COMPUTER SECURITY

OVERVIEW OF THE COURSE

Shiqing Ma, Rutgers University

ABOUT THE COURSE

- Instructor: Shiqing Ma
- Email: shiqing.ma AT rutgers.edu
- Location: HLL-114
- Time
  - Wednesday 10:20 - 11:40 AM
  - Friday 3:20 - 4:40 PM
- TA: TBD
- Make sure you have iLab accounts.
- Please send emails starting with "[419]:" in your subject title.
- Website: https://www.cs.rutgers.edu/~sm2283/20sp/

GRADING

- The grade will be based on homework (HW), classroom quiz (QZ), in-class midterm exam (ME), a group project (PR), and in-class final exam (FE), as follows:
- Grade = 30% * HW + 10% * PR + 15% * QZ + 20% * ME + 25% * FE.
- Exams are closed books and closed notes.
- There will be 4 HW, 3 QZ, 1 ME, 1 PR and 1 FE. Numbers of HW and QZ are subject to change.
- HW includes programming assignments. C/C++ and Python will be used.
- QZ will be announced ahead of time.

QUESTIONS?

WE HAVE HEARD SO MUCH ABOUT SECURITY

- Snowden leaks information about various NSA data collection programs
  - Phone call record, email, instant message, etc.
- Facebook CEO’s page hacked by Palestinian Khalil Shreateh to demonstrate bugs in Facebook
- Attacked companies or organizations
  - Sony, Capital One, Google, Facebook, Apple, Microsoft, Yahoo

IT AFFECTS US ALL

- Yahoo! Email credential leakage
  - 1 billion user accounts and passwords
- Check now
  - https://haveibeenpwned.com/PwnedWebsites
  - We re-use passwords. Info shared across platforms can lead to problems
- Password is an unsolved task …. '123456' remain the most commonly used password for years
  - Convenience

NATIONAL SECURITY: STUXNET (2010)

- Stuxnet: Windows-based Worm
  - Worm: self-propagating malicious software (malware)
- Attacking industrial control systems (ICS)
  - Used in factories, chemical plants, and nuclear power plants
- First reported in June 2010, public aware of it only in July 2010
- Seems to be a digital weapon created by a nation-state
  - 60% (more than 62 thousand) of infected computers in Iran
  - Iran confirmed that nuclear program damaged by Stuxnet
  - Sophisticated design, special targets, expensive to develop
  - One example of the Advanced Persistent Threat (APT)

MALWARE SEEMLY RELATED TO STUXNET

- Duqu (September 2011)
  - Use stolen certificates, exploits MS Word
- Flame (May 2012)
  - “Suicide” after being discovered
  - 20 MB, with SQLLite DB
  - Hide its own presence, exploit similar vulnerabilities as StuxNet, and adjust its behavior to different Anti-Virus
  - Presents a novel way to produce MD5 hash collision to exploit certificates

DEEPFAKE

Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case
(from the Wall Street Journal, Aug 30, 2019)

> *" … a fraudulent transfer of €220,000 ($243,000) "*

ANY THOUGHTS?

WHAT IS COMPUTER SECURITY?

WHAT IS COMPUTER SECURITY?

- Security = Sustain desirable properties under intelligent adversaries

- Desirable properties
  - What properties are needed?
- Intelligent adversaries
  - Needs to understand/model adversaries
  - Always think about adversaries

SECURITY PROPERTIES (C, I, A)

Confidentiality

(secrecy, privacy)

Only those who are authorized to know can know

Integrity

(authenticity)

Only modified by authorized parties and in permitted ways

do things that are expected

Availability

Those authorized to access can get access when needed

C, I, A VIOLATIONS

- Stuxnet attack compromises
  - Integrity of software systems, Availability of some control functionalities, Confidentiality of some keys in order to sign malware to be loaded by Windows
- The Apple/Amazon attack
  - Confidentiality of credit card digits, Integrity of password, Availability of data and devices
- The Facebook attack
  - Integrity, Potential availability concern

COMPUTER SECURITY ISSUES

- Malware (Malicious Software)
  - Computer viruses
  - Trojan horses
  - Computer worms
    - E.g., Morris worm (1988), Melissa worm (1999), Stuxnet (2010), etc.
  - Spywares
  - Malwares on mobile devices
- Computer break-ins
- Email spams
  - E.g., Nigerian scam (419 scam, advanced fee fraud), stock recommendations

MORE COMPUTER SECURITY ISSUES

- Identity theft
- Driveby downloads
- Botnets
- DDoS
- Security flaws electronic voting machines, ATM systems

WHY DO COMPUTER ATTACKS OCCUR?

Who are the attackers?

bored teenagers, criminals, organized crime organizations, rogue (or other) states, industrial espionage, angry employees, …

Why they do it?

fun, fame, profit, political/military objectives

WHY DO ATTACKS SUCCEED?

- Software/computer systems are buggy
  - Vulnerabilities, CVEs (*Common Vulnerabilities and Exposures*)
- Users make mistakes
  - Social engineering
- Technological factors
  - Von Neumann architecture: stored programs
  - Unsafe program languages
  - Software are complex, dynamic, and increasingly to be so
  - Making things secure are hard
  - Security may make things harder to use

WHY DO THESE FACTORS EXIST?

Economical factors

- Lack of incentives for secure software
- Security is difficult, expensive and takes time

Human factors

- Lack of security training for software engineers
- Largely uneducated population

SECURITY IS NOT ABSOLUTE

- Is your car secure?
- Are you secure when you drive your car?

- Security is relative
  - To the kinds of loss one consider
    - Security objectives/properties need to be stated
  - To the threats/adversaries under consideration
    - Security is always under certain assumptions

THREE GOLDEN RULES

> “
>
> The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it.
>
> ”

-- Dr. Robert H. Morris

SECURITY IS SECONDARY

- What protection/security mechanisms one has in the physical world?
- Why the need for security mechanisms arises?
- Security is secondary to the interactions that make security necessary

A CHAIN IS ONLY AS STRONG AS ITS WEEKEST LINK

HUMAN IN THE LOOP

PHISHING EMAILS

CLICKJACKING

INSIDERS

SECURITY IS INTERESTING

- The most interesting/challenging threats to security are posed by human adversaries
    - Security is harder than reliability
- Information security is a self-sustaining field
    - Can work both from attack perspective and from defense perspective
- Security is about benefit/cost tradeoff
    - Thought often the tradeoff analysis is not explicit
- Security is not all technological
    - Humans are often the weakest link

SECURITY IS CHALLENGING

- Defense is almost always harder than attack.
- In which ways information security is more difficult than physical security?
  - Adversaries can come from anywhere
  - Computers enable large-scale automation
  - Adversaries can be difficult to identify
  - Adversaries can be difficult to punish
  - Potential payoff can be much higher
- In which ways information security is easier than physical security?

TOOLS FOR INFORMATION SECURITY

- Cryptography
- Authentication and Access control
- Hardware/software architecture for separation
- Processes and tools for developing more secure software
- Monitoring and analysis
- Recovery and response

WHAT IS THIS COURSE ABOUT?

Learn to think about security when doing things

Learn to understand and apply security principles

Learn how computers can be attacked, how to prevent attacks and/or limit their consequences.

No silver bullet; man-made complex systems will have errors; errors may be exploited

Large number of ways to attack

Large collection of specific methods for specific purposes

ETHICAL USE OF SECURITY INFORMATION

- We discuss vulnerabilities and attacks
  - Most vulnerabilities have been fixed
  - Some attacks may still cause harm
  - Do *not* try these outside the context of this course

NEXT CLASS

BASIC CRYPTO: HOW TO HIDE MESSAGES?