CSE 40567 / 60567: Computer Security

Course Introduction / Security Basics 1
Course Info:

- CSE 40567 / 60567: Computer Security
- Instructor: Walter Scheirer (wscheire@nd.edu; @wjscheirer)
- Office: 182D Fitzpatrick
- Lectures: TR 2:00-3:15 DeBartolo Hall 126
- Office Hours: Tues. & Thurs. 12-1:45pm and by appointment.

Course Website: http://www.wjscheirer.com/teaching/security/
Course Slack Team

nd-cse.slack.com
#cse-40567-sp20
Grad TA

- **Sophia Abraham**
- sabraha2@nd.edu
- Office Hours: Fri. 11:30am-1:30pm
  - Center for Digital Scholarship
    (Hesburgh Library)
Grad TA

• Tanner Juedeman
  • tjuedema@nd.edu
  • Office Hours: Wed. 3:30-5:30pm
    - South Duncan Student Center
About me

• Joined Notre Dame Summer 2015
  - Ph.D. from the University of Colorado 2009
  - 2012 — 2015 Harvard University Center for Brain Science

• Research in Computer Vision and Machine Learning
How about you?

- Undergrad / M.S. / Ph.D.?
- Any experience with Operating Systems, Networking, or Cryptography?
- What interests you about Computer Security?
Course Overview

- 23 lectures
- 8 homework assignments
- 1 mid-term exam (in-class)
- 1 documentary film screening (*The Great Hack*)
- 3 invited talks
- Final exam
Course Overview

*Full syllabus on course website

Grading

<table>
<thead>
<tr>
<th>Component</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Participation</td>
<td>100</td>
</tr>
<tr>
<td>Homework assignments</td>
<td>8 x 125</td>
</tr>
<tr>
<td>Midterm Exam</td>
<td>400</td>
</tr>
<tr>
<td>Final Exam</td>
<td>500</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td>2000</td>
</tr>
</tbody>
</table>

Important Dates

- **Homework #1 (Security Basics)**
  - Released: 1/21; Due: 1/28
- **Homework #2 (Cryptographic Protocols)**
  - Released: 1/30; Due: 2/6
- **Homework #3 (Cryptographic Protocols)**
  - Released: 2/11; Due: 2/18
- **Homework #4 (Software Security)**
  - Released: 2/20; Due: 2/27
- **Midterm Exam**
  - 2/27
- **Film Response**
  - Released: 3/3; Due: 3/6
- **Homework #5 (Software Security)**
  - Released: 3/17; Due: 3/24
- **Homework #6 (Network Security)**
  - Released: 3/31; Due: 4/7
- **Homework #7 (Network Security)**
  - Released: 4/9; Due: 4/16
- **Homework #8 (Web Security)**
  - Released 4/21; Due: 4/28
- **Final Exam**
  - 5/7
March 24th

Ariel Herbert-Voss (aka Adversariel) from OpenAI on Hacking AI
April 16th

Stephen Watt from Farsight Security on His Odyssey Through the Criminal Justice System
April 28th

RC Johnson from PayPal on Keeping Your Money Safe from Hackers
Prerequisites

Required prerequisite course: data structures (CSE 30331/34331)

You especially need to be comfortable programming in Python and C/C++ in the Unix environment
Textbook

All chapters are a **free** download:  
http://www.cl.cam.ac.uk/~rja14/book.html

Other readings will be posted to the course website; keep an eye on the progress page
Course Objectives

- Describe and apply the principles of three core areas of computer security
- Engineer practical security systems with risk mitigation as a guiding philosophy
- Select current cryptographic algorithms with appropriate cryptographic primitive lengths
- Detect weaknesses in cryptographic implementations that can lead to data compromise
- Identify bugs and poor practices that can lead to vulnerabilities in hardware and software
Course Objectives

• Develop and deploy software solutions for system and network attacks and defense

• Reverse engineer proprietary and obfuscated binary code for auditing purposes

• Understand the components of secure web app development;

• Itemize the most up-to-date security threats propagating on the Internet, as well as the corresponding countermeasures
Course Roadmap

Basics
(weeks 1 & 2)

3 Core Areas
(weeks 3 - 6)

The Web
(weeks 15 & 16)

(weeks 6 - 10)  (weeks 11 - 15)
What is this course all about?
Six Representative Cases
Target Breach: December 2013

One of the largest thefts of credit card data in US history:

40 Million Stolen Numbers
70 Million Customer Records

The cost: over 90 lawsuits, $61M in immediate post-incident response, billions projected cleaning up the mess going forward…

How did the attack unfold?

1. Attackers obtained HVAC vendor credentials; performed network reconnaissance

2. CC sniffing program installed at cashier stations

3. Installed malicious code to send CC numbers to staging sites in the US and Russia

4. On Dec. 2nd, CC numbers started flowing out of POS terminals; Target's IDS detects the attack

5. On Dec. 12th, Federal investigators warned of a massive data breach at Target

6. On Dec. 15th, Target confirms eradication of threat, after 40 million CC numbers compromised
How was the attack detected?
Where was the incident response?

- Incident alert triggered on Nov. 30th by FireEye
- As attackers installed software, additional alerts were generated at the “urgent” level
- FireEye’s platform can automatically stop attacks after they are detected
  - This feature was disabled by Target
    - Such an action is not uncommon
Who was responsible?

• Some clues found in the code used in the attack
  - Recovered password was “Crysis1089”
    ‣ Known Xbox gamer handle (ranked 11,450,001 in March 2014)
    ‣ Reference to October 1989 demonstrations in Ukraine, preceding breakup of the Soviet Union
Who was responsible?

• Another string was embedded in the malicious code: “Rescator”
  - Reference to a pirate in the 1967 French film *Indomptable Angélique*
  - Also the handle of a prolific Ukrainian CC number trafficker
    • Operates a number of sites selling numbers
    • Based in Odessa
    • Could be an Odessa man named Andrey Khodyrevskiy, who was arrested previously for hacking
JPMorgan Chase Hack: Summer 2014

The Timeline:

June 2014: Intrusion begins

July 2014: Intrusion detected

October 2015: Intrusion disclosed. 76 million households, seven million small businesses affected

July 2015: Arrests made in case, pointing to larger conspiracy

Profile of the attack

- 90 servers compromised
- Customer contact information obtained: names, addresses, email addresses, and phone numbers
  - Ammunition for a phishing attack
- Attackers compiled list of programs running on JP Morgan Chase’s Network
  - Used to cross-check against known vulnerability lists

Curious factor: no attempt to steal money
Criminal syndicate

Three charged with complex securities fraud scheme

“Pump-and-dump” plot: used bulk email and pre-planned trading to boost certain stock prices to their benefit

Captured

Photo credit: Barel Efraim
Sony Pictures Entertainment Hack: November 2014

- “Guardians of Peace” claim to steal over 100TB of data from Sony pictures
- Apparent retribution for the production of the film *The Interview*
- Leaked emails continue to be released

Ransomware

- **Wiper**: targeted malware software that deletes data on command

- 3,500+ employees saw the screen on the right

- Several Twitter accounts also compromised

FBI and FireEye brought in to investigate and respond to the incident
Was it really North Korea?

- Evidence of North Korean involvement is circumstantial
- Doubts of infrastructure readiness to pull off such an attack
- Alternate explanation: an inside job
  - Six disgruntled employees could have perpetrated the attack

**US Response: additional sanctions enacted against North Korea**

WikiLeaks: 2006 - present

Technology is not always the weak link

Afghan War documents leak (75K)
Iraq War documents leak (392K)
Diplomatic cables leak (251K)

Chelsea Manning convicted or suspected of leaking in all three cases

Sentence commuted in 2017
Back in prison in 2019
WikiLeaks Interference in the 2016 Presidential Election

July 22nd 2016: ~20,000 emails and 8,000 files from the DNC released

October 7th 2016: emails and documents authored by Clinton campaign manager John Podesta released

Hacker or hacker persona “Guccifer 2.0” claims responsibility for the leaks
Internet of Things Powered Distributed Denial of Service Attacks: 2016

October 21st, 2016: Major DDoS attack hits DNS provider Dyn

• Mirai botnet contains millions of infected devices
• Attack vector: default usernames and passwords
Equifax Hack: 2017

“[The Equifax breach] very possibly is the most severe of all for a simple reason: the breath-taking amount of highly sensitive data it handed over to criminals.”

- Dan Goodin, *Ars Technica*, 2017

• 145.5 million U.S. consumers affected
  ▸ First and last names, **Social Security numbers**, birth dates, addresses and, in some instances, driver’s license numbers
Attack Vector: Web Exploit

Apache Struts Flaw (CVE-2017-5638)

Patch for vulnerability was released on March 7th, 2017

Data breach occurs May - July 2017

Other contributing factors: lack of network segmentation, weak encryption mechanisms for personally identifiable information, lack of intrusion detection mechanisms
What is the scope of the problem we face?

Snapshot of one threat: Distributed Denial of Service Attacks

Global DDoS attacks grew 90% from Q4 2013 to 2014

Is security getting better or worse?

Worse: More attacks

Better: Improved technologies and practices
Academic vs. practical security

Harsh Reality of Practical Security

Lush Garden of Academic Security Study
Modern approach to cryptography:

“studying the theory and designing systems which you can prove are secure.”

-Colin Percival
Provable Security

There are several approaches to this:

Unconditional
(information theoretic security)

- Security against all attackers
- No bound on computation
- Example: one-time pad

D. Stebila, “An introduction to provable security,” AMSI Winter School on Cryptography

Provable Security

There are several approaches to this:

- **Formal Methods**
  - Computer-verified security of scheme
  - Typically assumes underlying cryptography is perfect
Provable Security

There are several approaches to this:

Reductionist Proof

- Manual proof of security of scheme
- Typically reduces security of scheme to security of an underlying hard problem

“If it’s provably secure, it probably isn’t.”

-Lars Knudsen
Why isn’t provable security actually secure?

• Proofs take very specific forms against very specific attacks
• Proofs are predicated on assumptions (which aren’t realistic in all cases)
• Practical engineering problems
• They tend to miss the human element of attack
Cases where cryptographic systems break before the universe expires

- Software mistakes in implementations
- Key left in memory, OS wrote it back to disk
- Buffer overflows and other security flaws
- Side-channel attacks
- Bad UIs
- Bad user practices