COMP3632: Introduction & Security Mindset

Shuai Wang

香 港 科 技 大 學
THE HONG KONG UNIVERSITY OF SCIENCE AND TECHNOLOGY

Course Information

- COMP3632: Principles of Cybersecurity
  - We will meet every Wednesday/Friday from 16:30pm to 17:50PM
  - Zoom Online Meeting
  - We may change into the “mix-mode” after two weeks.
  - Room 2611
- Zoom
  - If you have any question: “Raise hands”
  - Or just write text and send via Zoom
  - Our TAs will keep an eye on Chat
  - And I will also read it before the end of the class

Who am I?

- Instructor: Shuai Wang
  - Assistant Professor of CSE at HKUST
  - Postdoc Scholar at ETH Zurich
  - PhD at Penn State University
  - B.S. at Peking University
- Research Interests:
  - Cybersecurity
  - Methodologies & techniques to secure/exploit software & systems
  - AI Security
- Office:
  - Room 3512
  - Office hour: Thursday 2:30pm to 3:30pm
  - Zoom link: https://hkust.zoom.us/j/7305996251
  - Let me know your feedback

TA & Tutorial Sessions & Contact Info

- TA: Yuanyuan YUAN & Qi PANG
- Office: Cybersecurity Lab (Room 3664, Lift 31-32)
- Please preface your e-mail title with “[COMP3632]”
  - Shuai Wang: shuaiw@cse.ust.hk
  - Yuanyuan: yyuanaq@cse.ust.hk
  - Qi: qpangaa@cse.ust.hk

TA & Tutorial Sessions & Contact Info

- Tutorial sessions
  - We will follow the convention of COMP3632 to setup a tutorial session.
  - NOT mandatory; will share the materials online and do the recording as well.
  - some Q&A (e.g., course materials; assignments)
  - Attack/defense Demo? Will do some during tutorial sessions, and I will let you know when it would be ☺
  - You can always send us an email and schedule individual time slots, if needed.

Course Website

- Course site: https://course.cse.ust.hk/comp3632/
  - Please make sure you can access the course site
- Schedule is tentatively posted:
  - Please frequently check this web-page for any schedule changes → I will also announce in the class
  - We will have a slow start but become slightly faster later.

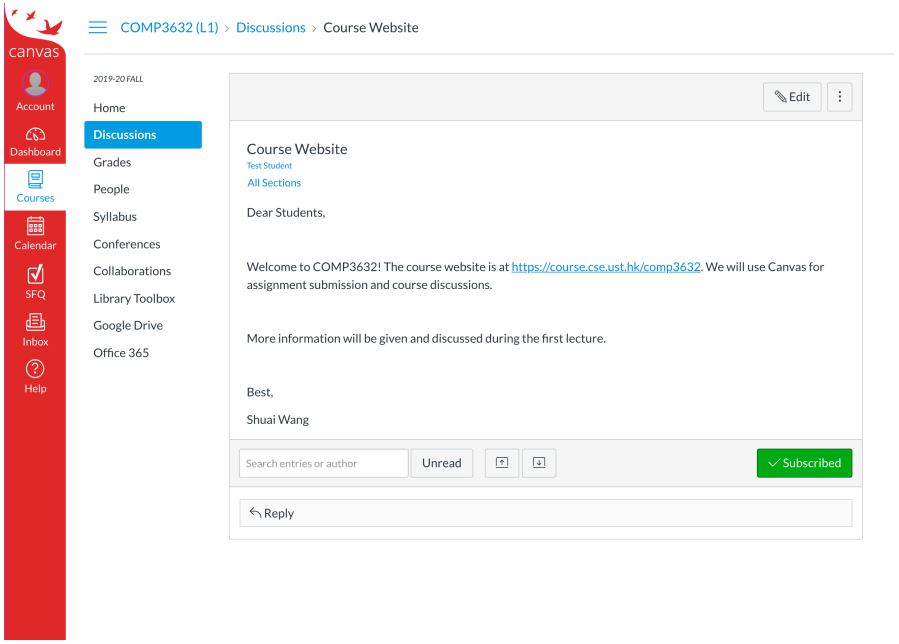
Class Schedule

Below is the calendar for this semester course. This is the preliminary schedule, which will be altered as the semester progresses. It is the responsibility of the students to frequently check this web-page for schedule, readings, and assignment changes. As the professor, I will attempt to announce any change to the class, but this web-page should be viewed as authoritative. If you have any questions, please contact me.

Date	Topic	Readings	Note
08/09	Introduction; Security Mindset | Slides	A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles. link.	
10/09	Classic Crypto | Slides		
15/09	Symmetric Key Crypto 1 | Slides		
17/09	Symmetric Key Crypto 2 | Slides		
22/09	Public Key Crypto 1 | Slides		
24/09	Public Key Crypto 2 & Hash Function | Slides		
29/09	Reverse Engineering | Slides		
01/10	Holiday; No Class		
06/10	Malware | Slides		
08/10	Software Exploitation : Buffer Overflow | Slides | ROP Attack		

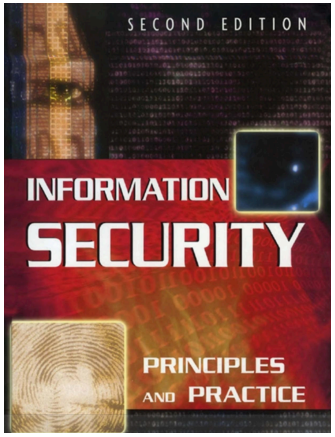
Canvas

- We tentatively decide to use Canvas for homework submission and make announcement.
  - Or you prefer to use Canvas for all COMP3632 matters?

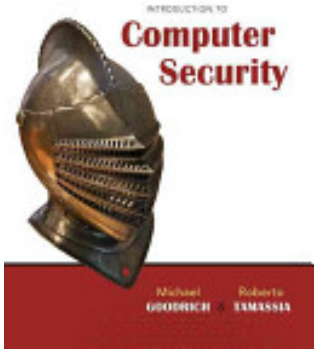


Slides & Text Book

- Will post on the course website before the class
  - Will post hand-written notes after each class
  - Will post the Zoom recording after each class
- Readings are optional, encourage to read after the class.
- Text book (optional):



Information Security: Principles and Practice



Introduction to Computer Security

Again, for text books, they are not required; E-book is fine.

Grading

- In-class quizzes – 5%
- Assignment (x4) – 40%
  - Written + Programming
- Hacking practice – 5%
  - Programming
  - Roughly within April
- Midterm exam – 20%
  - March-19th
  - during the class time; but open book, open notes (like another “homework”)
  - Topics taught for the first half of the course
- Final exam – 30%
  - TBD

*If any student needs special accommodations because of a disability, please contact me in the first week of classes

Policies

- Late policy
  - All homework assignments are assessed a 20% per-day late penalty, up to a maximum of 3 days.
- Assignment
  - Assignments have to be complete by the student individually.
  - The student will receive the same penalty if he/she let others copy the assignment.
- Classroom
  - Using laptops are allowed in class.
- Ethics statement
  - Be a happy and ethic hacker ☺
  - More in course website. You can always reach out to me and ask.

Questions?

Goals for this Course

- Mindset
  - How to think like an attacker/defender
  - How to reason about threats and risks
- Principles & Technical Skills
  - How to design and program secure software
  - …
- Get some senses on the "problem-driven" style studies in cybersecurity
  - It's always an arms race, between attackers and defenders
- Learn to become a "hacker", an ethic one

Cybersecurity is Real-World Problem-Driven

- Although we mostly focus on principle in this course.
  - See further slides on Cybersecurity roadmap at UST ☺
- Many (research) topics are indeed driven by security breaches in the real world!
  - That's one key reason I decide to work in this field

A True Story in Real Life

aws

Amazon Web Services

Mon May 18 2020 10:51:26

Translate

Was this response helpful? Click here to rate:

★★★★★

Hi there,

wangshuai

Hello,

aws

Amazon Web Services

Fri Jun 05 2020 15:00:49 GMT+0800 (Hong Kong Standard Time)

Translate

Was this response helpful? Click here to rate:

★★★★★

Hello there,

Martin here from AWS.

I'm happy to advise that 100% of the charges for the compromised activity on y
been waived. Rest assured, you no longer have to worry about the charges.

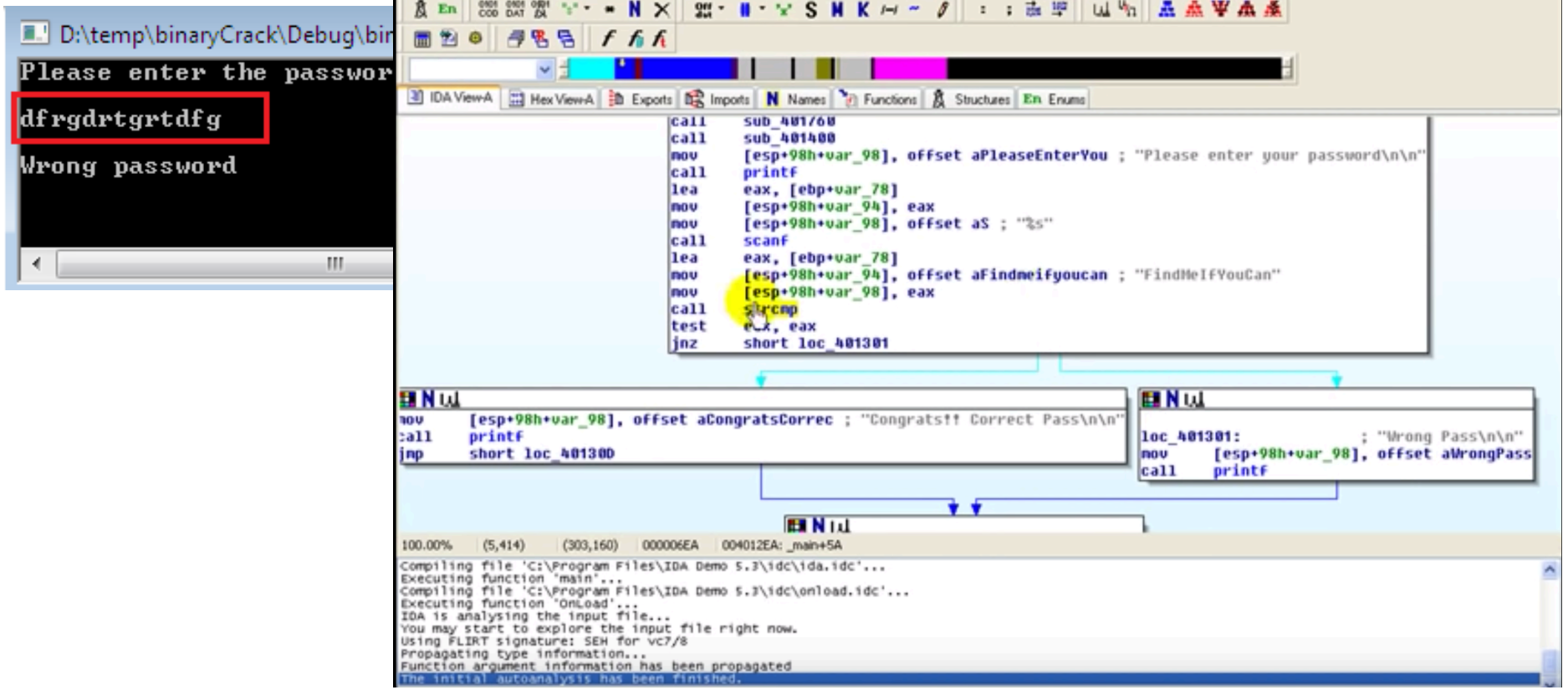
To avoid similar compromises in the future, please consider the following to he
security of your account.

Topics Covered in This Course

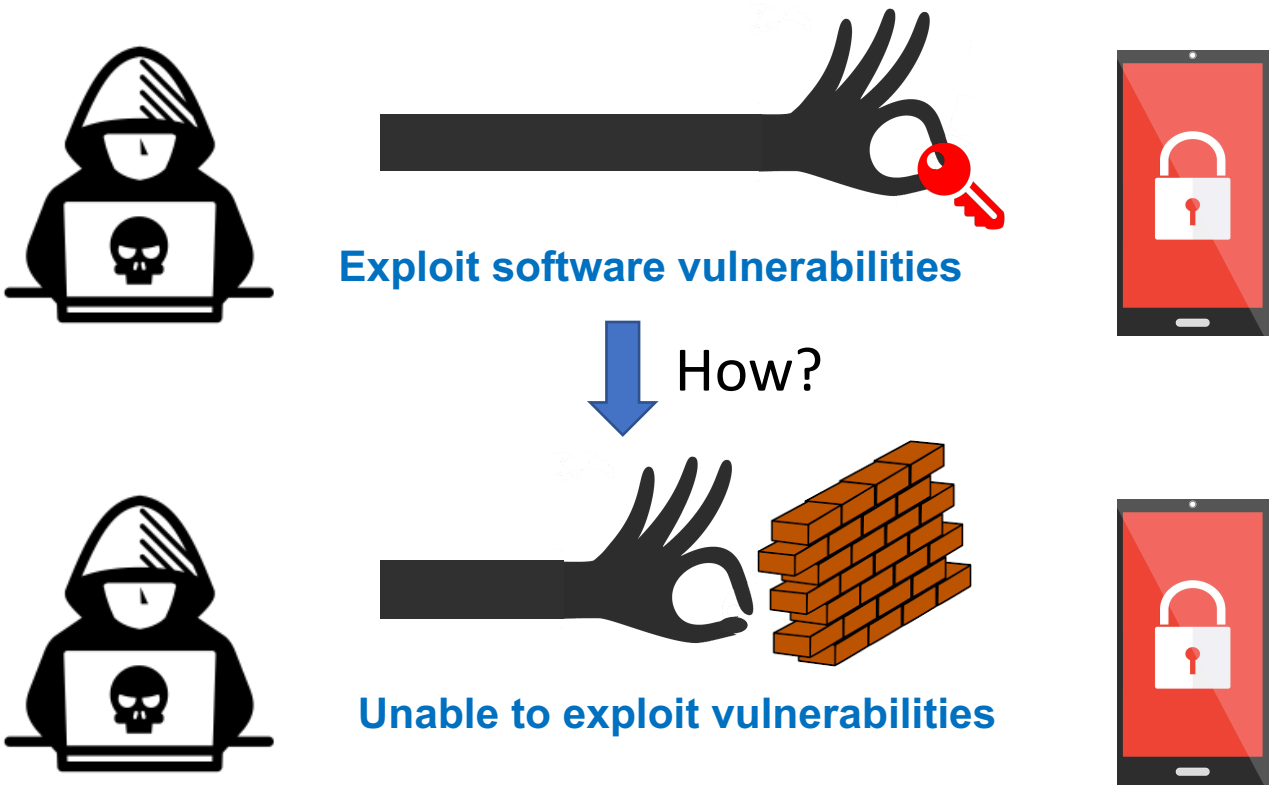
- Security basics and definitions:
  - Confidentiality, Integrity, Availability, attack models
- Cryptography:
  - Basic crypto primitives, public key crypto, signatures, authentication, symmetric crypto
- Software security:
  - Memory errors, buffer overflow, obfuscation, malware, security testing
- System & web security:
  - Authentication, access control, protocols, browser security, side channel attacks
- Security on emerging platforms:
  - blockchain; IoT; AI;

Reverse Engineering

- How to break the password protection of a Windows software?

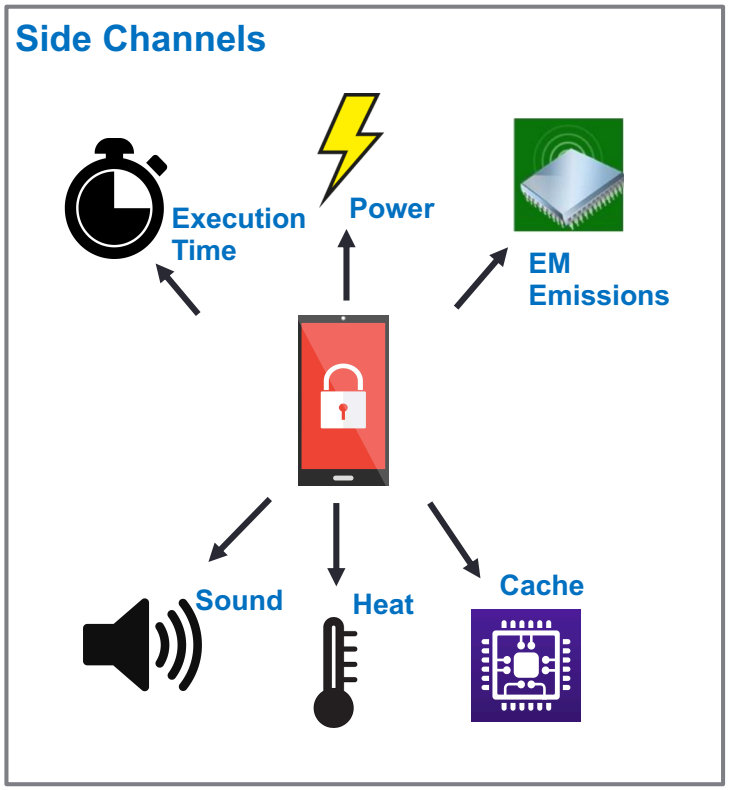


Side Channel Attacks



Side Channel Attacks

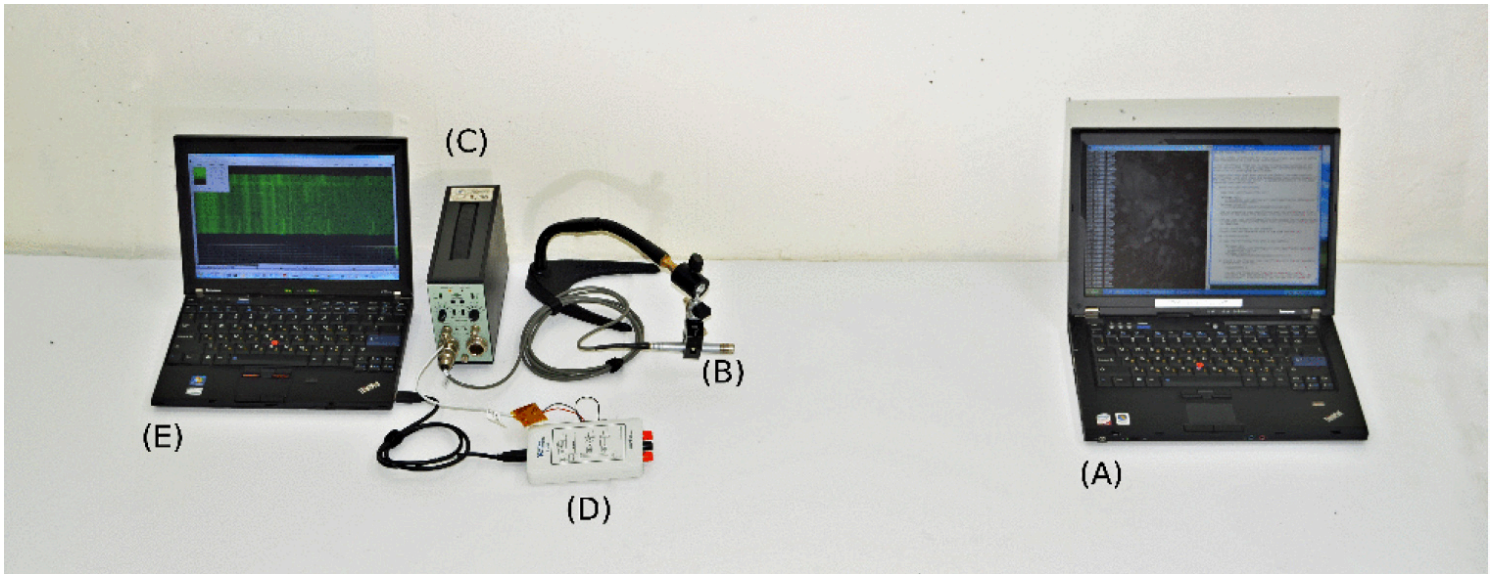
- De-facto exploitations in Cybersecurity



Infer secrets via **secret-dependent** physical information.

Side Channel Attacks

- Infer your secrets (password; private key) via acoustic side channel attack

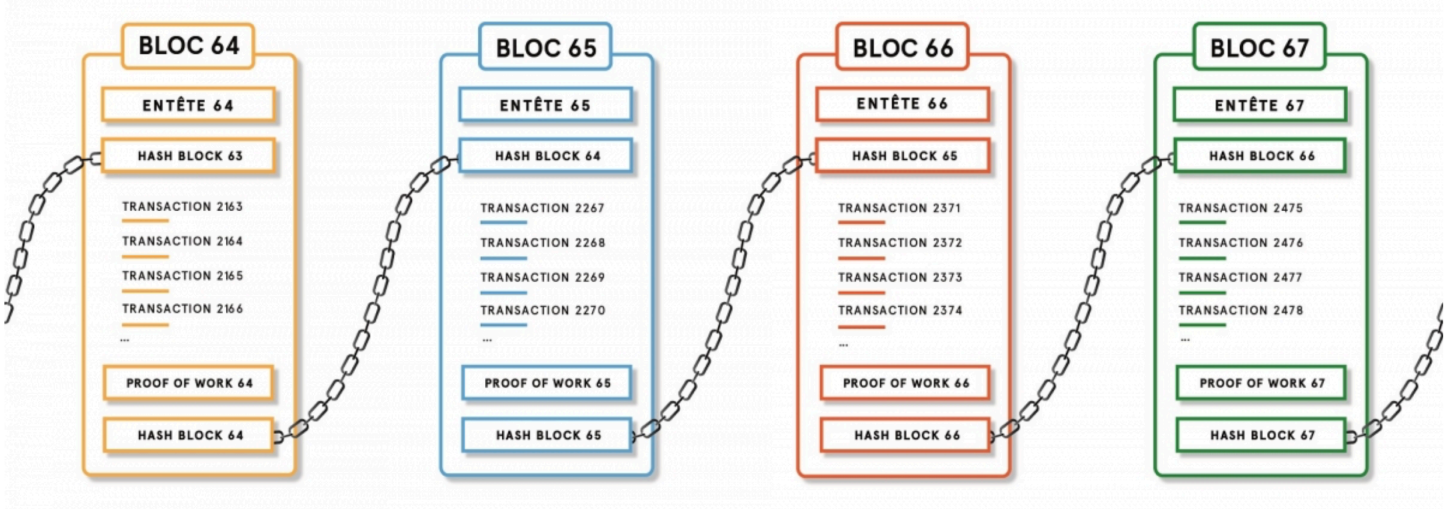


Attacker's

Victim's

Blockchain

The best real-world crypto application ~~and have made many millionaires~~?



Bitcoin

- Unregulated digital currency
- Bitcoin transactions are stored on Blockchain
- Each anonymous address on the blockchain acted as a simple bank account.

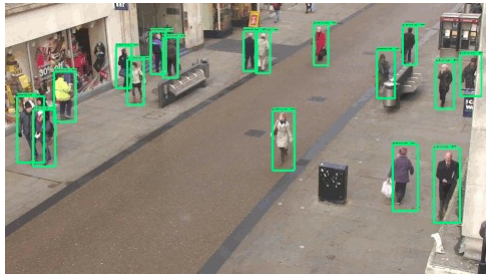
Ethereum

- Unregulated digital currency and computing system
- Smart contracts: programs executed on the blockchain
- Each anonymous address on the blockchain could be a user or a smart contract.

Blockchain figure from: https://blog.theodo.com/2018/01/deploy-first-ethereum-smart-contract-blockchain/

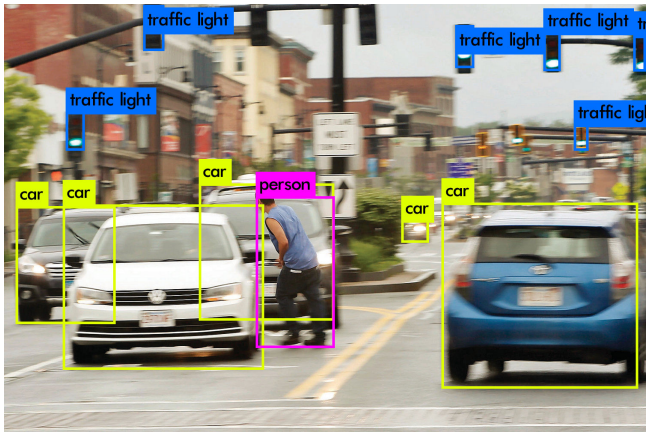
Artificial Intelligence

- AI techniques have been used for security purposes.

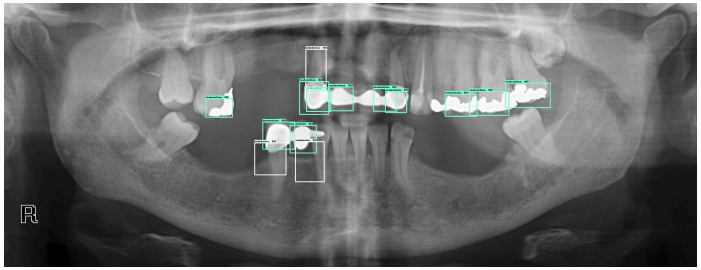


Surveillance Camera

Surveillance Camera



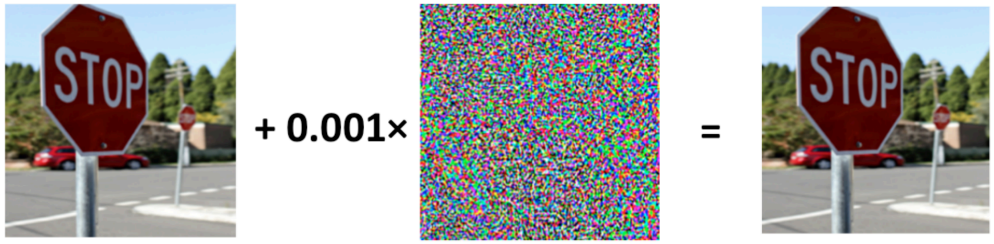
Auto-Driving Systems



Medical Image Processing

Artificial Intelligence

- Adversarial attacks are popular...



Classification failure

Object detection failure

We will talk more cases on AI security.

For more “practical” or “academic” aspects…

- COMP4632: *Cybersecurity: Attacks and Counter-measures*
  - You will see Prof. Ricci IEONG this semester
  - More on the practical attack/defense
    - Some well-made labs/tutorials
    - More hands-on experience
  - Usage of some tools

For more “practical” or “academic” aspects…

- Catch-The-Flag (CTF) team: *Firebird*
- FYP and UROP?
- PG courses?
- Doing research?
  - Cybersecurity lab at UST

HKUST Firebird CTF Team Won Championship of PwC Hackaday 2019

Questions?

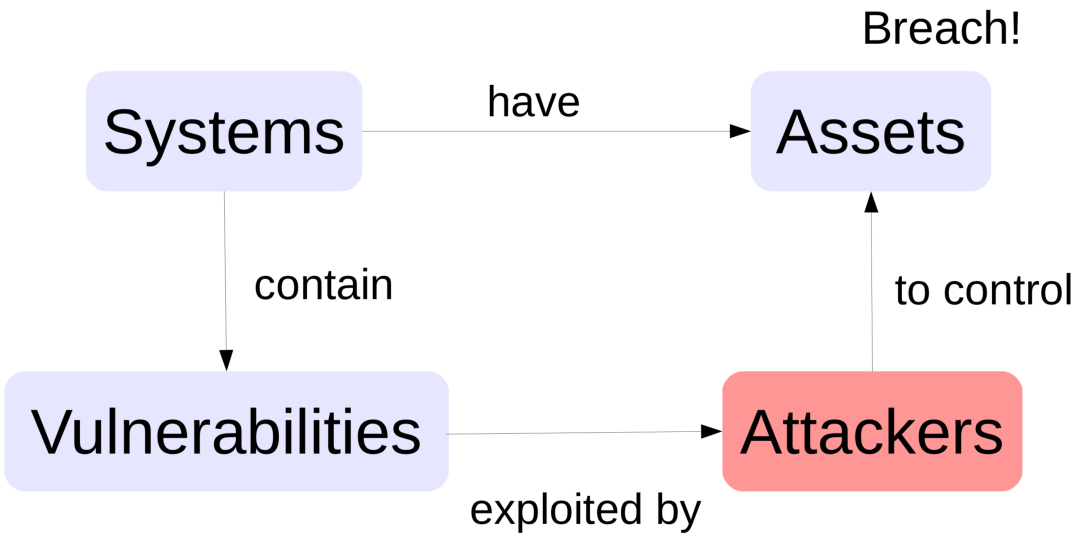
The Security Mindset

Attacker vs. defender

The Security Mindset

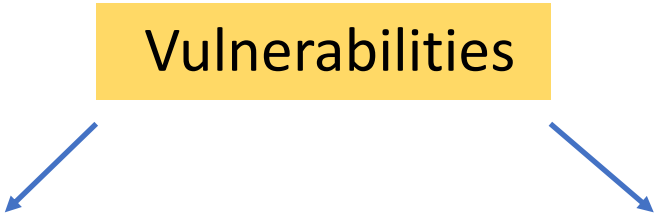
- Think like a cyber attacker
  - Understand techniques and opportunities for exploiting security. → next two slides
- Think like a cyber defender
  - Know yourself: security policy
  - Know yourself: risk assessment
  - Know your enemy: threat model
  - Benefits vs. costs:
    - Some security defenses are just too expensive

Think Like an Attacker



Think Like an Attacker

Where do vulnerabilities come from?



Design

- Theoretical limitations
- Lack of security features (e.g. authentication)
- Side channels
- Wrong threat model
- Wrong user model

Implementation

- Coding errors
- Hardware errors
- Injected errors
- Failure to meet specifications

Where can I get vulnerabilities?

- Find unknown vulnerabilities → hard
- Buy zero-day vulnerabilities → well, you can do that..?
- Reuse known vulnerabilities → easy?

But Why Good Citizens Need to Know How to Attack?

To understand this, think about why biologists would study (unknown) virus...

White hat wizards!

- Identify vulnerabilities so they can be fixed.
- Learn about unknown threats.
- Help venders to build more secure systems.
- ~~And get lots of bonus from vendors~~

Think Like a Defender

- Security policy
  - What property we are trying to enforce?
    - E.g., password can only be stored within my phone.
    - E.g., data pointers in your C code can only access certain memory region.
  - Could be difficult to even define the policy/specification
- Risk assessment
  - Identify assets (e.g., network, servers, applications, data centers, etc.) within the organization.
  - Asset criticality.
  - Measure the risk ranking for assets and prioritize them for assessment.

Think Like a Defender

- Threat model
  - Who are the attackers?
  - What kind of capability they have?
  - What kind of information/data they try to steal?

Think Like a Defender

- Threat model for a (simplified) cloud computing platform
  - Attacker; capability; assets

Think Like a Defender

- Threat model
  - Who are the attackers?
    - Service provider, and other users
  - What kind of capability they have?
    - Service provider can control anything
    - Attackers on the cloud VM can share the same hardware with you
      - Common threat model for side channels
  - What kind of assets they try to steal?
    - Anything valuable!

Think Like a Defender

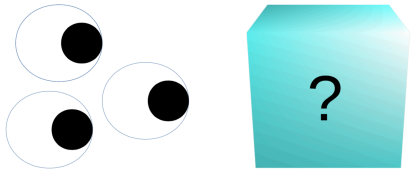
- Costs vs. benefits?
  - For example, to protect an OS kernel from being exploited, you can have two options:
    - Online monitoring:
      - easy to do.
      - slow down the performance
    - Offline formal verification:
      - very difficult to conduct for commercial OS.
      - But no penalty for online performance.
- Saltzer and Schroeder's Principles of Secure Design
  - A series of design principles for secure systems
    - Extensions for reading after the class.
  - Some of the rules may not be applicable nowadays.

Saltzer and Schroeder's Principles of Secure Design

- 1) Open Design vs. Obscure Design

The system's design should be openly available to everyone.

"Given enough eyeballs, all bugs are shallow"
-- Linus Torvalds



Saltzer and Schroeder's Principles of Secure Design

- 2) Economy of Mechanism

The system should be simple enough to understand and analyze.

Helpful for security analysis:
- Debugging/code audit
- Static/dynamic analysis
- Formal verification

Clean interfaces between modules, avoid global state, etc.

Saltzer and Schroeder's Principles of Secure Design

- 3) Least Privilege

A subject should only be given the minimum necessary privileges for completing its task.

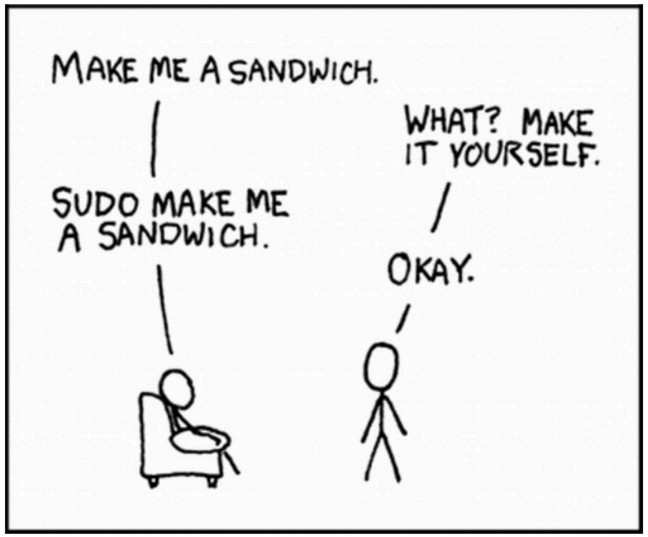


Figure out exactly what capabilities a program requires in order to run, and grant exactly those

- This is not easy. One approach is to start with granting none, and see where errors occur.

Principles of CIA

Confidentiality

Information is secret

Integrity

Information/System is correct

Availability

System is usable

We will talk more on these aspects later.

Summary

- The endless arms race between cyber attackers and defenders lead to many interesting problems
  - For doing research & engineering
- Be a happy and ethic hacker!
  - Otherwise your instructor might run into trouble …
  - Whenever in doubt, ask me