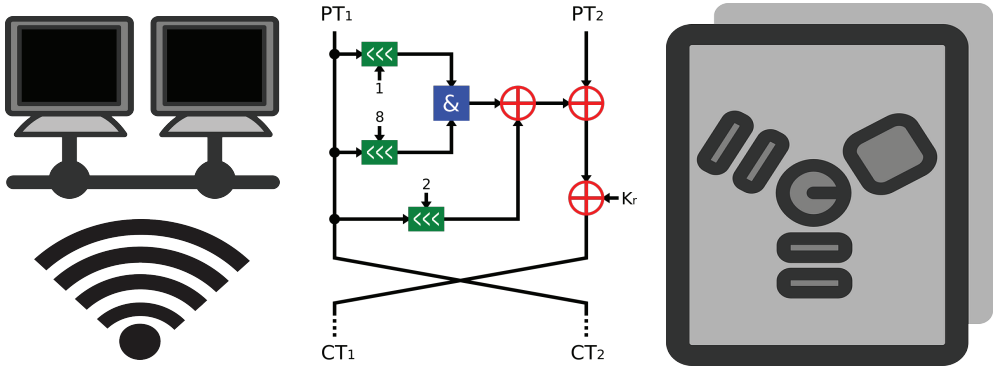
CSE 40567 / 60567: Computer Security



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)

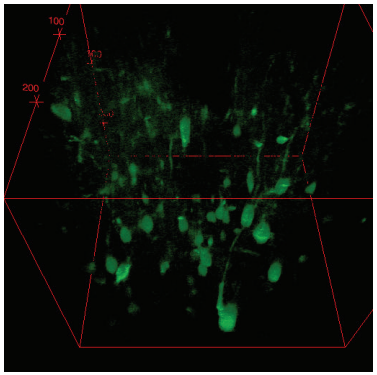
Grad TA

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

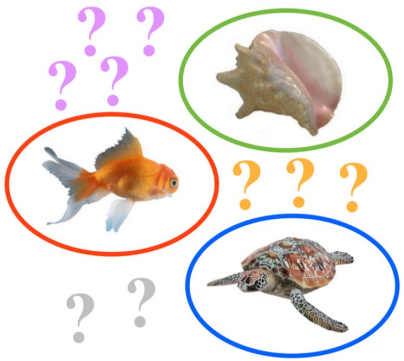
About me

- Joined Notre Dame Summer 2015
  - Ph.D. from the University of Colorado 2009
  - 2007 — 2012 **Security Startup Securics, Inc.**
  - 2012 — 2015 Harvard University Center for Brain Science
- Research in Computer Vision and Machine Learning

Reverse engineering biological vision



Tools for Neuroscience



Statistical methods for visual recognition

Digital Humanities

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

Component	Points
Participation Participation in class, film response, office hours, and slack chats.	100
Homeworks Homework assignments.	8 × 125
Midterm Exam Covering the first half of the course.	400
Final Exam Covering the second half of the course.	500
Total	**2000**

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

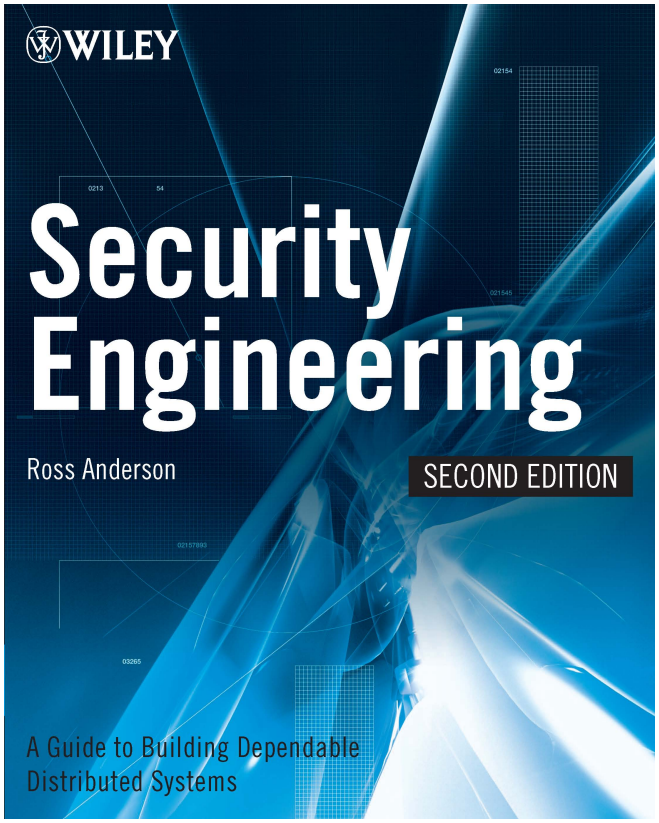
RC Johnson from PayPal on Keeping Your Money Safe from Hackers

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

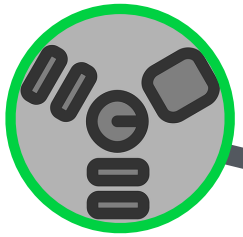
Course Objectives

- 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)



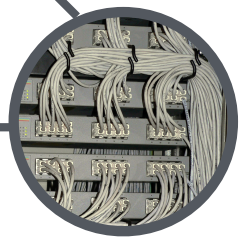
The Web

(weeks 15 & 16)

3 Core Areas

(weeks 3 - 6)

(weeks 6 - 10)



(weeks 11 - 15)

What is this course all about?

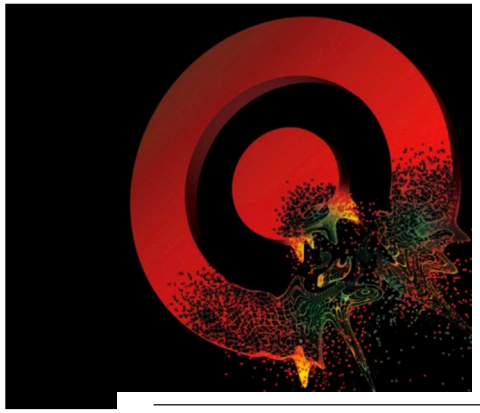
BloombergBusiness | News | Markets | Insights | Video

Features

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack | March 13, 2014

SEND TO kindle



KIM ZETTER SECURITY 12.03.14 4:02 PM

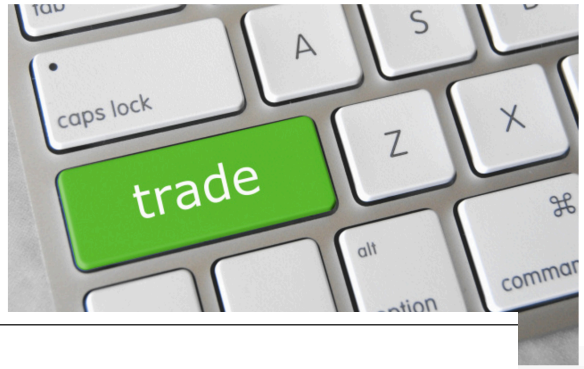
SONY GOT HACKED HARD: WHAT WE KNOW AND DON'T KNOW SO FAR

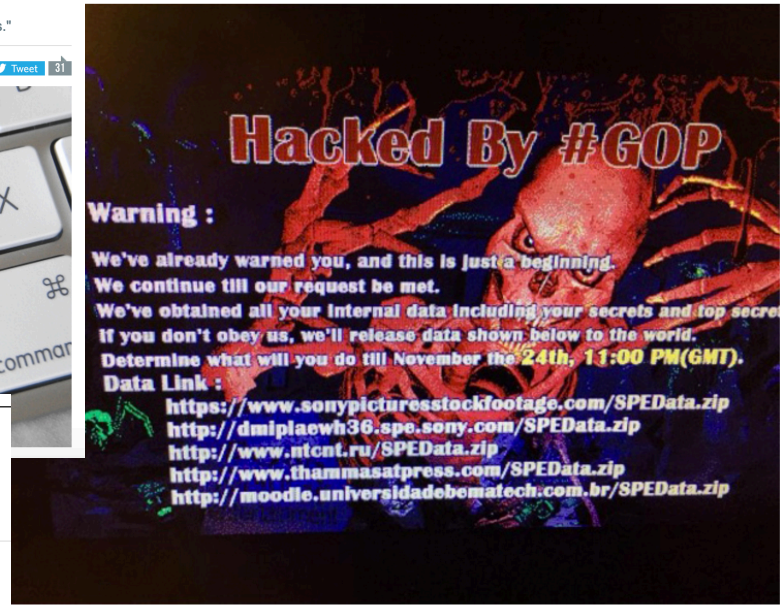
WikiLeaks drops new set of secret TISA docs: Yep, no one agrees

US: Any party can "undertake any action" to protect "essential security interests."

by Cyrus Farivar - Jul 2, 2015 1:53pm EDT

Share Tweet 31





The Opinion Pages | EDITORIAL

Edward Snowden, Whistle-Blower

By THE EDITORIAL BOARD JAN. 1, 2014

Email
Share
Tweet
Save

Seven months ago, the world began to learn the vast scope of the National Security Agency's reach into the lives of hundreds of millions of people in the United States and around the globe, as it collects information about their phone calls, their email messages, their friends and contacts, how they spend their days and where they spend their nights. The public learned in great detail how the agency has exceeded its mandate and abused its authority, prompting outrage at kitchen tables and at the des of Congress, which may finally begin to limit these practices.

Cyber-Safe

JPMorgan's accused hackers had vast $100 million operation

Recommend 1.7k

By Jose Pagliery @Jose_Pagliery

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…

M. Riley et al. “Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It,” Bloomberg Business, March 13th, 2014

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

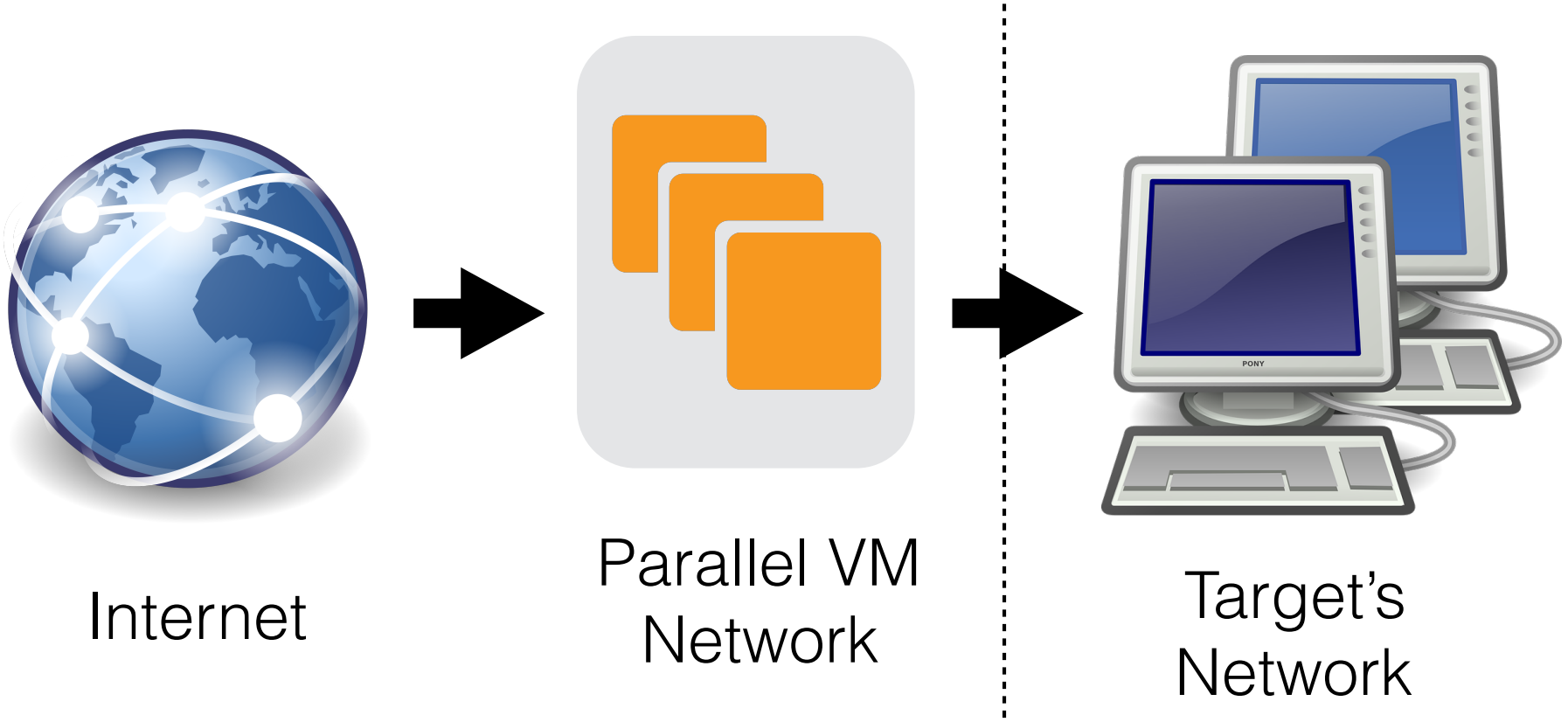
4. On Dec. 2nd, CC numbers started flowing out of POS terminals; Target's IDS detects the attack

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?

FireEye™



Where was the incident response?

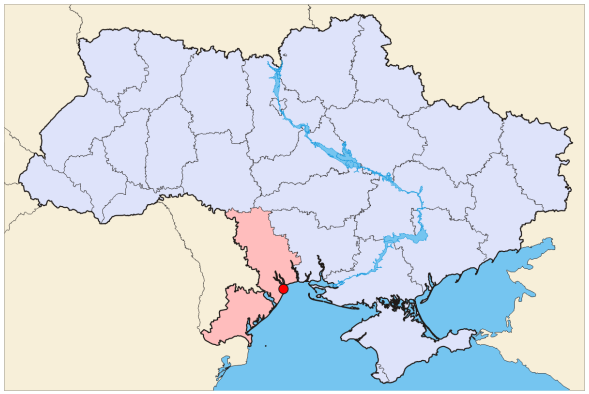
- Incident alert triggered on Nov. 30th by FireEye
- As attackers installed software, additional alerts were generated at the “urgent” level
- FireEye’s platform can automatically stop attacks after they are detected
  - ✳ This feature was disabled by Target
    - ▸ **Such an action is not uncommon**

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

Quiksilver, Reuters, Chase, JP Morgan Chase building New York

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

J. Silver-Greenberg et al. "JPMorgan Chase Hacking Affects 76 Million Households," New York Times, Oct. 2, 2014.

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

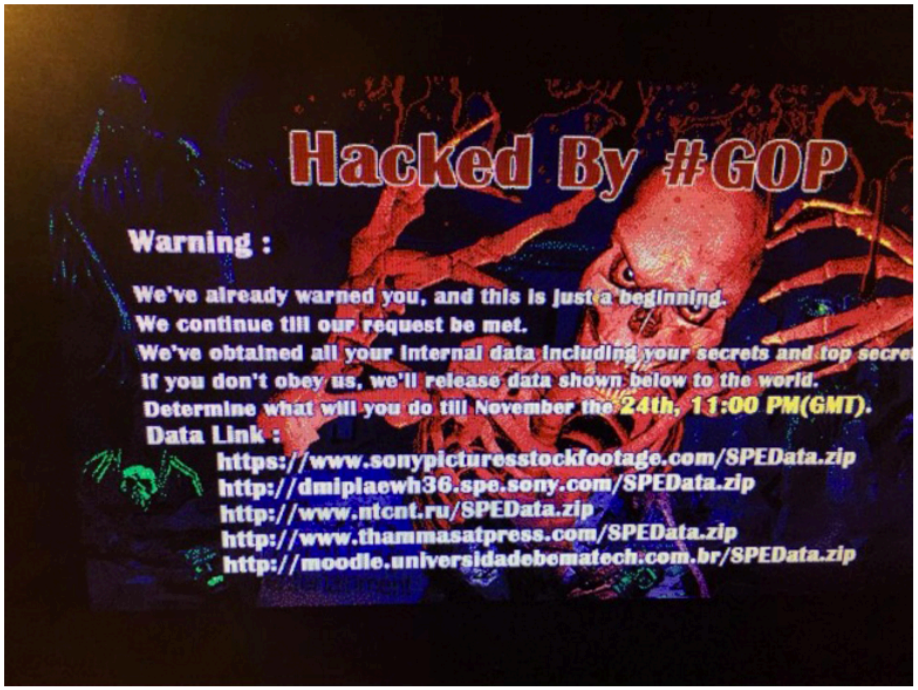
>
>> On Oct 21, 2014, at 1:18 PM, RM wrote:
>>
>> Dear Amy,
>> Hello, how are you? I hope you are well- its been a very long time!
>> I'm writing because I wanted to ask you about the Dragon Tattoo
>> sequels. Logic tells me they are not ever happening- as it's been
>> almost 3 years since it came out. But I had still been holding out a
>> little bit of hope. I know there had been talks to do some sort of TV
>> version without me. People still ask me about it ALL the time. And I
>> never know quite what to say. So I guess I just wanted to ask you so I
>> could know for myself and so that I can let it go for good if that's
>> the case. It's obviously a character and an experience I hold very
>> close.
>>
>> Hope you're doing really well.
>>
>> Xo
>> Sincerely,
>> Rooney

- "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

M. Seal, "An exclusive look at Sony's hacking saga," Vanity Fair, Feb. 2015

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

Image credit: Sony Pictures Entertainment

US Response: additional sanctions enacted against North Korea

J. Kiss, "Sony hack: sacked employees could be to blame, researchers claim," The Guardian, Dec. 2014

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

John Podesta in 2010

Internet of Things Powered Distributed Denial of Service Attacks: 2016

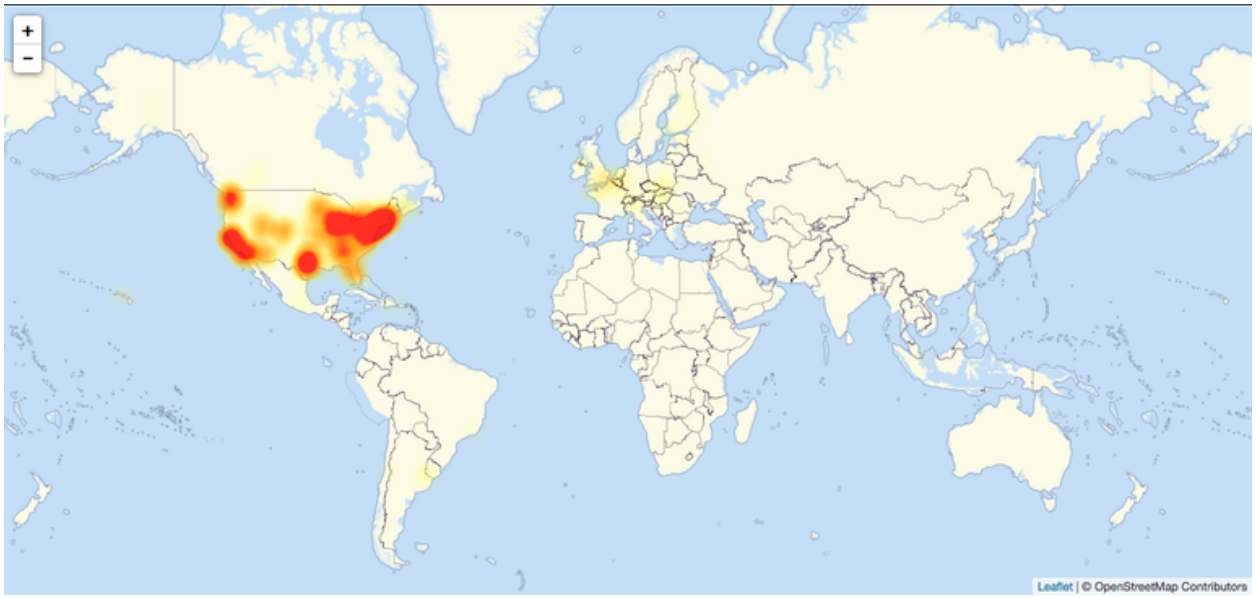
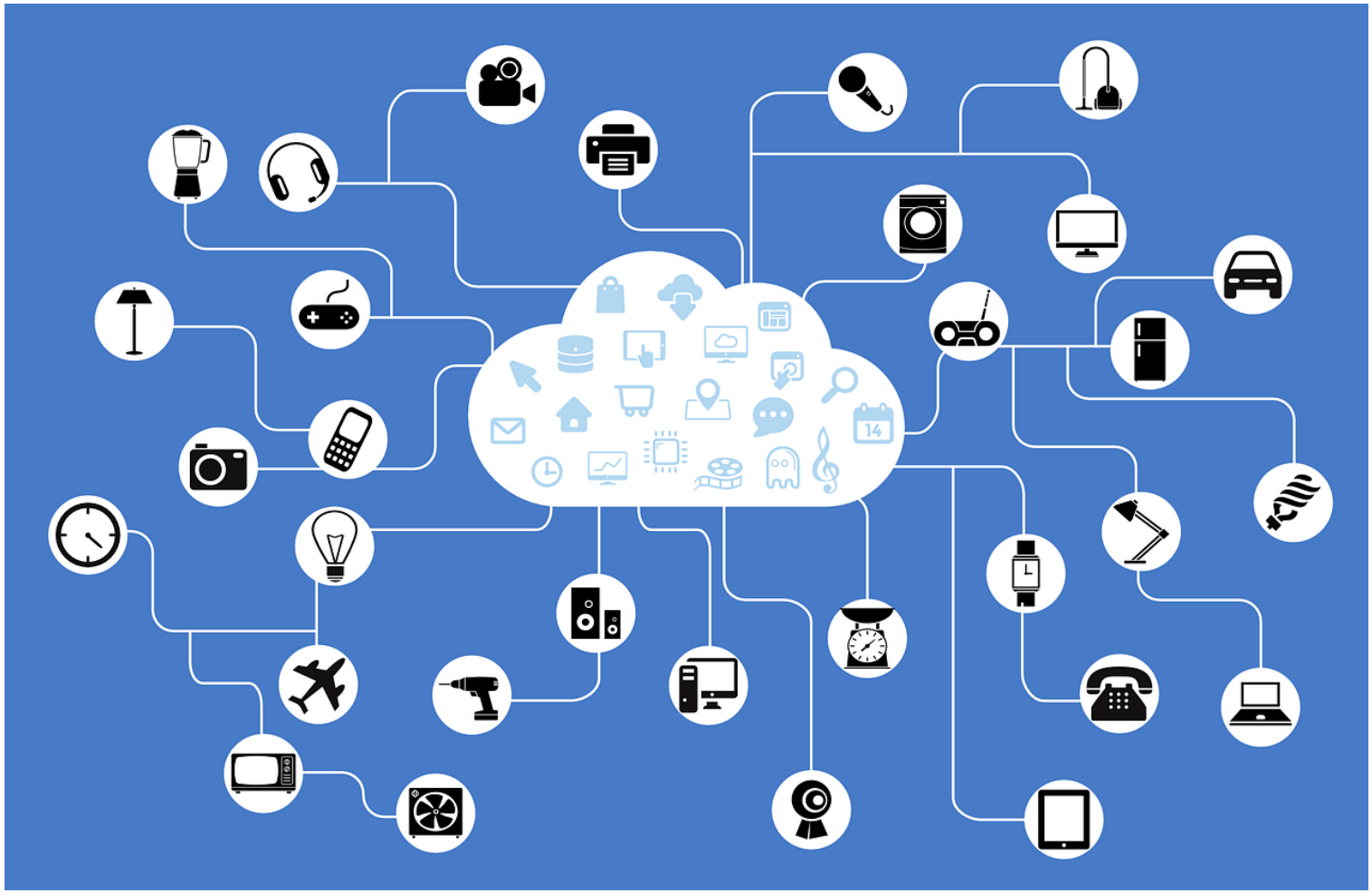


Image credit: downdetector.com

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

Sites affected: Twitter, Netflix, Spotify, Airbnb, Reddit, Etsy, SoundCloud, GitHub,The New York Times.

Threat Frontier: IoT



- 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

Credit Score

Attack Vector: Web Exploit

Apache Struts Flaw
(CVE-2017-5638)

Patch for vulnerability was released on March 7th, 2017

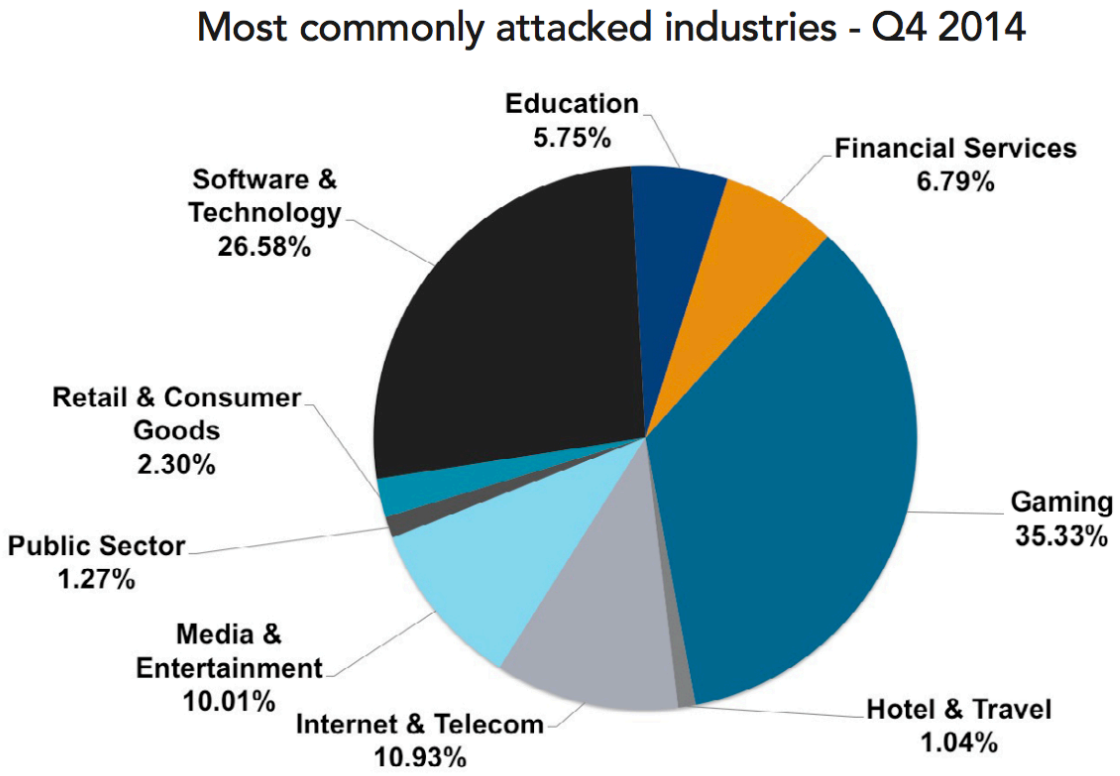
Data breach occurs May - July 2017

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

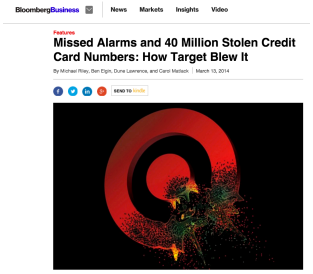
Global DDoS attacks grew 90% from Q4 2013 to 2014



Source: Akamai's [state of the internet] / security, 2014

Is security getting better or worse?

Worse: More attacks



. . .

Better: Improved technologies and practices

LibreSSL

OpenBSD

PKI

NaCl: Networking and Cryptography library

SNORT®

Academic vs. practical security

Grand Canyon National Park: Yaki Point After Sunset

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

C. E. Shannon. Communication theory of secrecy systems. Bell System Technical Journal, 28(4):656–715, October 1949.

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

Shafi Goldwasser and Silvio Micali. Probabilistic encryption. Journal of Computer and System Sciences, 28(2):270–299, 1984.

“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

B. Schneier, "Is cryptography engineering or science?" Schneier on Security, 2013

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