

CS165 – Computer Security

Introduction

Sep 23, 2021

Outline

2

- Welcome!
- Goals of this course
 - ▣ Get to know computer security
 - ▣ Master a subset of critical skills in security
- Introduction of the class
- Exercises
- Grading


Self intro



3

- Zhiyun Qian, CSE Prof.
- Email: zhiyunq@cs.ucr.edu
- iLearn used for announcements and materials
- Piazza for forum discussions
- Course webpage:
<https://www.cs.ucr.edu/~zhiyunq/teaching/cs165/>
- Office: Zoomland
- Office Hours: 3 to 4pm Tuesdays (Tentative) or by appointment
- TA: Guoren Li, 12 to 2pm Wednesdays


My work - Vulnerable Firewall

4


 **Check Point**
SOFTWARE TECHNOLOGIES LTD.



Global Sites  | My Account 

Home | Products & Services | Buy | **Support** | About Us

 [Support Center](#) > [Search Results](#) > SecureKnowledge Details

Support Center



 Print  Email

Check Point response to "Off-Path TCP Sequence Number Inference Attack"

Solution ID: sk74640
Severity: **Low**
Product: Security Gateway
Version: All
Date Created: 24-May-2012
Last Modified: 14-Mar-2013

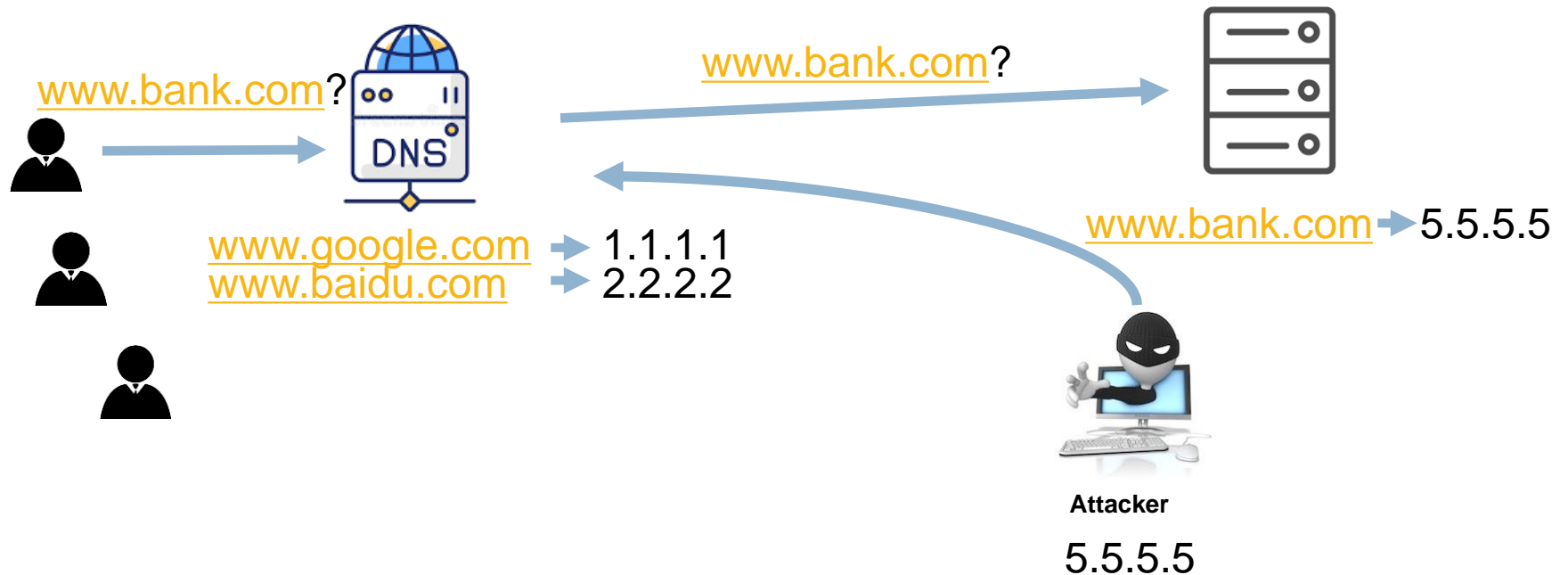
Rate this document
☆☆☆☆☆ [1=Worst,5=Best]

SYMPTOMS

- Researchers at the University of Michigan have published a paper ["Off-Path TCP Sequence Number Inference Attack How Firewall Middleboxes Reduce Security"](#).
- This attack identifies the current sequence range of a TCP connection, by exploiting the fact that firewalls drop out-of-window TCP packets. After the sequence range is identified, an off-path attacker may inject data or hijack the TCP connection.
- Client applications that use cleartext connections (e.g., HTTP and not HTTPS) are potential targets for these attacks.

My work – DNS cache poisoning

5



My work – TCP remote hijack

6

CVE-2016-5969



Client



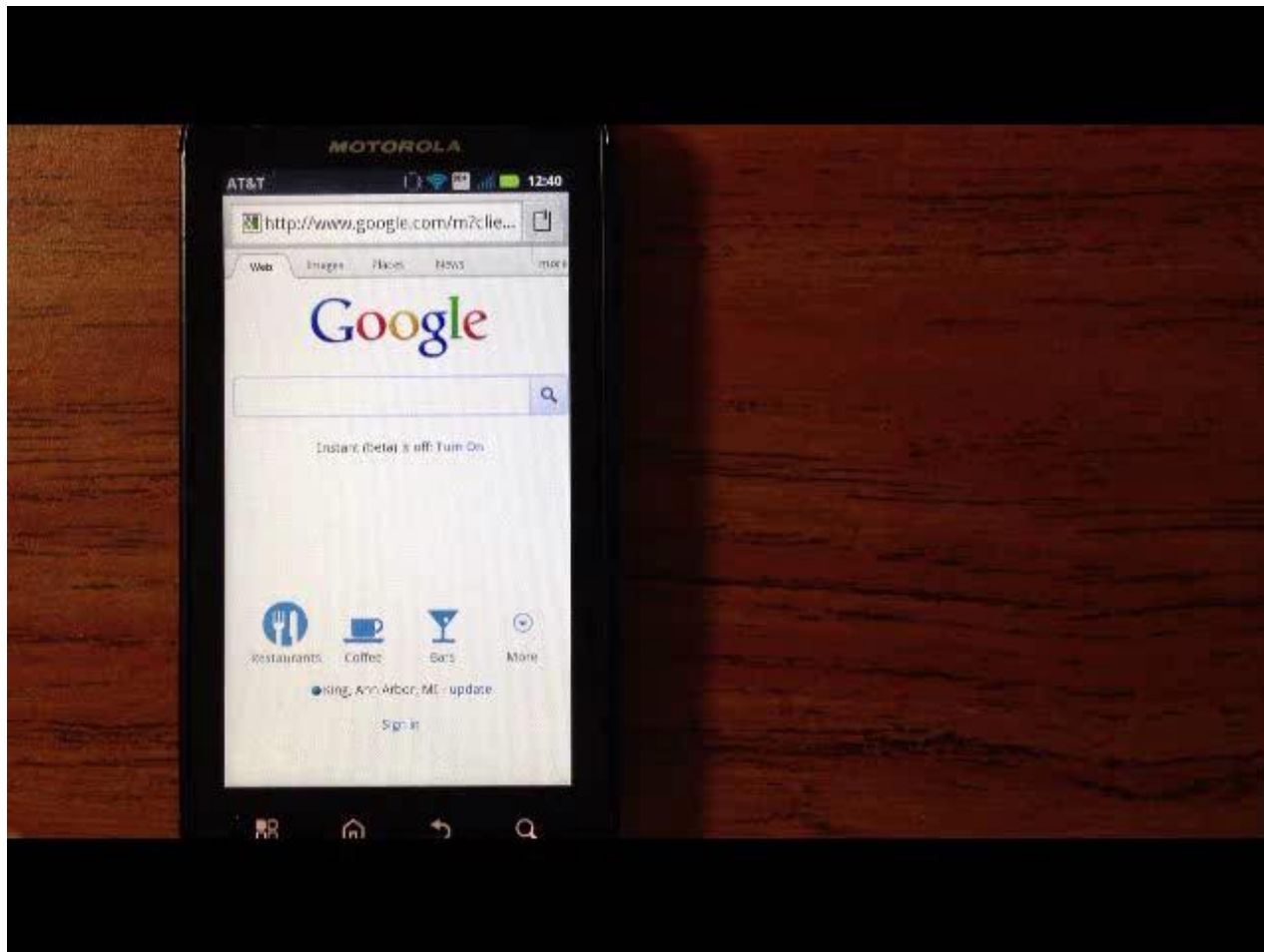
Server



Attacker

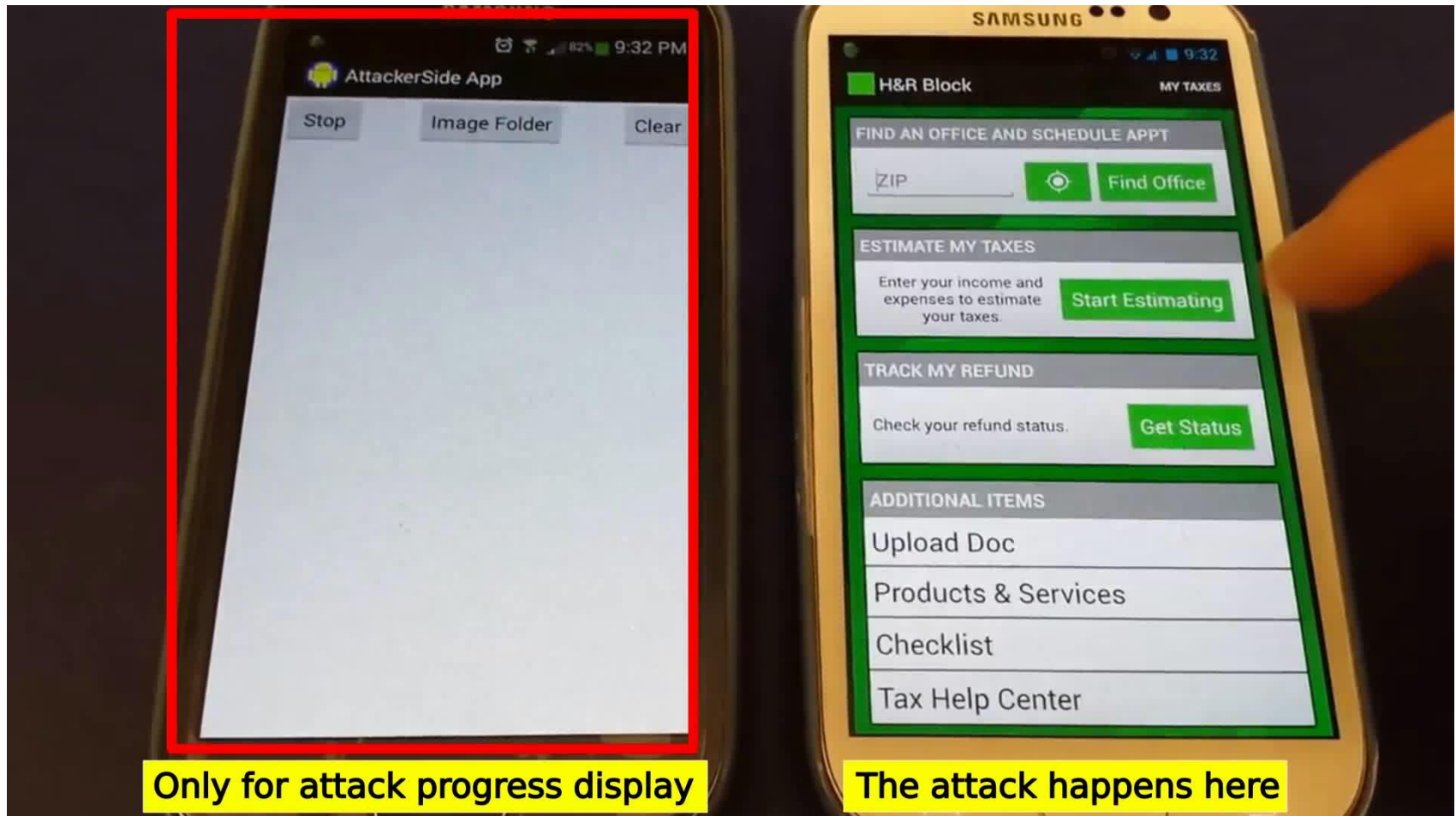
My work – TCP remote hijack

7



My work – App hijacking

8



Goals of this course

9

□ Le

□

□ Ga

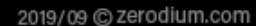
□

ZERODIUM Payouts for Desktops/Servers*										
<div>Up to \$1,000,000</div> <div>Up to \$500,000</div> <div>Up to \$250,000</div> <div>Up to \$200,000</div> <div>Up to \$100,000</div> <div>Up to \$80,000</div> <div>Up to \$50,000</div> <div>Up to \$10,000</div>										
<div>Windows</div> <div>macOS</div> <div>Linux/BSD</div> <div>Any OS</div> <div>RCE: Remote Code Execution</div> <div>LPE: Local Privilege Escalation</div> <div>SBX: Sandbox Escape or Bypass</div> <div>VME: Virtual Machine Escape</div>										
<div>1.001</div> <div>Win RCE</div> <div>Zero Click</div> <div>Win</div>										
<div>3.001</div> <div>Chrome</div> <div>RCE+LPE</div> <div>Win</div>										
<div>2.001</div> <div>Apache</div> <div>RCE</div> <div>Linux</div>										
<div>2.002</div> <div>MS IIS</div> <div>RCE</div> <div>Win</div>										
<div>5.001</div> <div>MS Outlook</div> <div>RCE</div> <div>Win</div>										
<div>4.001</div> <div>MS Exchange</div> <div>RCE</div> <div>Win</div>										
<div>2.003</div> <div>OpenSSL</div> <div>RCE</div> <div>Linux</div>										
<div>2.004</div> <div>PHP</div> <div>RCE</div> <div>Linux</div>										
<div>6.001</div> <div>VMware ESXi</div> <div>VME</div> <div>Win/Linux</div>										
<div>5.002</div> <div>Thunderbird</div> <div>RCE</div> <div>Win/Linux</div>										
<div>4.002</div> <div>Sendmail</div> <div>RCE</div> <div>Linux</div>										
<div>4.003</div> <div>Postfix</div> <div>RCE</div> <div>Linux</div>										
<div>4.004</div> <div>Dovecot</div> <div>RCE</div> <div>Linux</div>										
<div>4.005</div> <div>Exim</div> <div>RCE</div> <div>Linux</div>										
<div>2.005</div> <div>nginx</div> <div>RCE</div> <div>Linux</div>										
<div>3.002</div> <div>Safari</div> <div>RCE+LPE</div> <div>Mac</div>										
<div>3.003</div> <div>Edge</div> <div>RCE+LPE</div> <div>Win</div>										
<div>3.004</div> <div>Firefox</div> <div>RCE+LPE</div> <div>Win</div>										
<div>5.003</div> <div>Word/Excel</div> <div>RCE</div> <div>Win</div>										
<div>7.001</div> <div>WordPress</div> <div>RCE</div> <div>Linux</div>										
<div>7.002</div> <div>cPanel/WHM</div> <div>RCE</div> <div>Linux</div>										
<div>7.003</div> <div>Plesk</div> <div>RCE</div> <div>Linux</div>										
<div>7.004</div> <div>Webmin</div> <div>RCE</div> <div>Linux</div>										
<div>6.002</div> <div>VMware WS</div> <div>VME</div> <div>Win/Linux</div>										
<div>5.004</div> <div>Adobe PDF</div> <div>RCE+SBX</div> <div>Win</div>										
<div>5.005</div> <div>WinRAR</div> <div>RCE</div> <div>Win</div>										
<div>5.006</div> <div>7-Zip</div> <div>RCE</div> <div>Win</div>										
<div>6.003</div> <div>Windows</div> <div>LPE/SBX</div> <div>Win</div>										
<div>6.004</div> <div>USB</div> <div>LPE</div> <div>Win/Mac</div>										
<div>8.001</div> <div>Antivirus</div> <div>RCE</div> <div>Win</div>										
<div>5.007</div> <div>WinZip</div> <div>RCE</div> <div>Win</div>										
<div>5.008</div> <div>tar</div> <div>RCE</div> <div>Linux</div>										
<div>6.005</div> <div>macOS</div> <div>LPE/SBX</div> <div>Mac</div>										
<div>6.006</div> <div>Linux</div> <div>LPE</div> <div>Linux</div>										
<div>6.007</div> <div>BSD</div> <div>LPE</div> <div>BSD</div>										
<div>9.001</div> <div>Routers</div> <div>RCE</div> <div>Win</div>										
<div>8.002</div> <div>Antivirus</div> <div>LPE</div> <div>Win</div>										
<div>7.005</div> <div>phpBB</div> <div>RCE</div> <div>Linux</div>										
<div>7.006</div> <div>vBulletin</div> <div>RCE</div> <div>Linux</div>										
<div>7.007</div> <div>MyBB</div> <div>RCE</div> <div>Linux</div>										
<div>7.008</div> <div>Joomla</div> <div>RCE</div> <div>Linux</div>										
<div>7.009</div> <div>Drupal</div> <div>RCE</div> <div>Linux</div>										
<div>7.010</div> <div>Roundcube</div> <div>RCE</div> <div>Linux</div>										
<div>7.011</div> <div>Horde</div> <div>RCE</div> <div>Linux</div>										

* All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.

2019/01 © zerodium.com

10



Goals of this course

11

- Learn the principles of computer security
 - ▣ Generally a diverse area and domain-specific
- Gain hands-on experience (not just theory)
 - ▣ Learn to break things
 - \$2M bounty for remote jailbreak!
 - ▣ and secure systems
 - Write secure code, configure systems securely
 - Analyze a system critically for weaknesses

Goals of this course

12

- From the class projects, you'll learn to:
 - ▣ Crack passwords
 - ▣ Crack real-world applications
 - ▣ Perform memory-corruption attacks
- Of course, how to avoid these

Getting an A

13

- This class requires knowledge of computer organization, operating system, networking
 - ▣ CS61, CS161, CS153, CS164 (a little bit)
- And also a mature understanding of software and systems in general

Outline

14

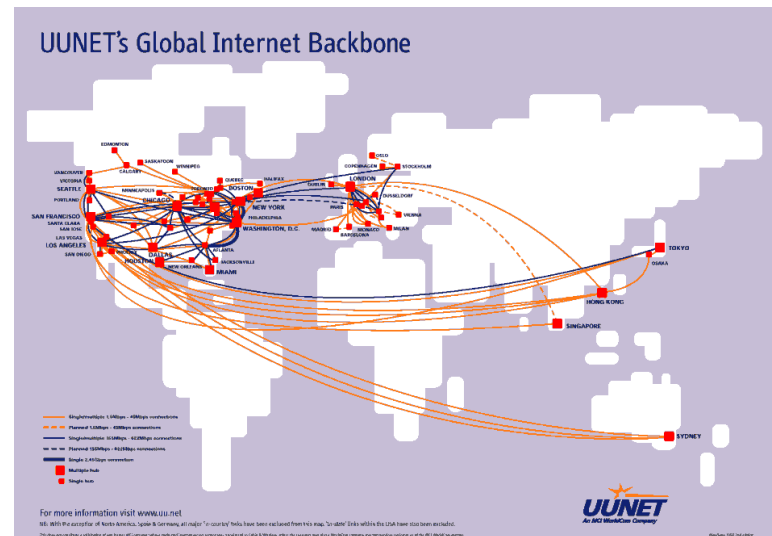
- Welcome!
- Goals of this course
- Introduction of the class
- Exercises
- Grading

15



Network

16



Physical
Sensing



Object
Domain



Actuation
Information



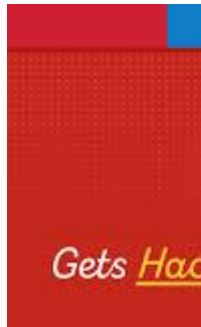


HOW **SAFE** IS YOUR
COMPUTER?

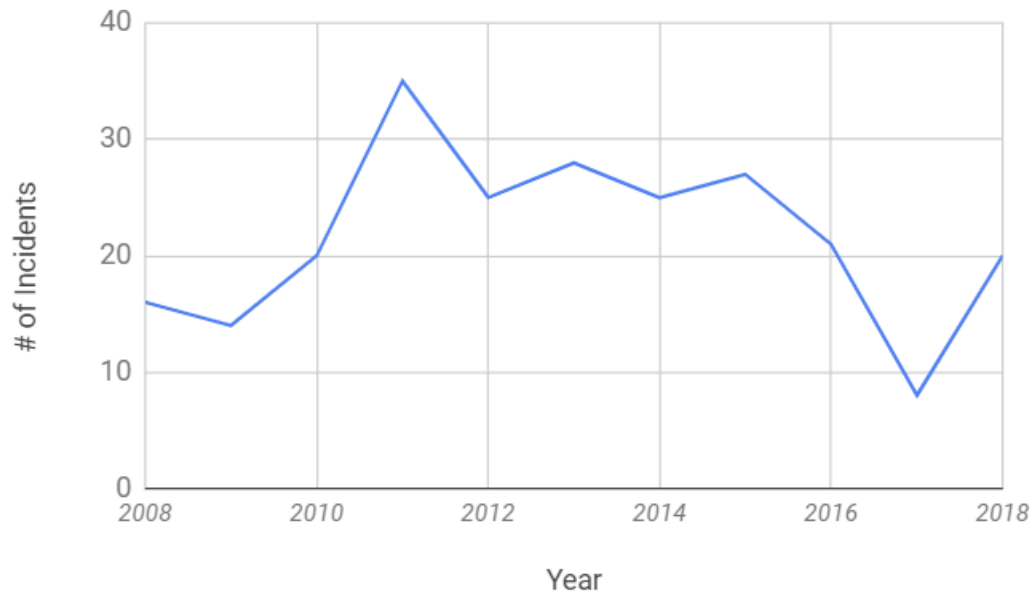


Recent news

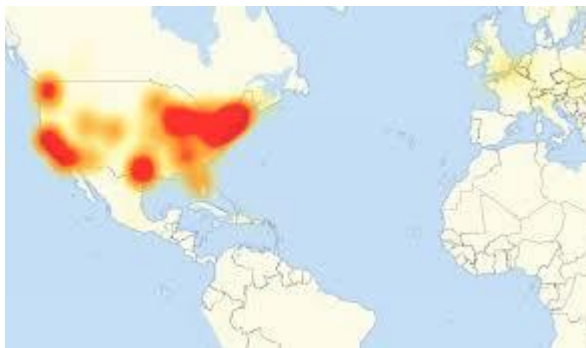
19



Google plu:



M accounts



Dyn DDoS attack



Insider threats

What is security about?

20



Security and security mindset

21

- “The study of how a system behaves under adversarial actions”
 - ▣ Intelligent attackers actively trying to lead the system to misbehave or do unexpected things

□ Security vs. System
II

□ Corner cases vs. Common case

Play Games vs. Security Games

22

- Both deal with a set of man-made rules!
- Man-made rules have bugs (which can be exploited)!
 - ▣ Think about tax systems...
 - ▣ Warren Buffett's tax rate is lower than his secretary's
 - 17.3% on \$39.8 million taxable income
 - Heck, it's much lower than my tax rate
 - ▣ The more complex, the more dangerous

Play Games vs. Security Games

23



Thinking like an attacker

24

- Analyze game rules with different goals (threats)
 - ▣ Break in to a door? Steal? Fake identity?
- Think outside the box
 - ▣ Side channel attacks (e.g., steal crypto keys)
- Challenge security assumptions
 - ▣ E.g., Physical access to a system
- One successful attack exploiting a vulnerability is good enough!

Thinking like a defender

25

- Discover loopholes in game rules and fix them
 - ▣ With respect to various possible threats (MANY!)
 - ▣ Need to cover all corner cases (HARD!)
 - ▣ Always catch-up
- Design favorable rules
 - ▣ Prevention of bad consequences (also HARD!)
 - ▣ Need to allow legitimate functionalities (e.g., mobile apps)

Goals of defenders

26

Before
attacks
happen

- Risk avoidance
 - Bug discovery and fixing
 - No guarantee, but reduces/minimizes risk
- Deterrence
 - No guarantee. E.g., surveillance
- Prevention
 - By design, bad things cannot happen (e.g., VPN). Do require system change

After
attacks
happen

- Detection
 - Long history! Misuse vs. Anomaly
 - Cat and Mouse
- Recovery
 - Generic is hard. Domain-specific.

Proactive

Reactive

Case study (detection): how people ensure physical security

27

Allow “non-malicious/dangerous” people in →



Case study (detection): how people ensure cyber security

28



AV industry in 1998



AV industry in 2008



Threat model

30

- What resources/ capabilities / motivations the attacker has? What defenses are in place?



VS



Weakness < Vulnerability < Exploit < Attack

Basic Components (CIA) in Security

31

□ Confidentiality

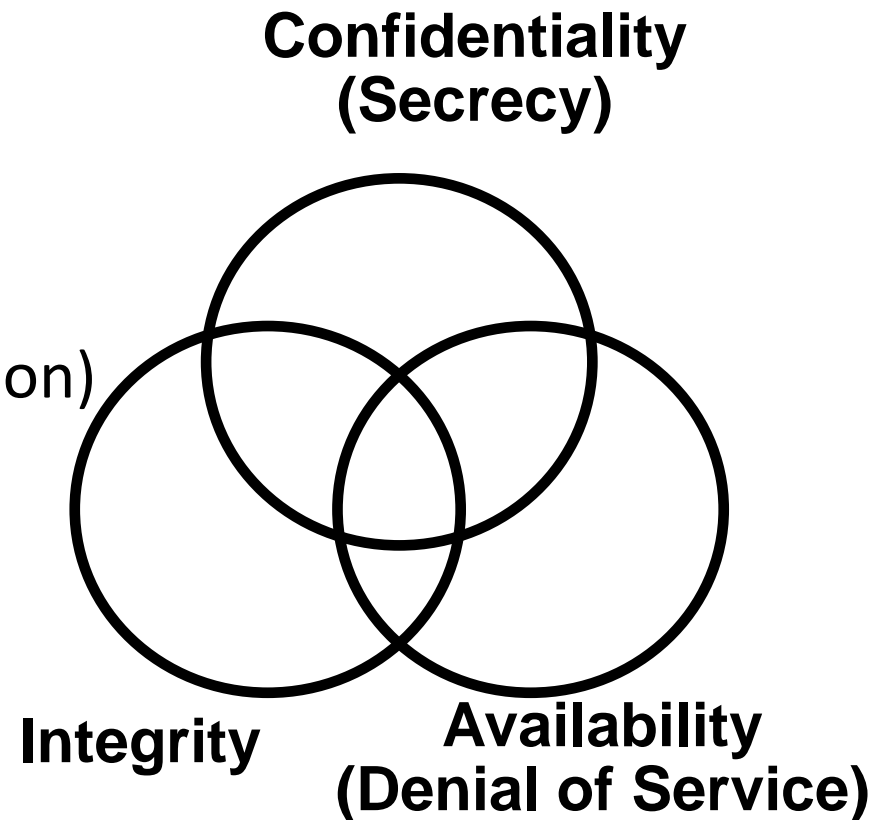
- ▣ Keeping data and resources hidden

□ Integrity

- ▣ Data integrity (integrity)
- ▣ Origin integrity (authentication)

□ Availability

- ▣ Enabling access to data and resources



Topics

32

- ❑ Passwords
- ❑ Software security
- ❑ System security
- ❑ Network security

Not a theory
or
crypto class

Outline

33

- Welcome!
- Goals of this course
- Introduction of the class
- Exercises
- Grading

Thinking like an attacker

34

- Exercise: How to steal my password?
- Under what threat model / assumptions?

Thinking like a defender

36

- Exercise: How to protect your PIN at ATMs?

(With respect to what threats?)

Thinking like a defender

37

- Exercise: How to raise security at airport checkpoint?

Outline

38

- Welcome!
- Goals of this course
- Introduction of the class
- Exercises
- Grading

Textbooks and Lecture Notes

39

- Recommended (NOT required) textbooks
 - ▣ Computer Systems: A Programmer's Perspective, Randal E. Bryant and David R. O'Hallaron.
 - Assembly instruction. Hardware-software interface.
 - ▣ Computer Security: Principles and Practice (3/E or 4/E), by William Stallings and Lawrie Brown
 - *An in-depth book. You may read and consult portions of it only.*
 - ▣ Hacking: The Art of Exploitation (2nd Edition), by Jon Erickson
 - *Useful for projects and understanding attacks.*
- Lecture notes and additional materials
 - ▣ see ilearn

Grading

40

- 4 Projects : 35%
- 2 homeworks: 20%
- 1 midterm: 15%
- 1 final: 25%
- Participation: 5%
 - ▣ Questions, answering others' questions, forum activities, intellectual contribution

4 Projects --- 35% (+bonus points)

41

- Password cracking: 5%
- Reverse engineering: 11%
- Buffer overflow: 11%
- Static analysis: 8%

- Interesting and time-consuming!
 - ▣ You most likely won't be able to finish them in the last few days!
 - ▣ Requires good understanding of low level details (machine instructions)

- Work in a group of two

Late policy

42

- 4 slack days for homework or project (combined)
- 2% bonus points if you do not use any
 - ▣ All or nothing

Law and Ethics

43

- Respect others' privacy and rights
- Federal and state laws criminalize computer intrusion and wiretapping
 - ▣ e.g. Computer Fraud and Abuse Act (CFAA), Electronic Communications Privacy Act (ECPA)
 - ▣ Legal implications!
- University of California Electronic Communications Policy
 - ▣ You can be expelled
- Do not share your work outside of class!

Questions

44



Computer and Network Security

50

