTF for credit!
In-class labs and lab notebook

- Flipped classroom: Students are expected to watch video lectures which will review an issue in web security
- In-class labs to demonstrate and exploit
- Can optionally be done in pairs
  - Peer learning
  - Ensure progression
- Write-ups for each level to be kept in a single lab notebook document turned in at the end of course
  - Grading rubric
    - Number of levels solved
    - Description of vulnerability
    - Description of technique, URL, or script used to exploit vulnerability
    - Description of prevention or other remediation to mitigate threat
- Will require some short Ruby programs
Homework and programs

- To be done individually
- Homework CTF
  - [http://cs410.oregonctf.org](http://cs410.oregonctf.org)
  - Levels opened up (and closed) as we go along
- Programming assignments
  - Python programs to programmatically attack web vulnerabilities
  - Assumes knowledge of Python or willingness to learn it on your own
Final project

- Can optionally be done in pairs
- Chosen from selected PentesterLab exercises
- Turned in as a screencast walkthrough posted on course channel on MediaSpace (https://media.pdx.edu)
- Grading rubric
  - Exercise difficulty
  - Availability of prior walkthroughs
  - Clarity and completeness of walkthrough (including setup)
  - Analysis of vulnerability and description of prevention/remediation
- Final exam slot
  - Walkthrough of another group’s final project
Attendance and Weekly Quiz

- Attendance Required
  - Not included in grading scheme
  - Treat classes as practice (e.g. like in sports, music)
- Weekly Quiz
  - Quiz on Thursdays covering the topics scheduled for that particular week
Schedule and Grading Scheme

- Check the course web site
Course logistics

- Course site ([https://thefengs.com/wuchang/courses/cs410](https://thefengs.com/wuchang/courses/cs410))
  - Schedule
  - Grading
  - Content links
- Homework site ([http://cs410.oregonctf.org](http://cs410.oregonctf.org))
- Program submission via D2L ([https://d2l.pdx.edu](https://d2l.pdx.edu))
- Final project submission via Media Space ([https://media.pdx.edu](https://media.pdx.edu))
- Course discussion on #cs410_510_websec2018 on Slack ([https://pdx-CS.slack.com](https://pdx-CS.slack.com))
- Instructor contact @Liz on pdx-CS Slack
- In-class questions and feedback (anonymous)
  - [https://sayat.me/lizlawrens](https://sayat.me/lizlawrens)
Ethics

- You will learn techniques and tools for compromising web systems
- Do *NOT* use them against any site outside of the course web sites unless given permission
- CTFs and private instances help you learn and practice security concepts (without breaking the law)
  - CFAA
• Jeff Williams, Dave Wichers (2013)
  • Vulnerabilities ranked based on business risk (likelihood + impact)