CS165 – Computer Security

Introduction

Sep 23, 2021

Outline

- 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

- 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

Check Point
SOFTWARE TECHNOLOGIES LTD.

Global Sites | My Account

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

Support Center > Search Results > SecureKnowledge Details

Support Center

Search

Print Email

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

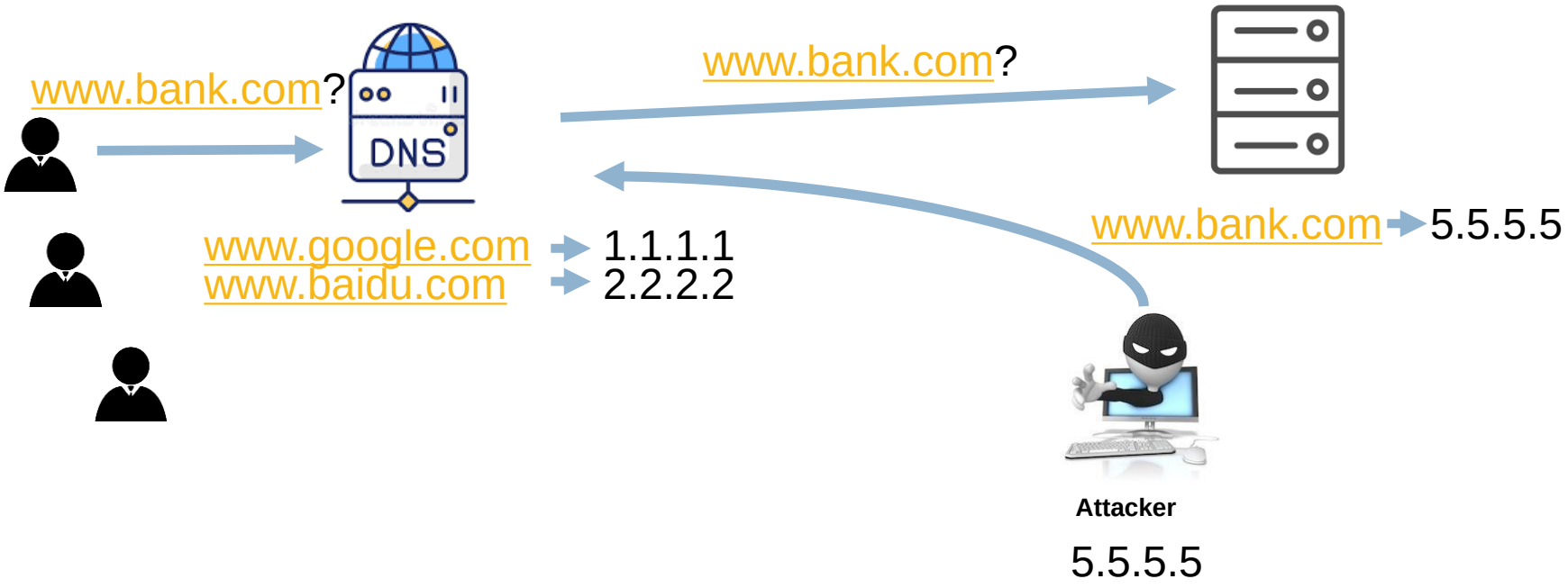
Solution ID: sk74640
Severity: Low
Product: Security Gateway
Version: All
Date Created: 24-May-2012
Last Modified: 14-Mar-2013

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



My work – TCP remote hijack

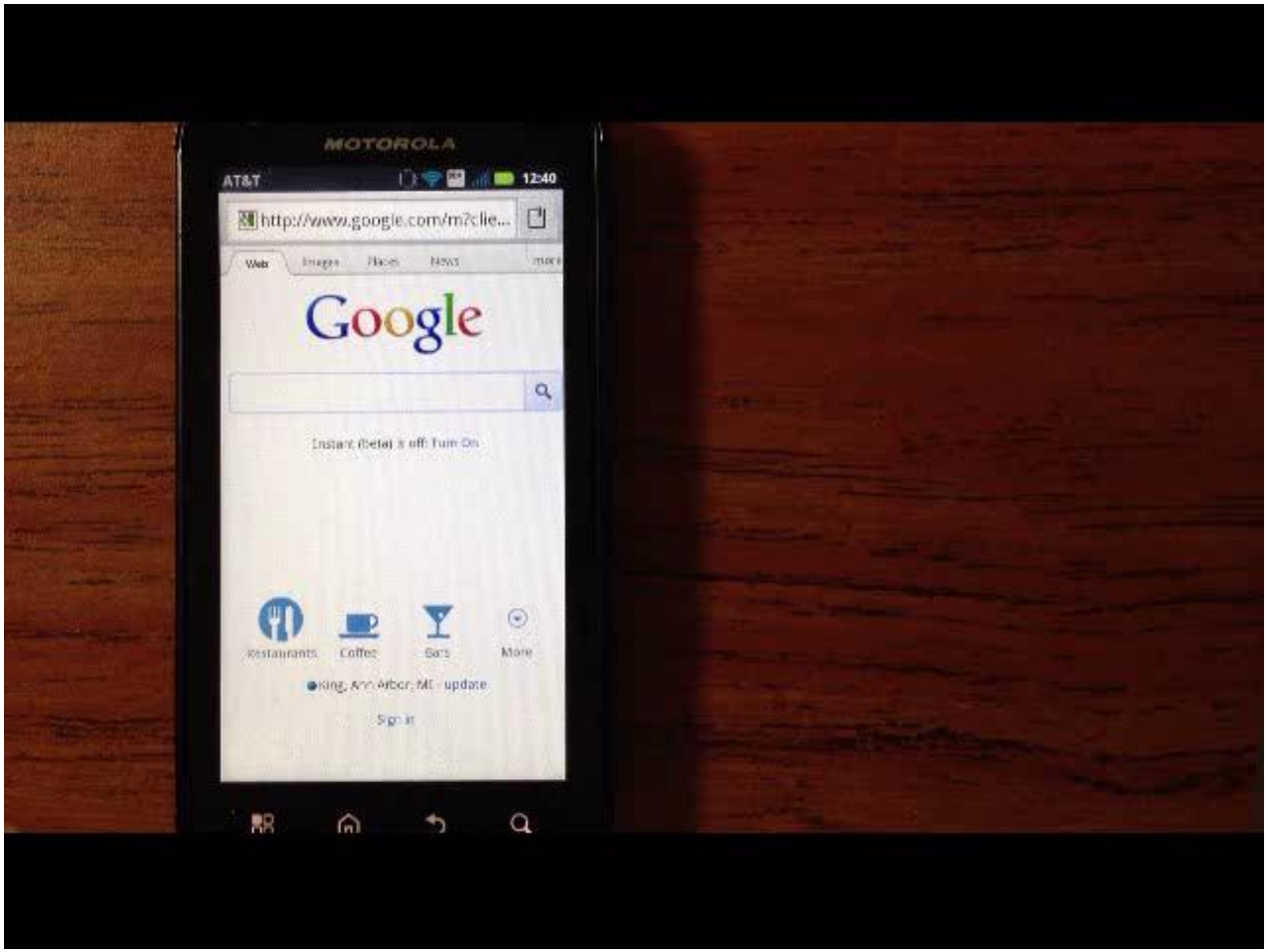
CVE-2016-5969

Client

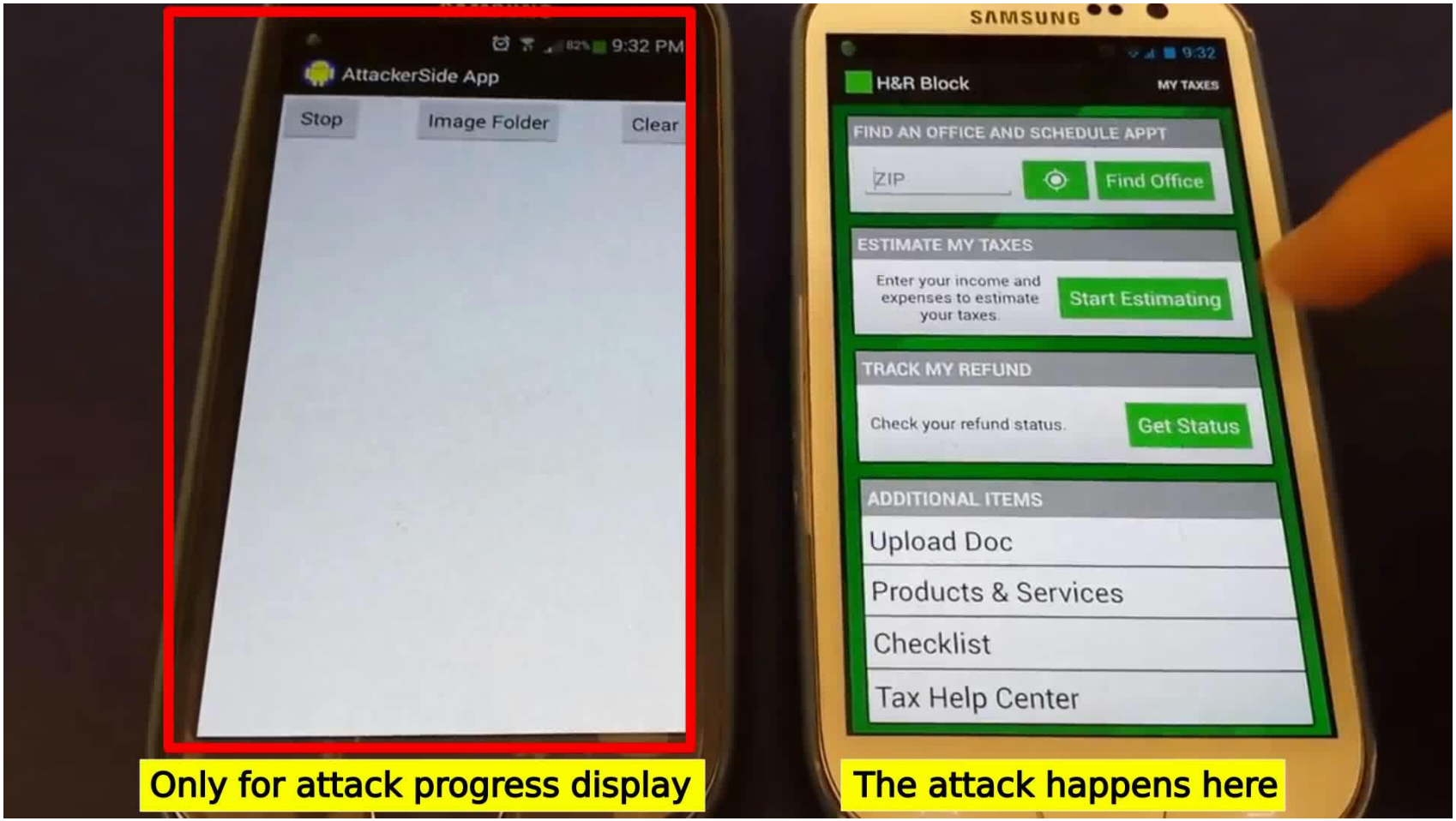
Server

Attacker

My work – TCP remote hijack

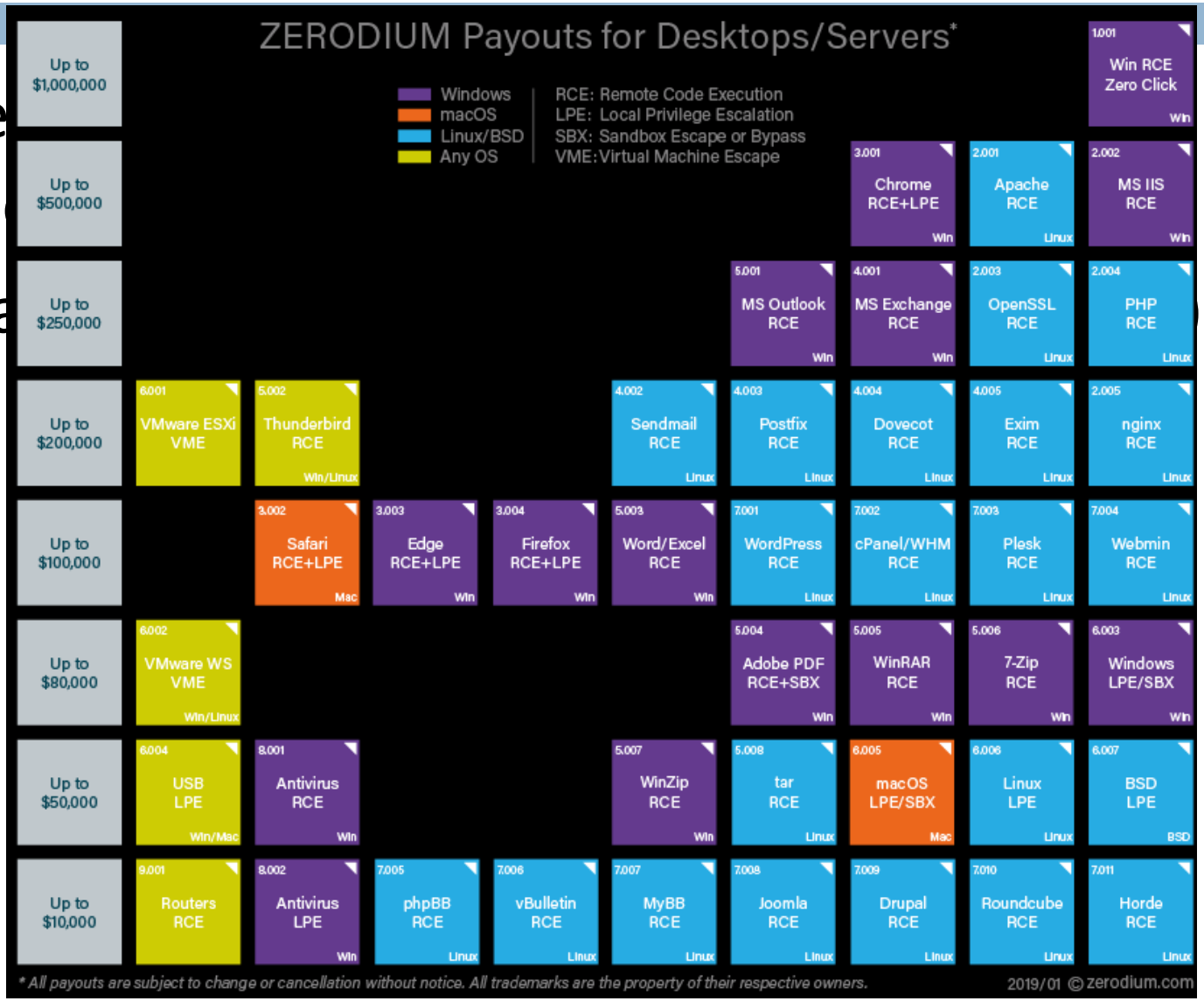


My work – App hijacking

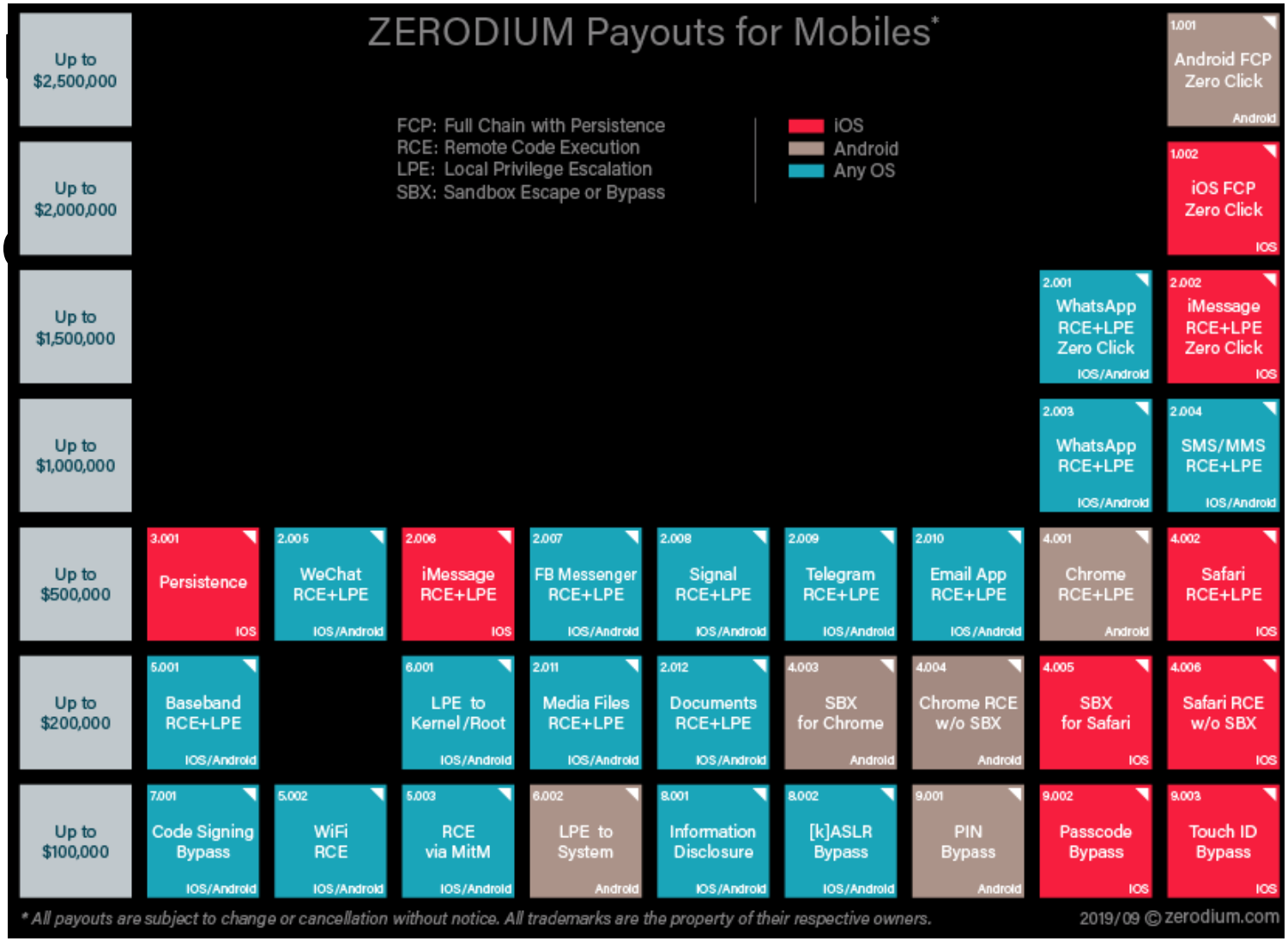


Goals of this course

- Le
  -
- Ga
  -



Goals of this course



Goals of this course

- 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

- 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

- 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

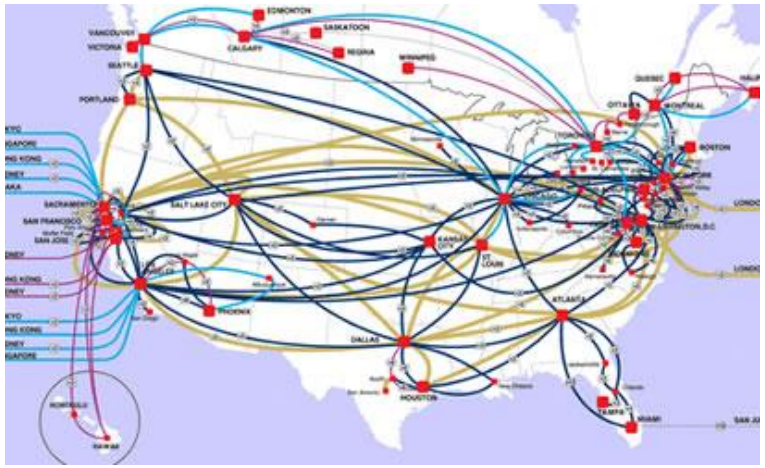
Outline

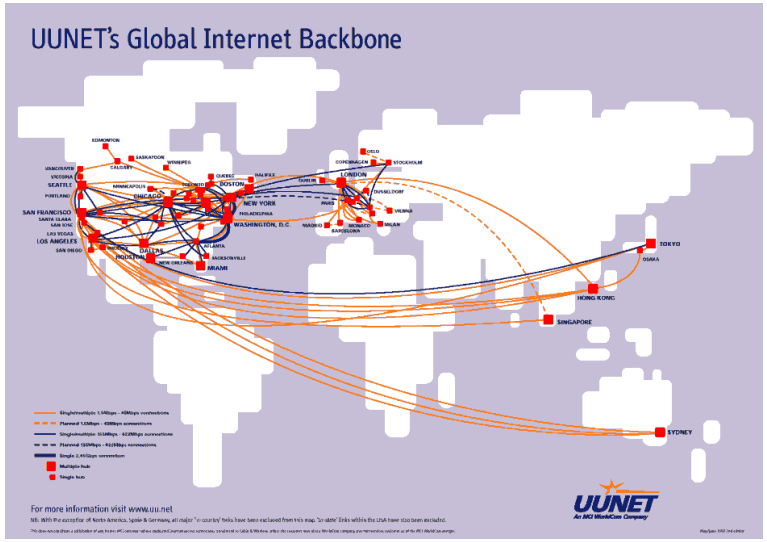
- Welcome!
- Goals of this course
- Introduction of the class
- Exercises
- Grading

Computer

Network

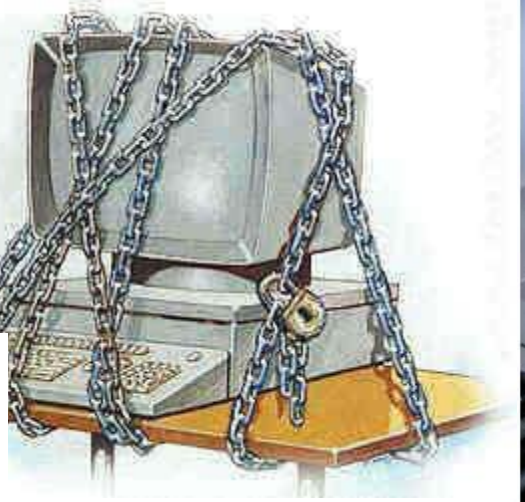

OC192
OC48
OC12
DS3
AT&T




UUNET's Global Internet Backbone
For more information visit www.uu.net
UUNET

/is/labs/lim-lab/image/4.CPS.jpg

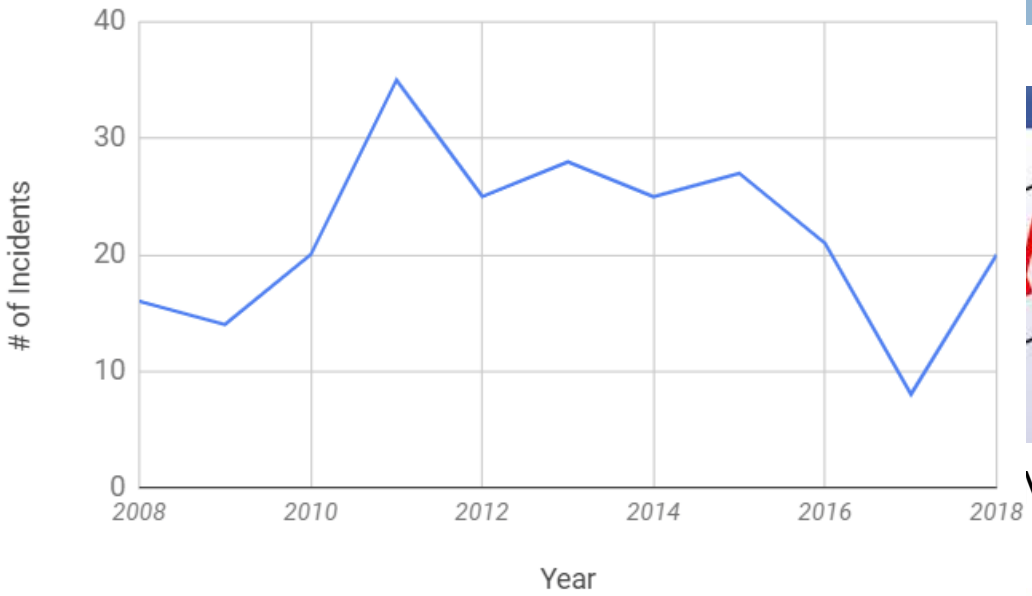

SECURITY
RISK
HOW SAFE IS YOUR
COMPUTER?




IS IT SAFE?

Recent news

Google plu



M accounts

Dyn DDoS attack

Insider threats

What is security about?

Security and security mindset

- "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 II
- Corner cases vs. Common case

Play Games vs. Security Games

- 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

Thinking like an attacker

- 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

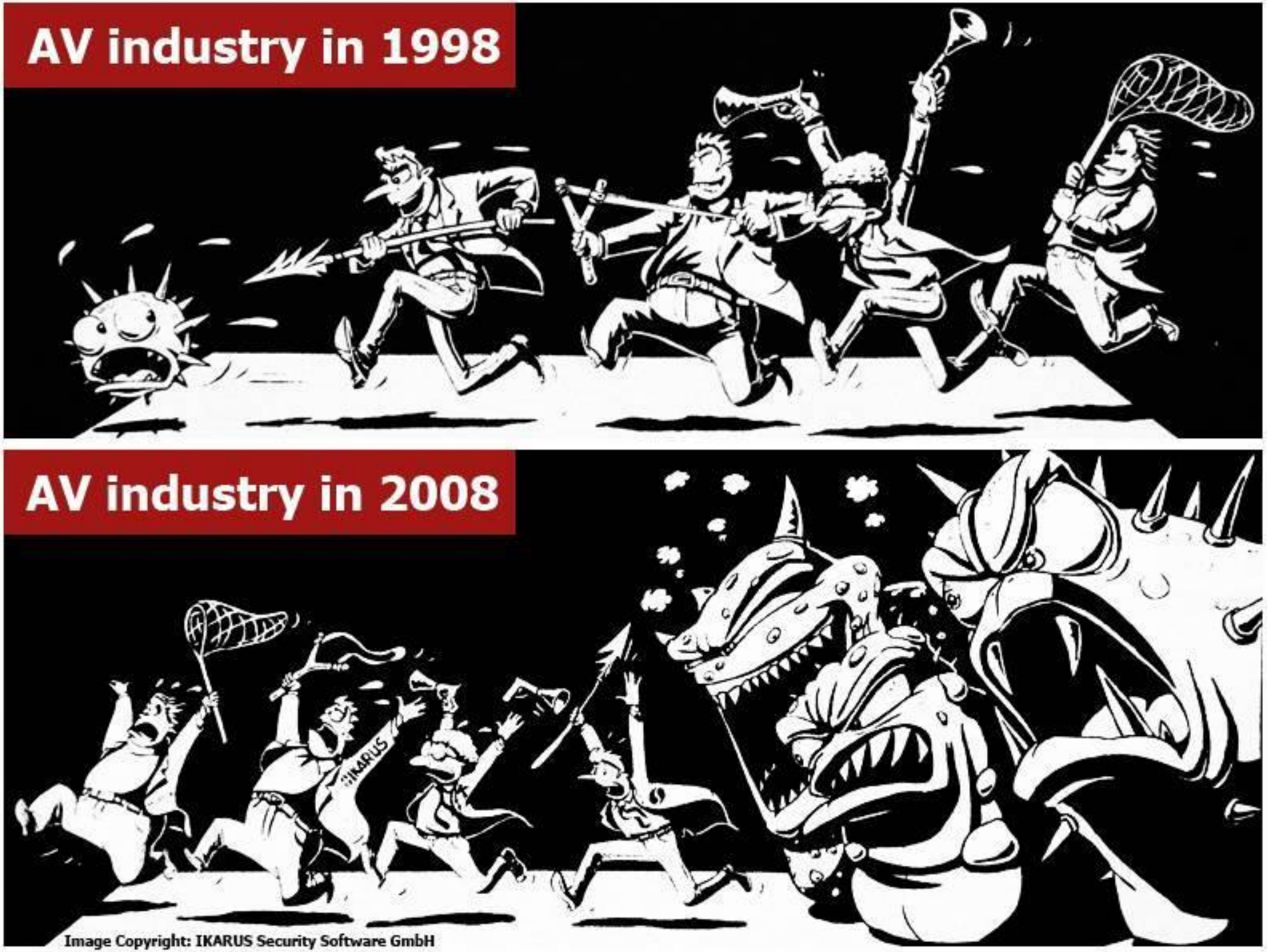
- Discover loopholes in game rules and fix them
  - With respect to various possible threats (MANY!)
  - Need to cover all corner cases (HARD!)
  - Always catch-up
- Design favorable rules
  - Prevention of bad consequences (also HARD!)
  - Need to allow legitimate functionalities (e.g., mobile apps)

Goals of defenders

Case study (detection): how people ensure physical security

Allow “non-malicious/dangerous” people in →

Case study (detection): how people ensure cyber security


AV industry in 1998
AV industry in 2008
IKARUS
Image Copyright: IKARUS Security Software GmbH

Threat model

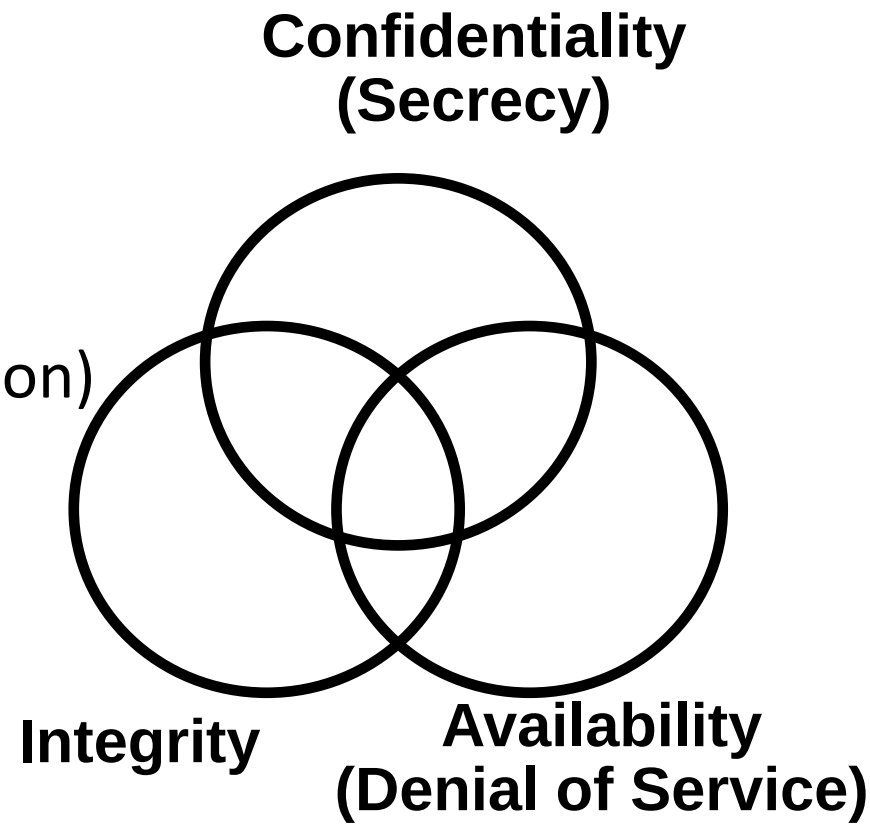
- What resources/ capabilities / motivations the attacker has? What defenses are in place?

VS

Weakness < Vulnerability < Exploit < Attack

Basic Components (CIA) in Security

- Confidentiality
  - Keeping data and resources hidden
- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)
- Availability
  - Enabling access to data and resources



Topics

- Passwords
- Software security
- System security
- Network security

Not a theory
or
crypto class

Outline

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

Thinking like an attacker

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

Thinking like a defender

- Exercise: How to protect your PIN at ATMs?

(With respect to what threats?)

Thinking like a defender

- Exercise: How to raise security at airport checkpoint?

Outline

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

Textbooks and Lecture Notes

- 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

- 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)

- 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

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

Law and Ethics

- 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

Computer and Network Security