Security Features

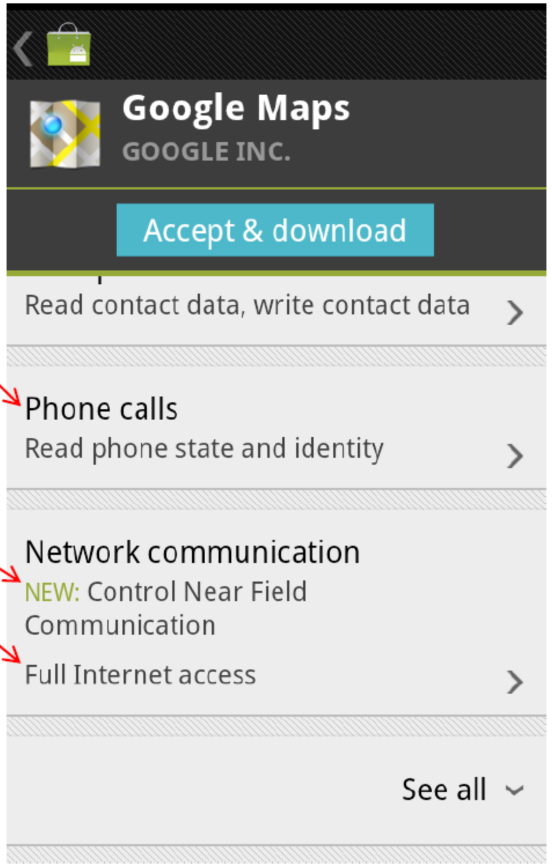
- Application sandbox
  - Each application runs with its UID in its own runtime environment
    - Provides CPU protection, memory protection
  - Access control to resources based on SELinux (MAC model)
- Applications announce permission requirement
  - Create a whitelist model – user grants access at install time
- Communication between applications
  - May share same Linux user ID
    - Access files from each other
    - May share same Linux process and runtime environment
  - Or communicate through application framework
    - “Intents,” reference monitor checks permissions

Android Permissions

- Example of permissions provided by Android
  - “android.permission.INTERNET”
  - “android.permission.READ_EXTERNAL_STORAGE
  - “android.permission.SEND_SMS”
  - “android.permission.BLUETOOTH”
- Also possible to define custom permissions

Android Permission Model

```
...
<uses-permission android:name="android.permission.READ_PHONE_STATE" />
<uses-permission android:name="android.permission.NFC" />
<uses-permission android:name="android.permission.INTERNET" />
...
```



Google Maps
GOOGLE INC.

Accept & download

Read contact data, write contact data

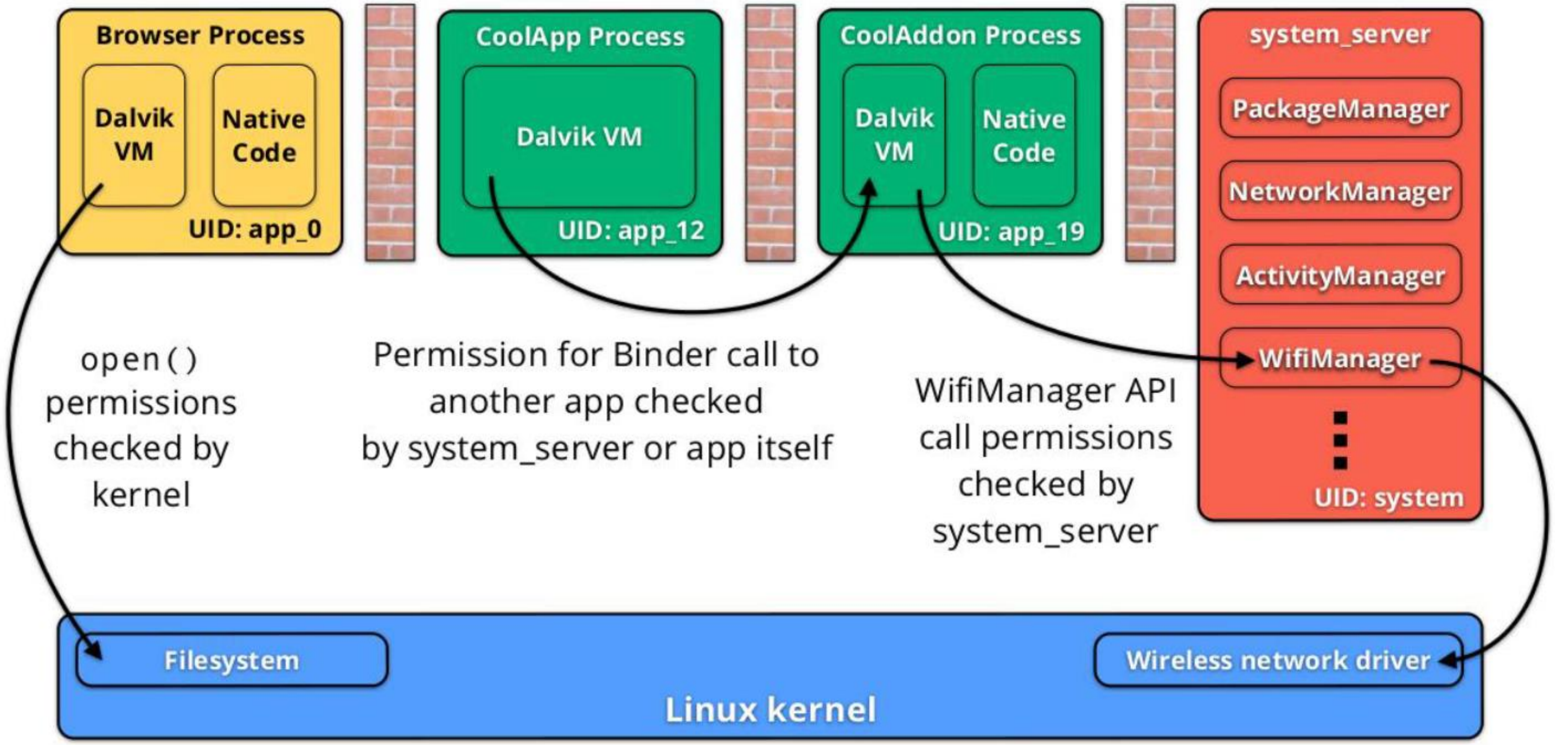
Phone calls
Read phone state and identity

Network communication
NEW: Control Near Field Communication
Full Internet access

See all

https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

Android Permission Model



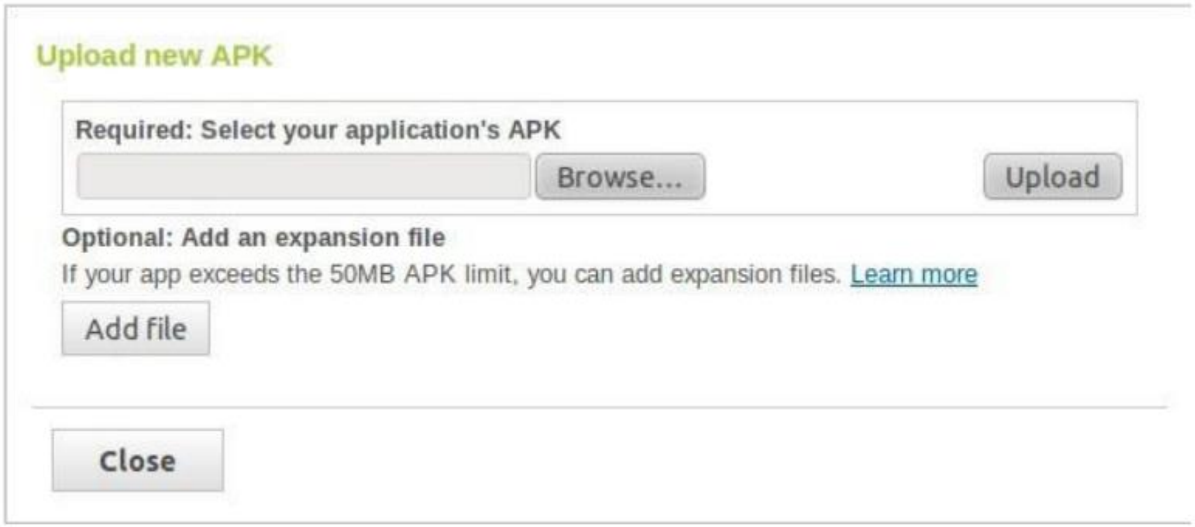
https://www.owasp.org/images/3/3e/Danelon_OWASP_EU_Tour_2013.pdf

Android market

- Apps are signed by the developers
- App scanning when uploaded to market
  - Bouncer for Google Play
- Open market
  - Bad applications may show up on market
  - Shifts focus from remote exploit to privilege escalation

Bouncer in a nutshell

- Runtime analysis of app
- Emulated Android environment
- Runs for 5 minutes
- On Google's infrastructure
- User action simulated to trigger and detect malicious payload



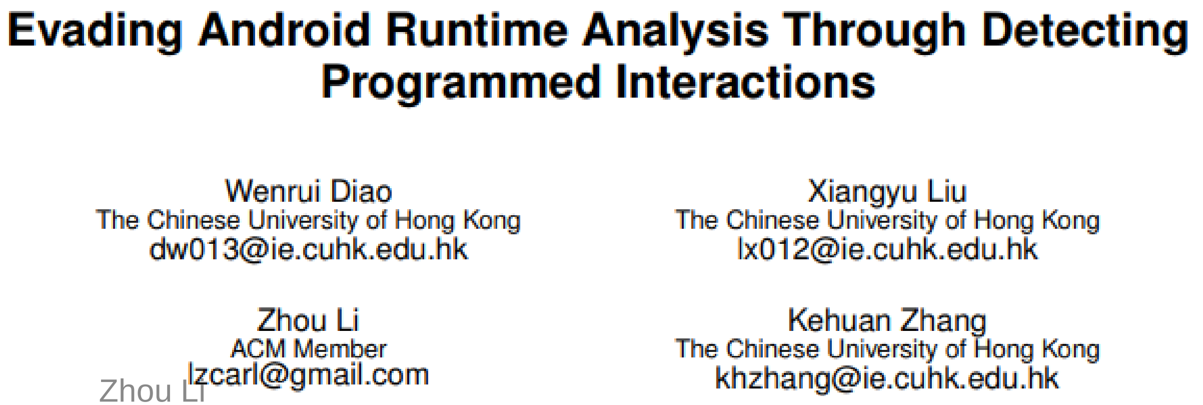
Upload new APK

Required: Select your application's APK

Optional: Add an expansion file

If your app exceeds the 50MB APK limit, you can add expansion files. Learn more

How to evade?



Evading Android Runtime Analysis Through Detecting Programmed Interactions

Wenrui Diao
The Chinese University of Hong Kong
dw013@ie.cuhk.edu.hk

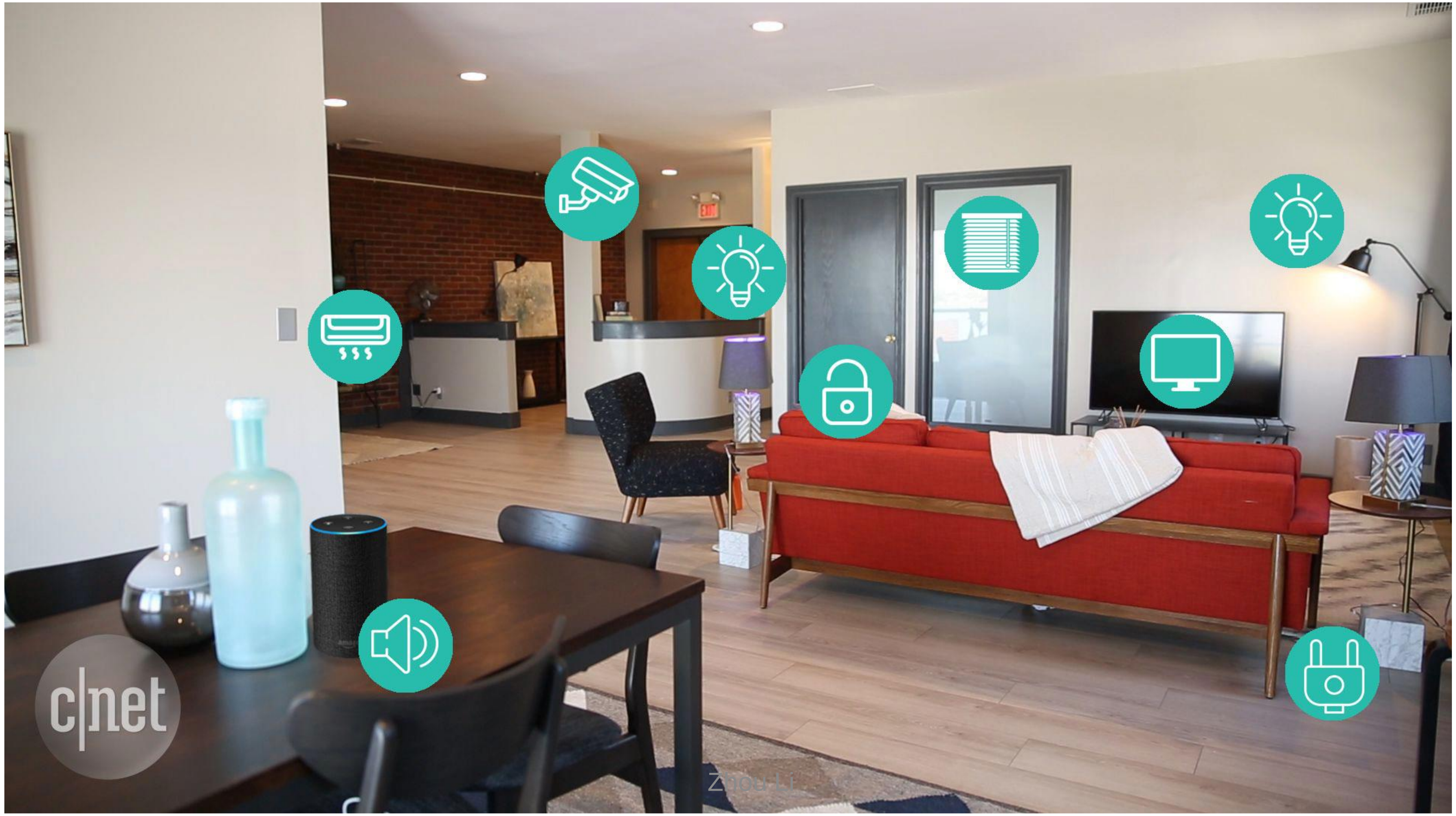
Xiangyu Liu
The Chinese University of Hong Kong
lx012@ie.cuhk.edu.hk

Zhou Li
ACM Member
lzcarl@gmail.com

Kehuan Zhang
The Chinese University of Hong Kong
khzhang@ie.cuhk.edu.hk

IOT (Internet of Things)

Smart
Home

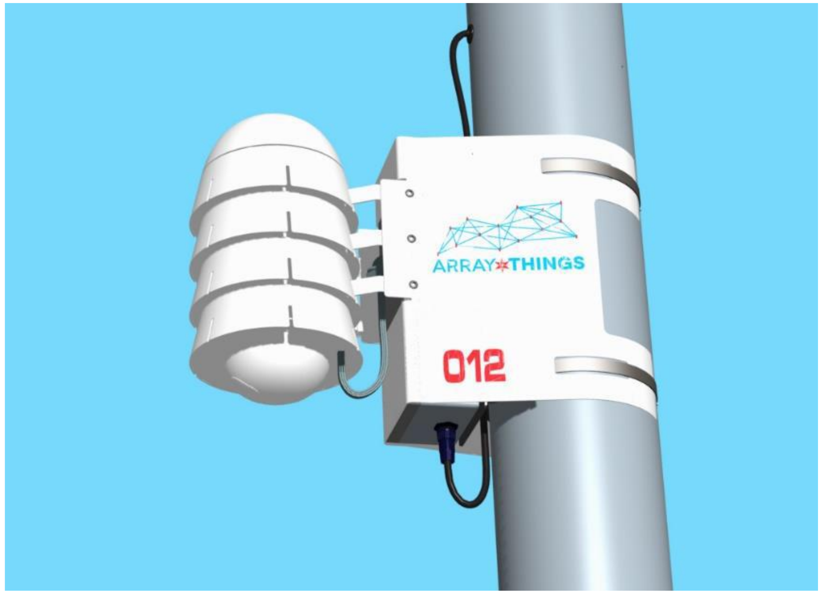


Beyond Smart Home

Industrial Internet

Autonomous Vehicles

Smart Cities

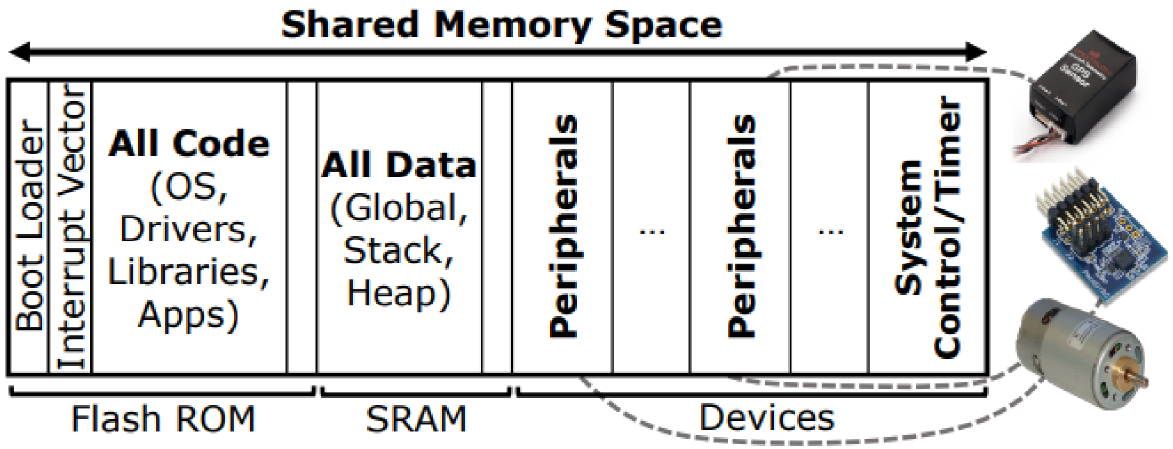


What's different with IoT security?

- Customized hardware & OS
  - Resource-limited and energy-saving
  - Not all security features can be applied
- Customized network protocols and behaviors
  - Can enable new security and privacy issues
- Physical interactions with environment
  - New input and output channels whose security and privacy implications are not well understood

Real-time microcontroller systems (MCS)

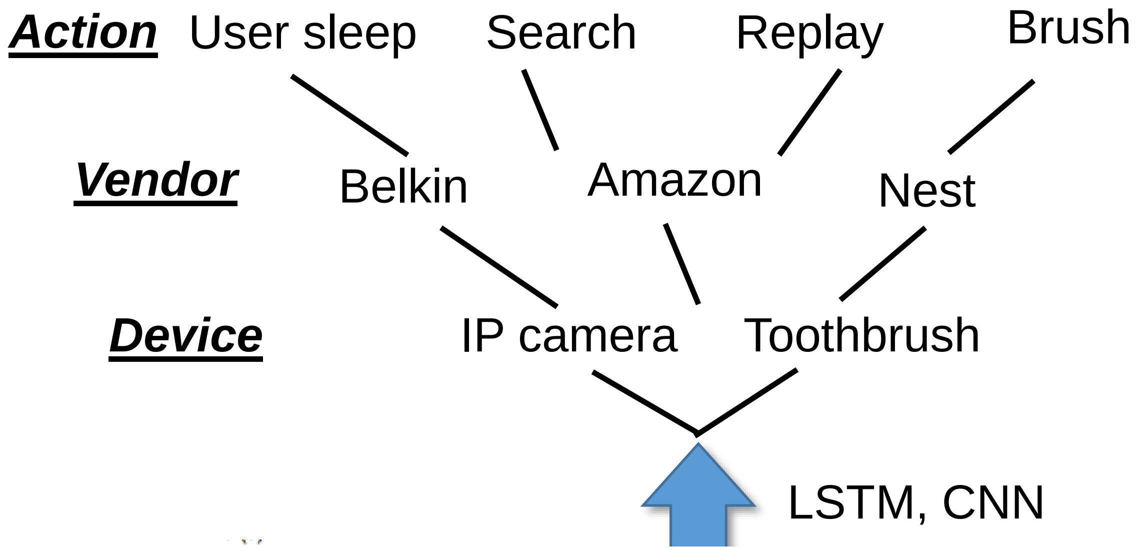
- A real-time operating system (RTOS) designed in 1991.
  - Used in Avionics, Medical equipment and devices, Industrial controls, Automotive
- No process memory isolation
  - No Memory Management Unit (MMU), no virtual memory
  - Memory space shared by all processes
- No kernel memory isolation
  - Do not make use of 1) privileged and unprivileged processor modes and 2) Memory Protection Unit (MPU)

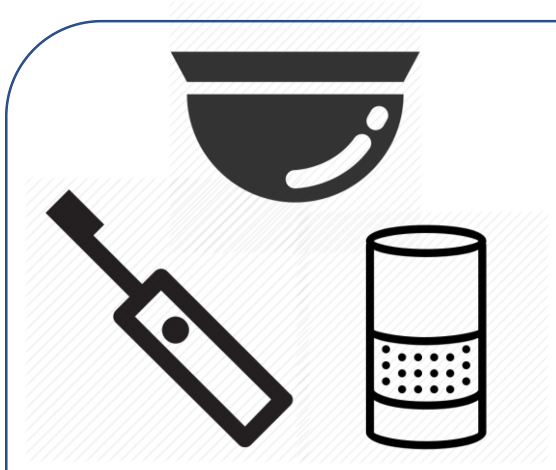


Securing Real-Time Microcontroller Systems through Customized Memory View Switching, NDSS’18

Privacy leakage from IoT network traffic

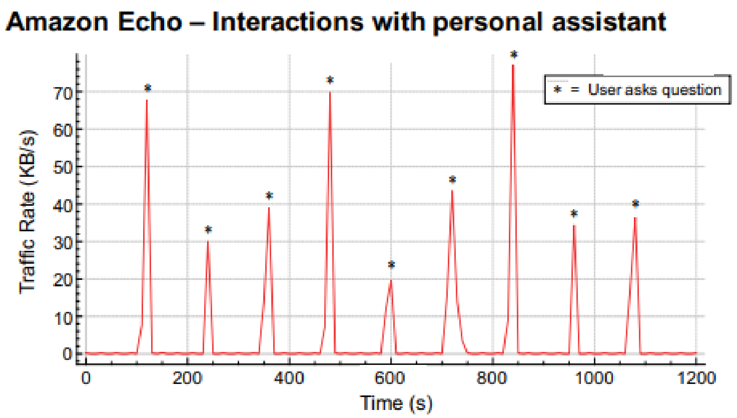
- ***My ongoing work:*** network traffic profiling



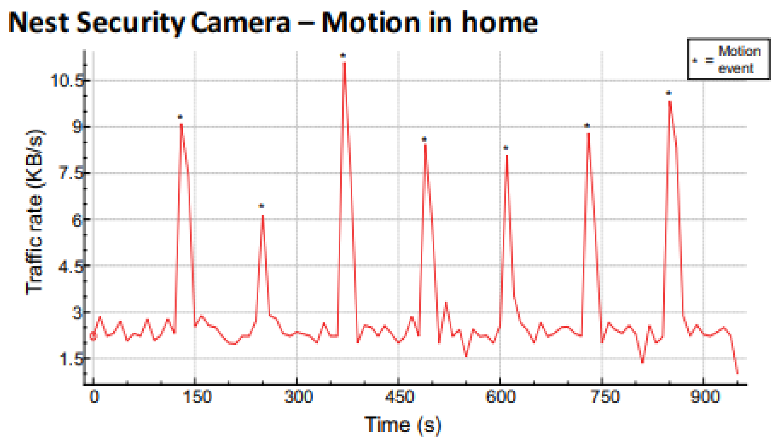


- *Less user-interactions*

Amazon Echo – Interactions with personal assistant



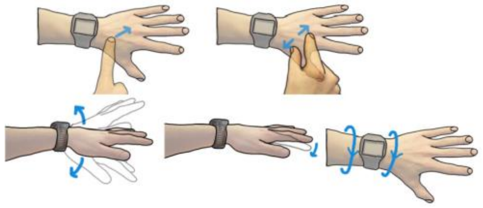
Nest Security Camera – Motion in home



Side-channel inference from sensors

- Wearable device with sensors

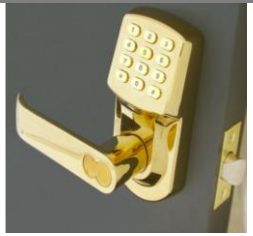
- Enable a broad range of useful applications



- Sensitive information could be leaked

Accessing sensors doesn't require any permission!

Electronic door lock



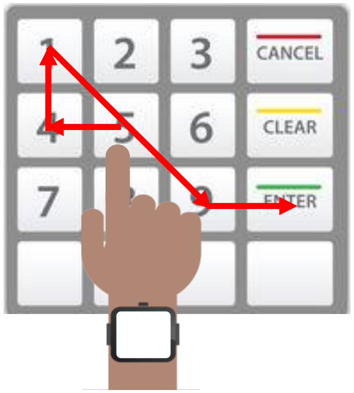
ATM machine

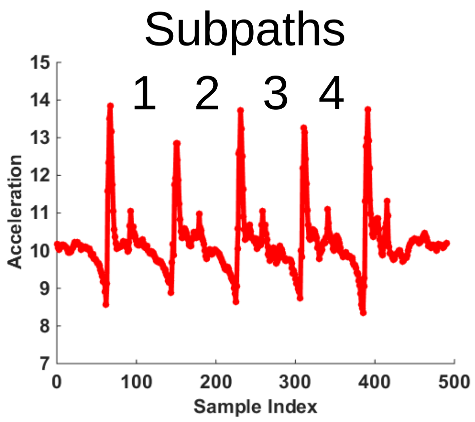
Keypad controlled server

Friend or Foe? Your Wearable Devices Reveal Your Personal PIN, AsiaCCS'14

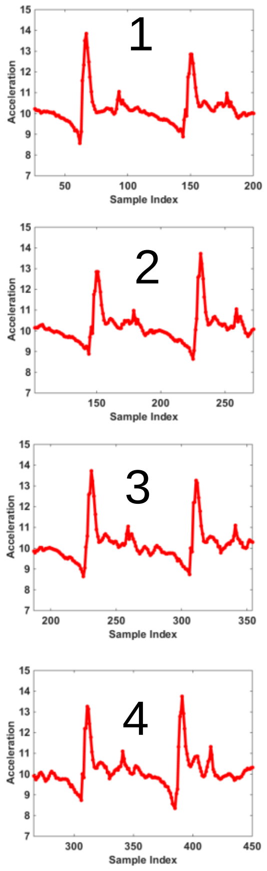
Inferring what you type through accelerometers

Input “5419-Enter”

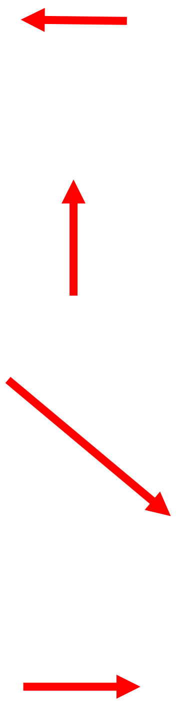




Key-click trace segmentation



Subpath recovery



Slides credit

- Security in computing 5th edition, Textbook Slides
- DISSECTING GOOGLE BOUNCER Lecture 11a, Muhammad Rizwan Asghar
- Mobile Device and Platform Security, John Mitchell

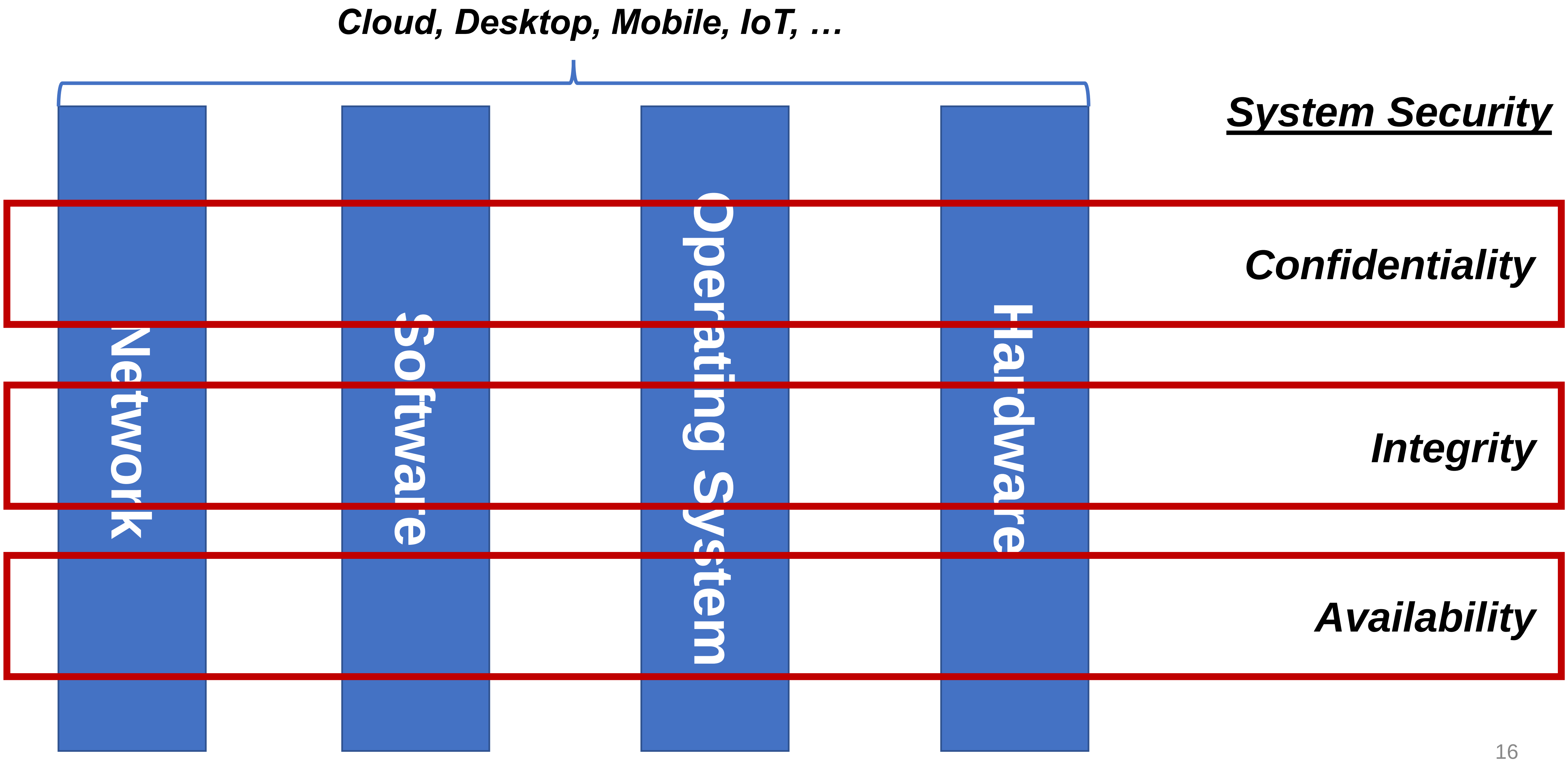
Course Summary

EECS 195

Spring 2019

Zhou Li

System Security



Cloud, Desktop, Mobile, IoT, …

Network

Software

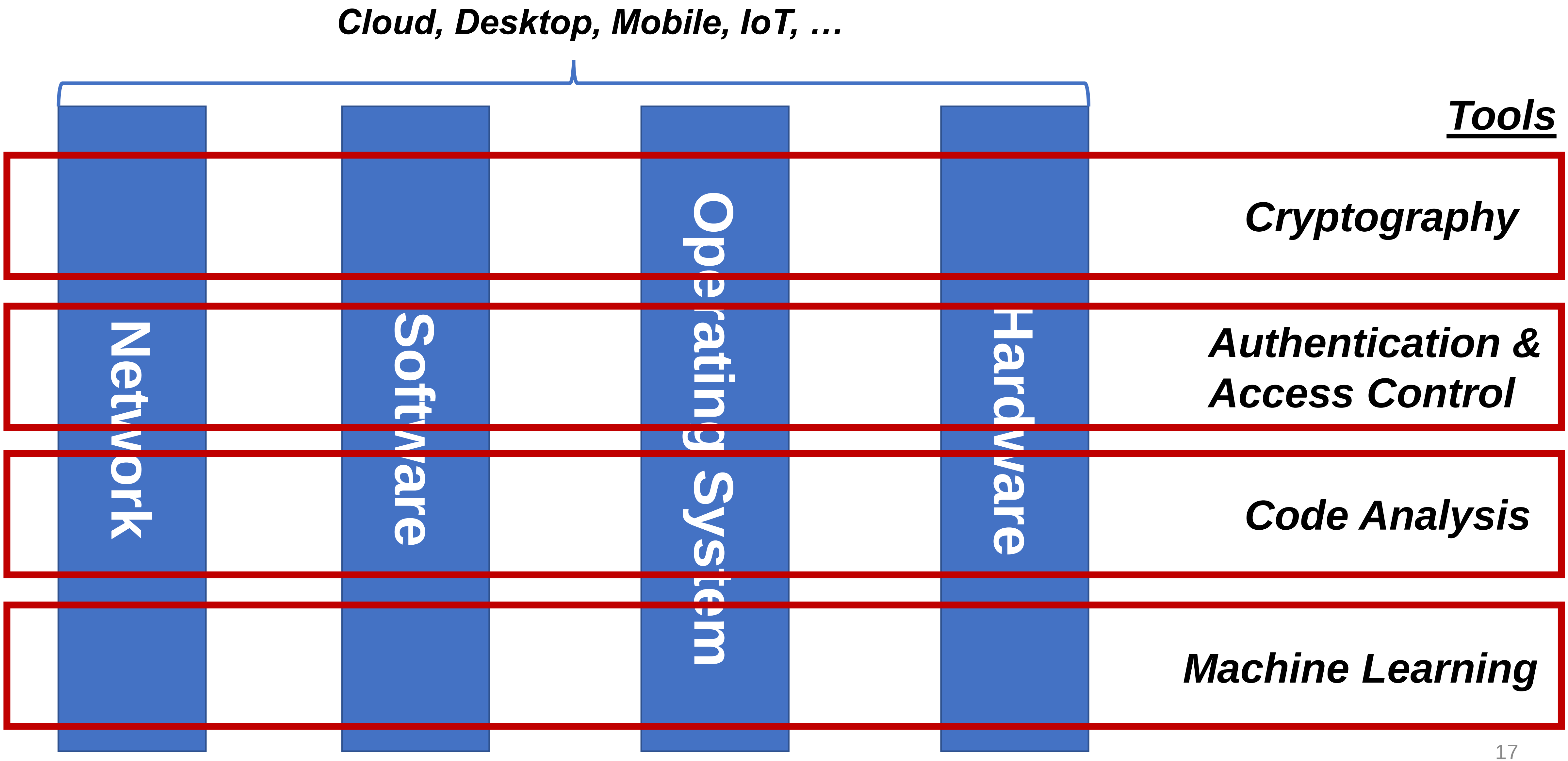
Operating System

Hardware

Confidentiality

Integrity

Availability



Cloud, Desktop, Mobile, IoT, …

Network

Software

Operating System

Hardware

Tools

Cryptography

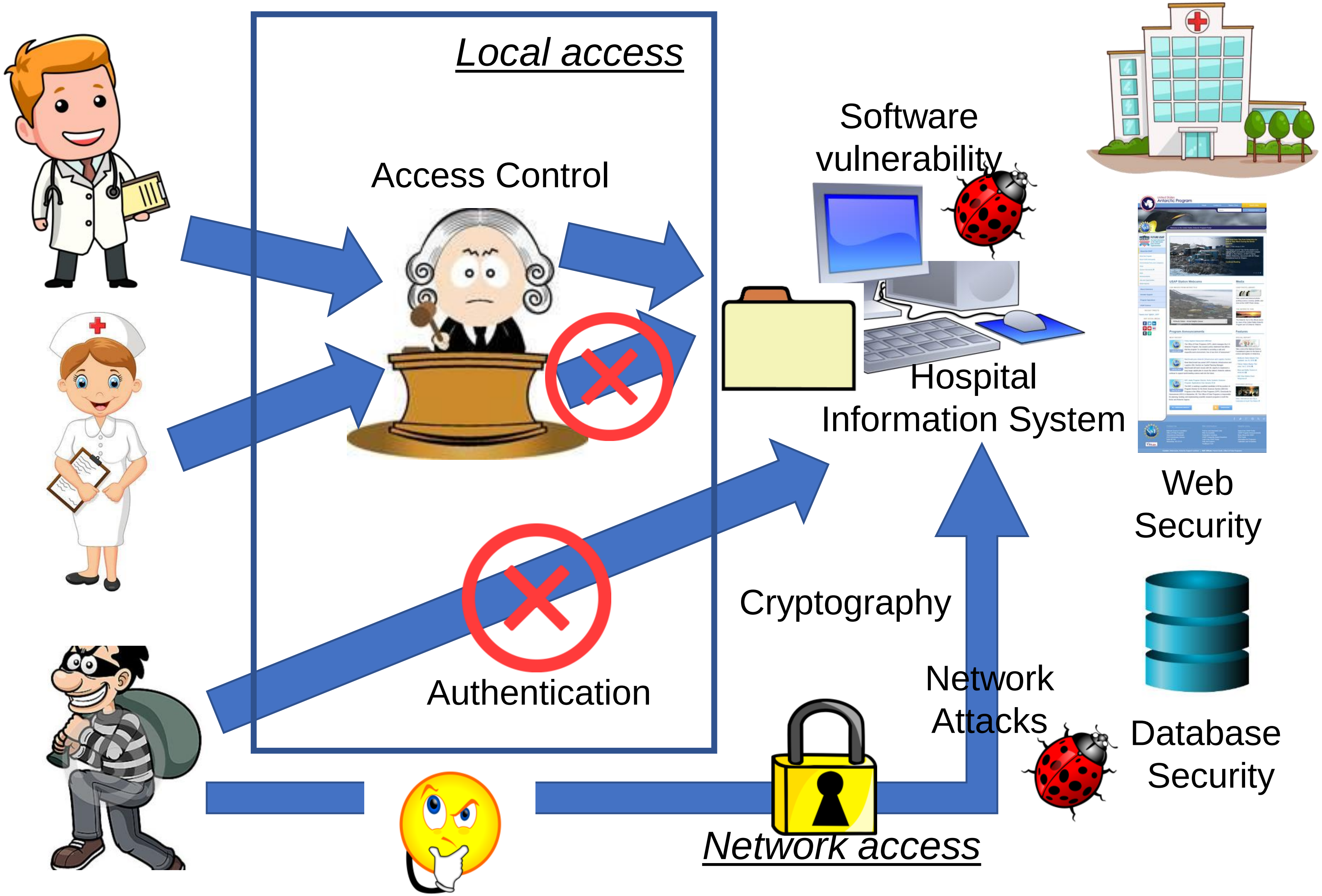
Authentication & Access Control

Code Analysis

Machine Learning

Leo, doctor

Jim, programmer



Authentication

- Definition
  - The act of proving that a user is who she says she is
- Methods:
  - Something the user *knows (password, security questions)*
  - Something the user *is (biometrics)*
  - Something user *has (token)*

Access Control

- Goals
    - Limiting who can access what in what ways
- Access control components
    - Reference monitor
    - Policy storage: access control directory/matrix/list
- Real-world examples
    - Linux permission bits, …

Cryptography

- Goals
  - Protect confidentiality, integrity and authenticity when authentication and access control cannot be performed
- Stream Cipher
  - OTP: key and plaintext are of same size
  - Stream cipher based on PRG: e.g., RC4
- Block Cipher
  - DES, AES, Modes of Operation
- Asymmetric key encryption
  - RSA, key exchange protocols
  - PKI for public key distribution and identity verification
  - Message integrity: cryptographic checksum

Software Security

- Stack: stack frame, registers
- Buffer overflow
  - Malicious data overwrite the return address of current stack frame and with the address of shell code
  - Protection: StackGuard, ASLR, DEP, …
- Other vulnerabilities
  - Integer overflow, race conditions, …
- Malware

OS Security

- OS Provides interface between software and hardware, resource management, protection and isolation
- Memory management
  - Fence register, base/bounds registers
  - Virtual memory: segmentation and paging
  - Contemporary design: MMU, TLB, page protection/presence bit
- Trusted Platform Module (TPM)
- Rootkits

Network Security

- Networks are threatened by attacks aimed at packet interception, modification, fabrication, and interruption
- Attacks depend on layers and protocols
- Data-link layer
  - WiFi: WEP, WPA, WPA2
- Network layer
- Transport layer: Syn flooding, TCP session hijacking
- Application layer: DNS spoofing
- Protection: Protocol (TLS), Tools (Firewall, IDS, VPN)

Web & Database Security

- Browser is the main target of web attacks
- Privacy issues of web
  - User tracking: cookies, device fingerprinting
- Web Attacks
  - Injection attack exploiting JavaScript: XSS, XSRF
- Unique attacks against database
  - Statistical inference attacks: arithmetic (sum, count)
  - SQL Injection

Privacy

- What data is considered private is subjective
- Confidentiality protects what one person considers private
- Privacy laws and act
  - 1974 Privacy Act, GDPR, HIPAA, CCPA
- De-anonymization attacks
  - Defense: differential privacy
- New privacy enhancement technologies: anonymous communication (Tor)

Don’t Forget!

- Final exam
  - 06/12 (Wed) 8-10AM DBH 1429 (same room)
  - Similar format as mid-term, close-book, no calculation-intensive problems, scratch paper provided
- Course evaluation
  - Due 06/09

The Last Slide ☺

- I’m looking for PhD students interested in security & privacy
  - Skills needed: code analysis,
  - My primary research areas: side-channel analysis, Internet measurement, data-driven security analytics, and IoT security
  - More can be found on https://faculty.sites.uci.edu/zhouli/
- I’m advising senior design teams starting from Fall 2019
- If you want to do individual research/study with me
  - A few open slots
  - Let’s talk