ECE 568F Computer Security

Lecture 1: Introduction to Security and Course Information

Course Instructor: Wei Huang

UNIVERSITY OF TORONTO

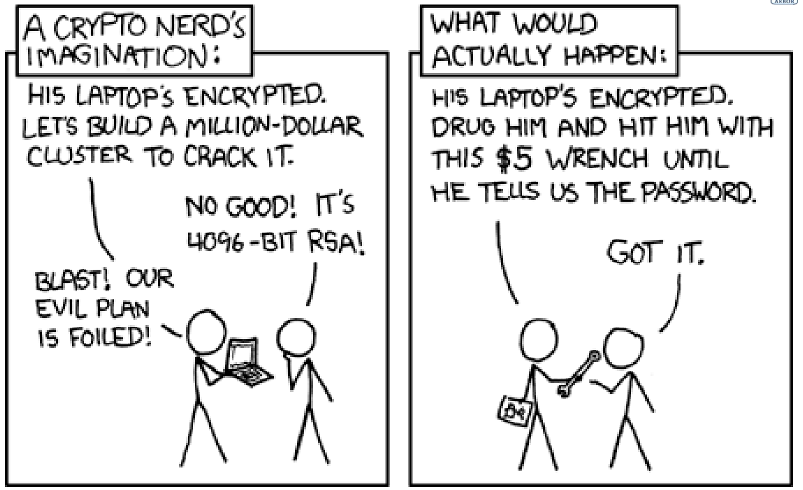
What is Security?

- Goal vs. Adversary

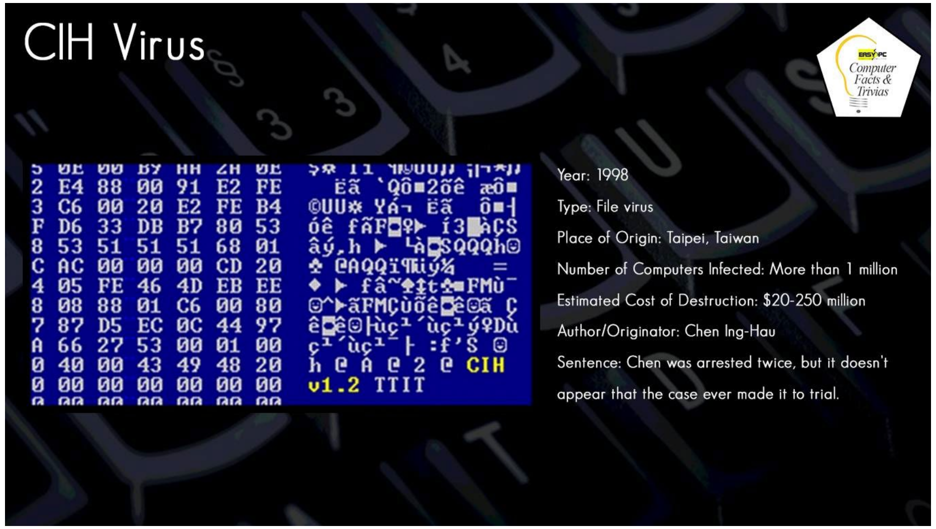
- Security Policies
  - Confidentiality
  - Integrity
  - Availability
  - …

Threat Model

- Assumptions about the adversary
- Attacker’s motivation --- Economics
  - Fun & Profit
  - Vulnerability Marketplace


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.
$5

(Xkcd-538)



CIH Virus

```
2 E4 88 00 91 E2 FE     Ëã `Qô■2õê æô■
3 C6 00 20 E2 FE B4   ©UU☼ YÁ¬ Ëã  ô■┤
F D6 33 DB B7 80 53   óê fÃF◘♀► í3█àÇS
8 53 51 51 51 68 01   âý,h ►  └à◘SQQQh☺
C AC 00 00 00 CD 20   ♣ @AQQï¶iý½    =
4 05 FE 46 4D EB EE   ♦ ► fâ~♠↨t♣■FMù¯
8 08 88 01 C6 00 80   ☺^►ãFMÇùõê◘ê☺ã Ç
7 87 D5 EC 0C 44 97   ê◘ê☺├ùç¹´ùç¹ý♀Dù
A 66 27 53 00 01 00   ç¹´ùç¹¯├ :f'S ☺
0 40 00 43 49 48 20   h @ A @ 2 @ CIH
0 00 00 00 00 00 00   v1.2 TTIT
```

Year: 1998

Type: File virus

Place of Origin: Taipei, Taiwan

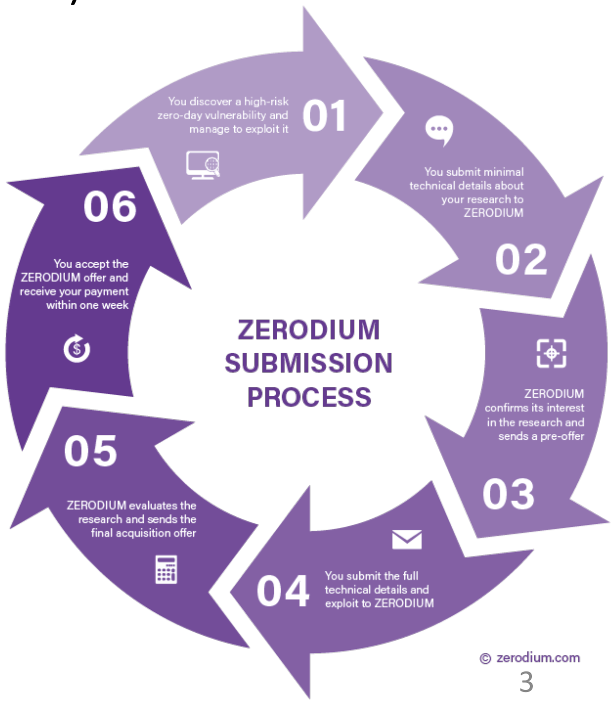
Number of Computers Infected: More than 1 million

Estimated Cost of Destruction: $20-250 million

Author/Originator: Chen Ing-Hau

Sentence: Chen was arrested twice, but it doesn't appear that the case ever made it to trial.

Photo from Wikipedia



ZERODIUM SUBMISSION PROCESS

01 You discover a high-risk zero-day vulnerability and manage to exploit it

02 You submit minimal technical details about your research to ZERODIUM

03 ZERODIUM confirms its interest in the research and sends a pre-offer

04 You submit the full technical details and exploit to ZERODIUM

05 ZERODIUM evaluates the research and sends the final acquisition offer

06 You accept the ZERODIUM offer and receive your payment within one week

© zerodium.com

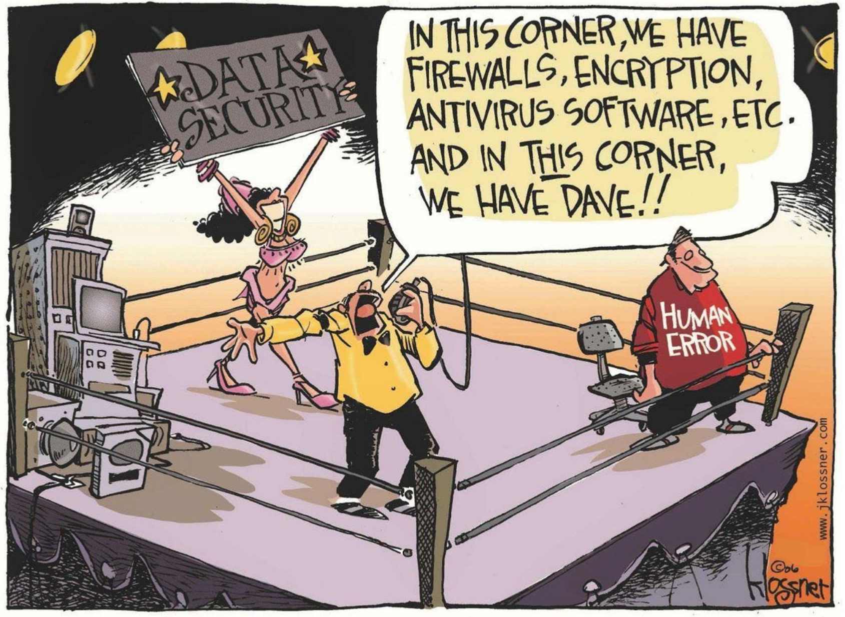
Security Mechanism

- How to help uphold a security policy, e.g.,
  - Permission system
  - Encryption
  - Hardware protection
  - …

- Security goal has nothing to say about security mechanism

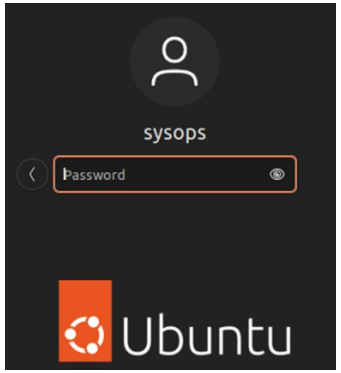
Why is Security Hard?

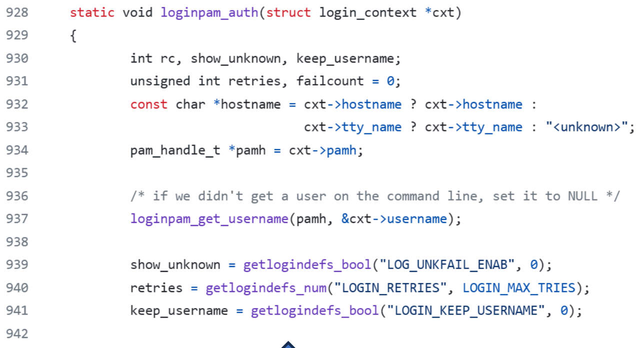
- Assuming the threat model
  - Realistic scenario
  - Updating environment
- Enumerating all possible ways to attack
- Weakest link matters
- Hardware changing
- There are always human errors


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©06 Lossner

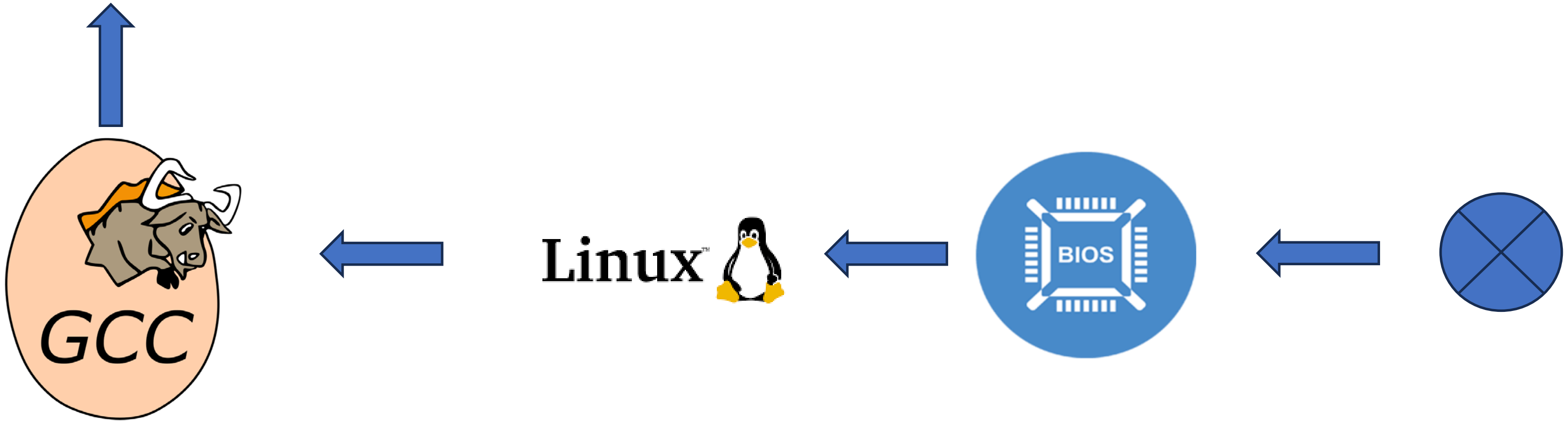
What Can We Trust?

- Ken Thompson: Reflections on Trusting Trust (CACM, 1984)



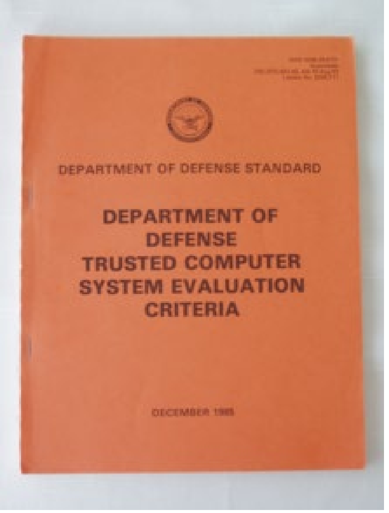


```
static void loginpam_auth(struct login_context *cxt)
{
        int rc, show_unknown, keep_username;
        unsigned int retries, failcount = 0;
        const char *hostname = cxt->hostname ? cxt->hostname :
                               cxt->tty_name ? cxt->tty_name : "<unknown>";
        pam_handle_t *pamh = cxt->pamh;

        /* if we didn't get a user on the command line, set it to NULL */
        loginpam_get_username(pamh, &cxt->username);

        show_unknown = getlogindefs_bool("LOG_UNKFAIL_ENAB", 0);
        retries = getlogindefs_num("LOGIN_RETRIES", LOGIN_MAX_TRIES);
        keep_username = getlogindefs_bool("LOGIN_KEEP_USERNAME", 0);

```



What Can We Trust?

- Nothing can be trusted
  - But we still need to work something out
- Assuming TCB: Trusted Computing Base
  - The minimal part of the system is not compromised
  - All secure systems built on top of that



DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

DECEMBER 1985

Class Break

- See you in 15 minutes
- Next Session: Computer Security in the Future, Course information, Logistics, Q&A

Computer Security in the Future

- Data Privacy
- Artificial Intelligence (AI)
- Internet-of-things (IoT)
- Cybercrime-as-a-service (CaaS)

Future: Data Privacy

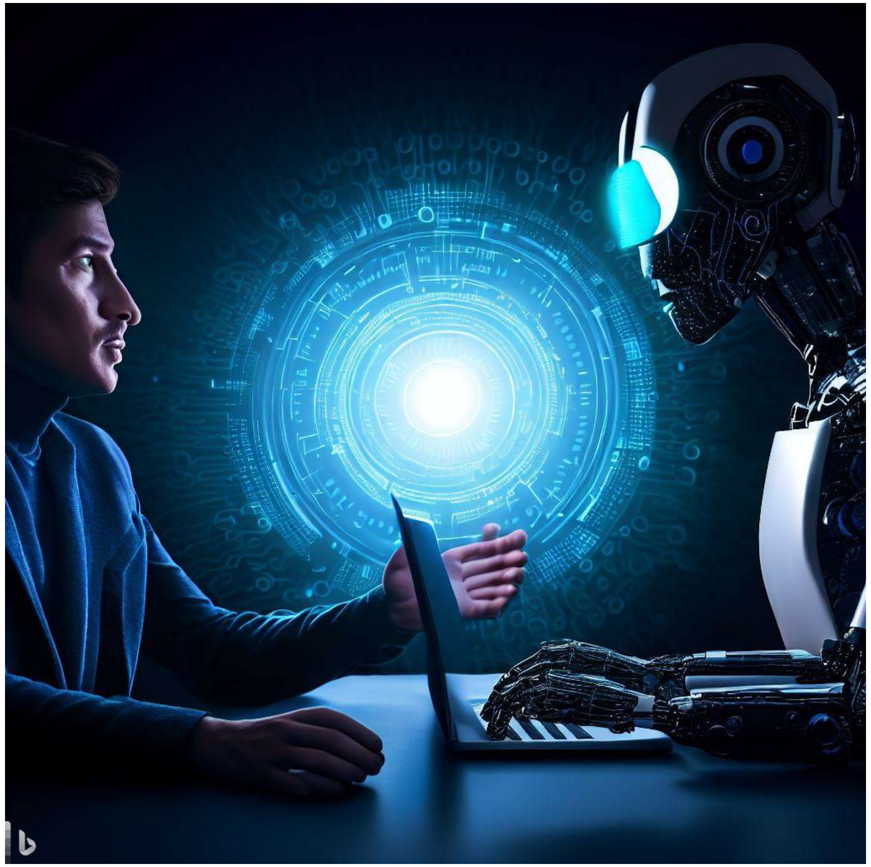
- Governing how data is collected, shared and used
- Compliance with data protection laws and regulations

- Protecting data from internal and external attackers
- Measures that an organization is taking in order to prevent any third party from unauthorized access

Future: Artificial Intelligence

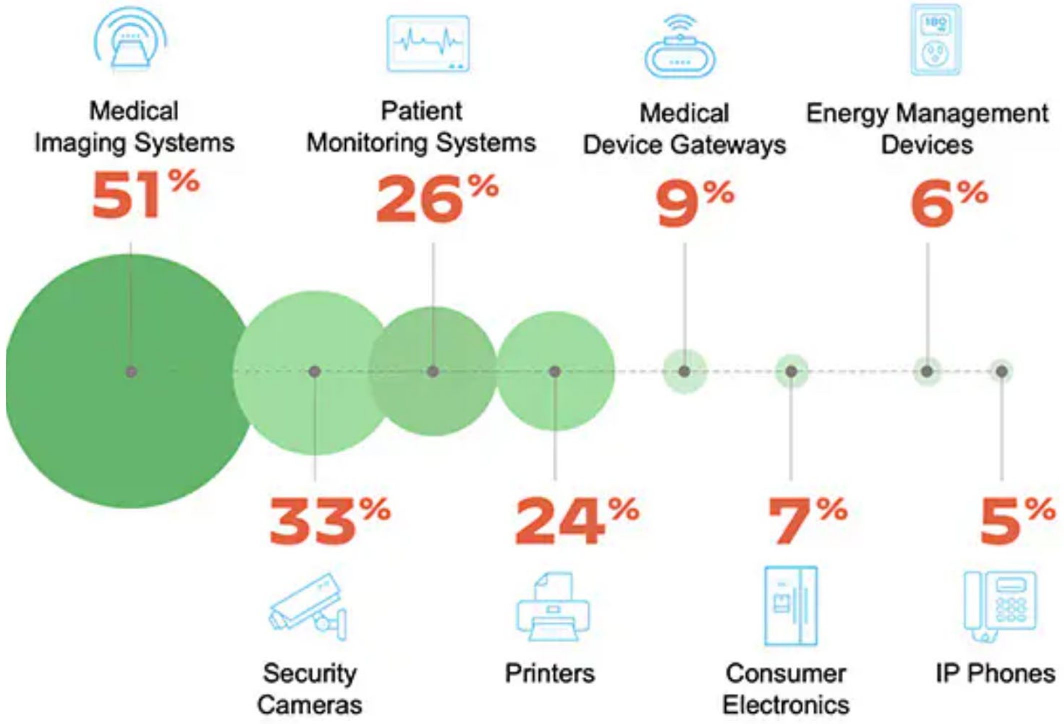
- Concept and scope may change:
    - Adversaries
    - Defenders

- Laws and regulations may need to adapt



Future: Internet of Things

- IoT systems lack of
  - Secure update system
  - Physical barriers
  - Privacy protection
  - Network services
- Legacy liabilities
- Insecure or outdated components

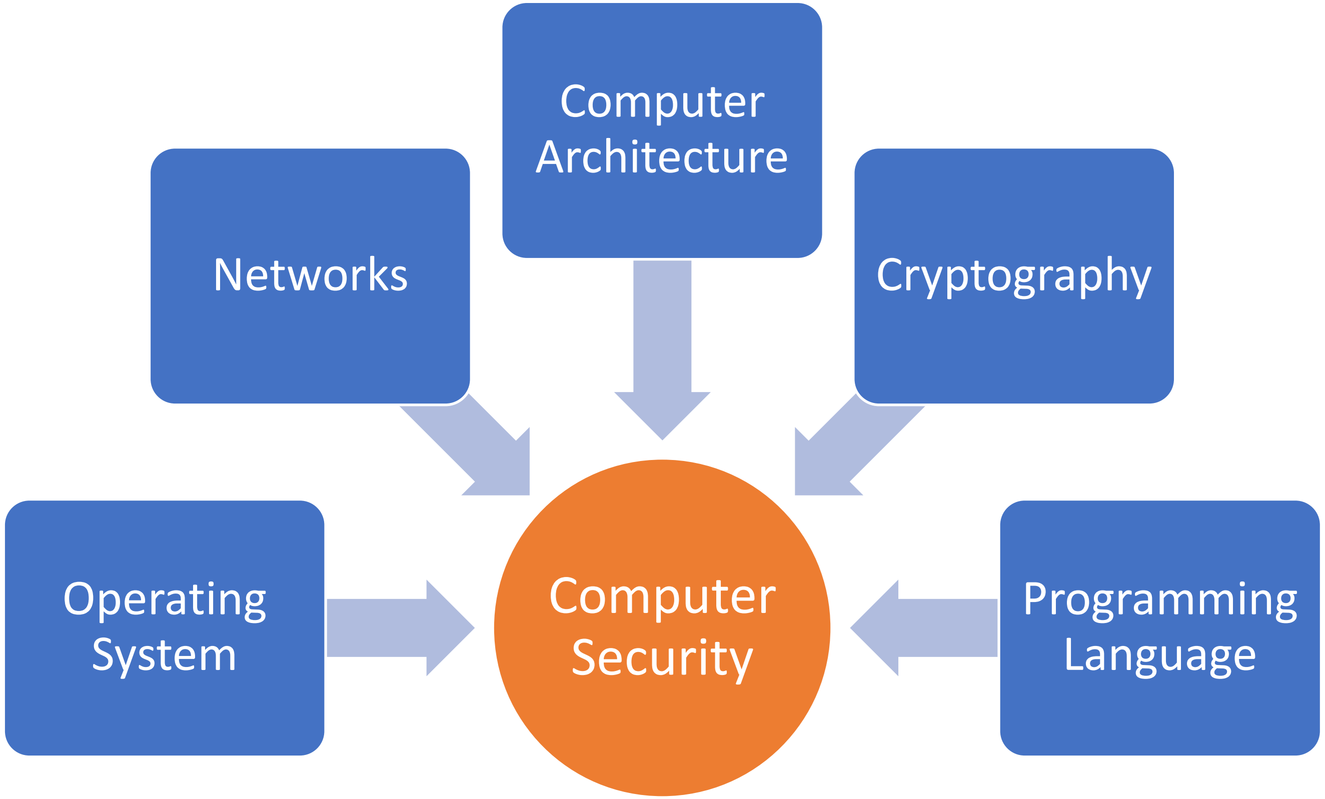


IoT Devices with highest share of security issues (from: Palo Alto Networks)

Future: Cybercrime

- Cybercrime prevention and security
- Mysterious guest lecturer

Course Prerequisites and Placement



Course Outline

- Introduction
- Software Code Vulnerabilities
  - Buffer Over-flows, ROP, Format String, CFI …
- Cryptography and OS Security
  - Basic ciphers, encryptions, Key exchange, MAC,
  - Secure hardware, OS kernel security, Side channel ..
- Network Security
  - Secure communication, SSL, Web authentication, XSS…
  - Network protocol attacks, DNS security …
  - Blockchains, Crypto currencies, Cybercrimes …

Course Deliveries

- Lecture slides
  - Every week
- Reference books and articles
  - Provided on course website, optional readings, not required
- 4 Labs assignments
  - Provided on course website
- Office hours
  - By appointment

Course Marking

- Labs
  - 30%
- Mid-Term Exam
  - 30%
- Final Exam
  - 40%

Course Policy

- Discussion policy:
  - Raise your question on class discussion board
  - Email instructor and TAs
  - Schedule office hours with instructor

- Plagiarism
  - University policy

- Artificial intelligence aid:
  - (ChatGPT, Co-Pilot, Codeium, Code Whisperer, …)
  - Need to claim which part is AI-generated, even after manual modifications
  - Use with care

Summary of Computer Security Introduction

- You can’t get any further away, before you start coming back

-- The Truman Show (1998)

Questions about the course

- Q&A