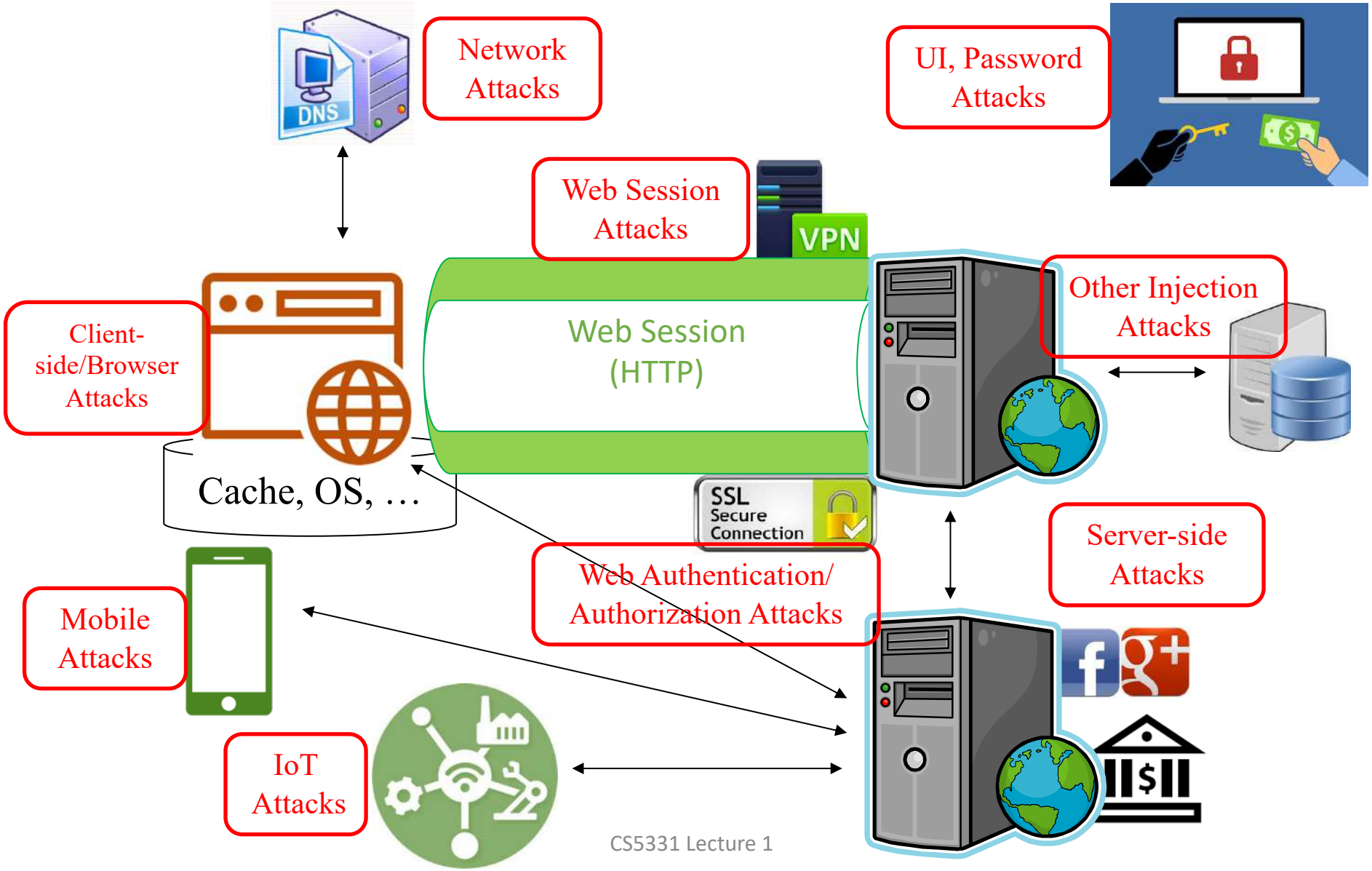
CS5331: Web Security

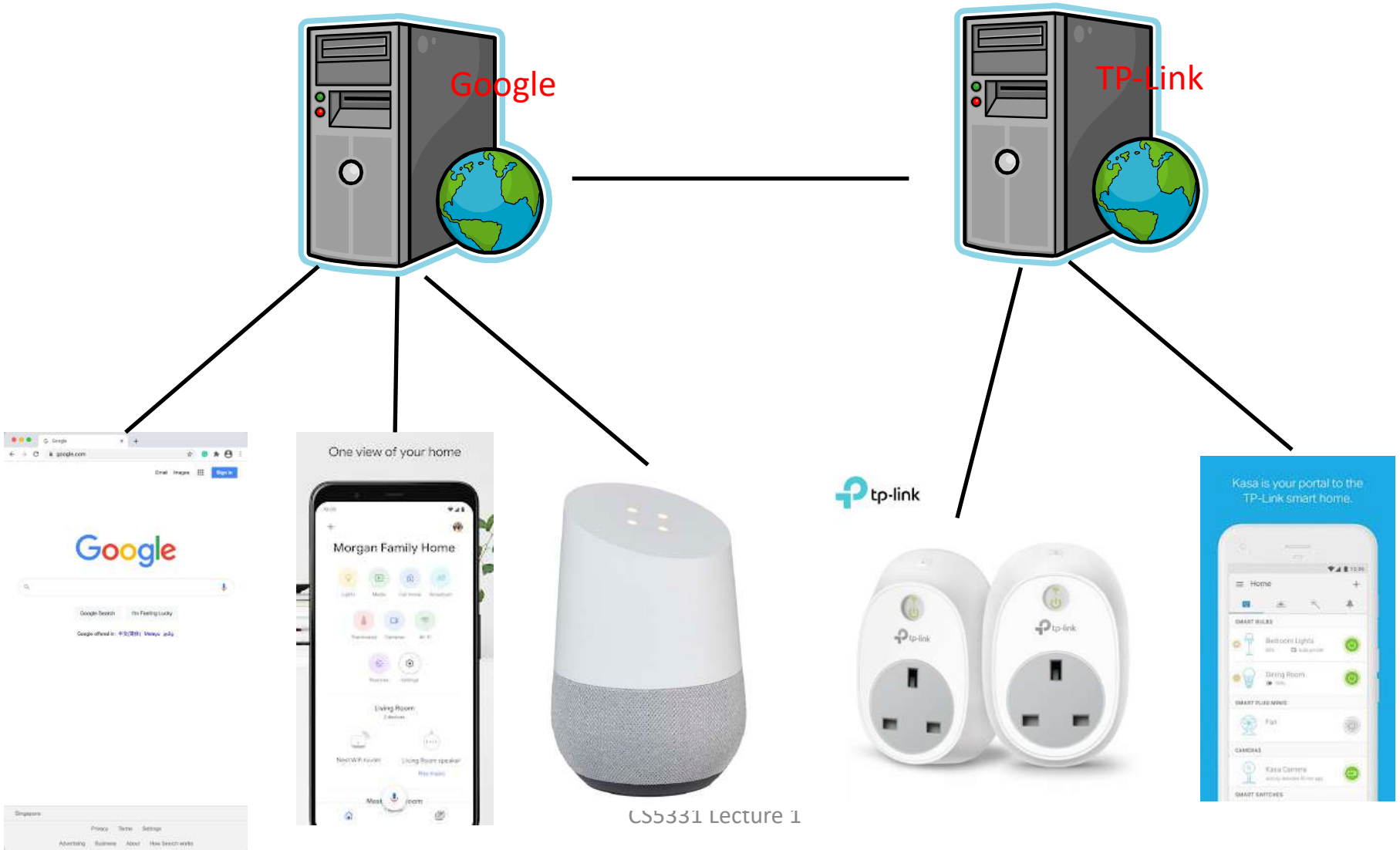
Lecture 10: Beyond Web Systems

Overview of Web Threats



IoT Security

Why are they Web objects?



From Web to IoT. Old Problems

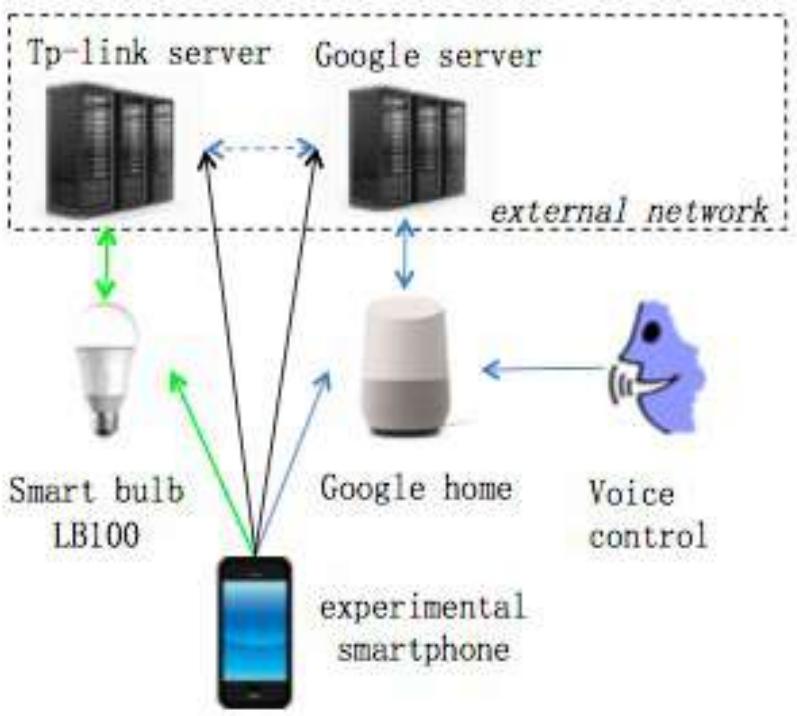
- IoT devices play the role of web clients

Network Attacks

Web Session Attacks

Client-side/Browser Attacks

Mobile Attacks



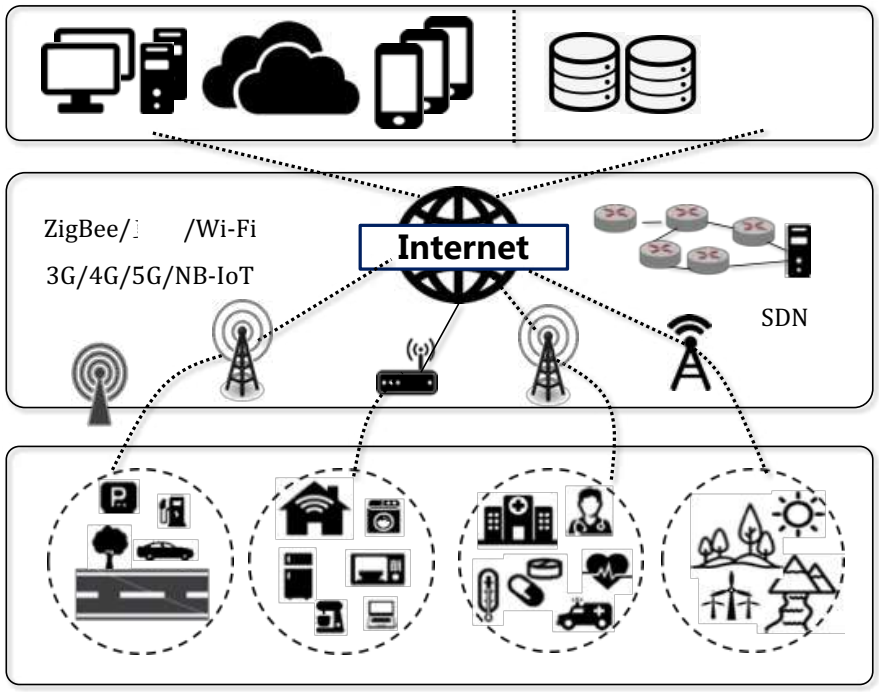
UI, Password Attacks

Other Injection Attacks

Web Authentication/ Authorization Attacks

Server-side Attacks

New Techniques in IoT Domain



- Artificial intelligence， block chain
- Cloud & fog computing
- Big data analysis and mining
- Multi-granularity distributed storage

- NFV/SDN,5G
- Smart routing & data sharing
- Dynamic spectrum access

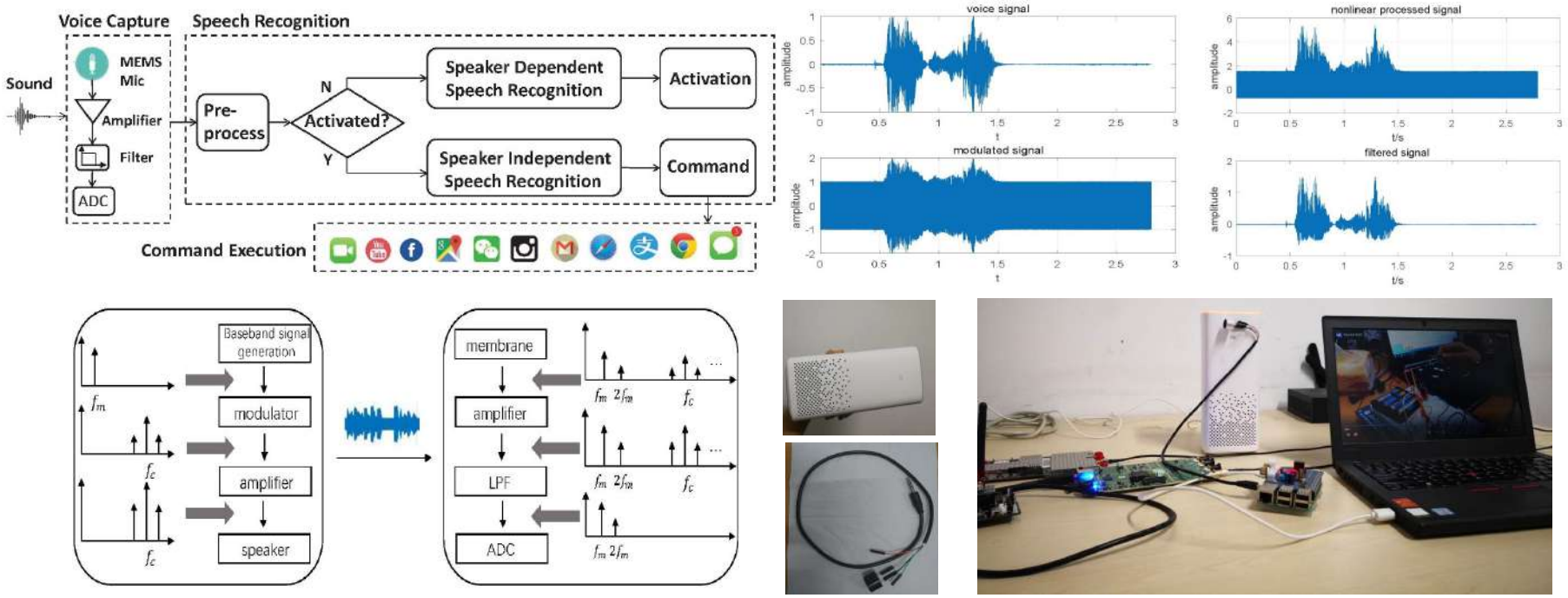
LoRa	470-510MHz
NB-IoT	800/900MHz
WIFI/	2.4GHz
NFC	13.56MHz
ZigBee	868MHz

- Voice activation
- Multisource data fusion
- Crowdsensing & Crowdsourcing
- ……

IoT Security Problems – Device Layer

- Hardware compromise, non-patch
- Signal attack – Dolphin attacks
- Privacy leakage
  - Data transmission, signal level side channel
  - Hardware level side channel

Signal level attack –Dolphin Attacks

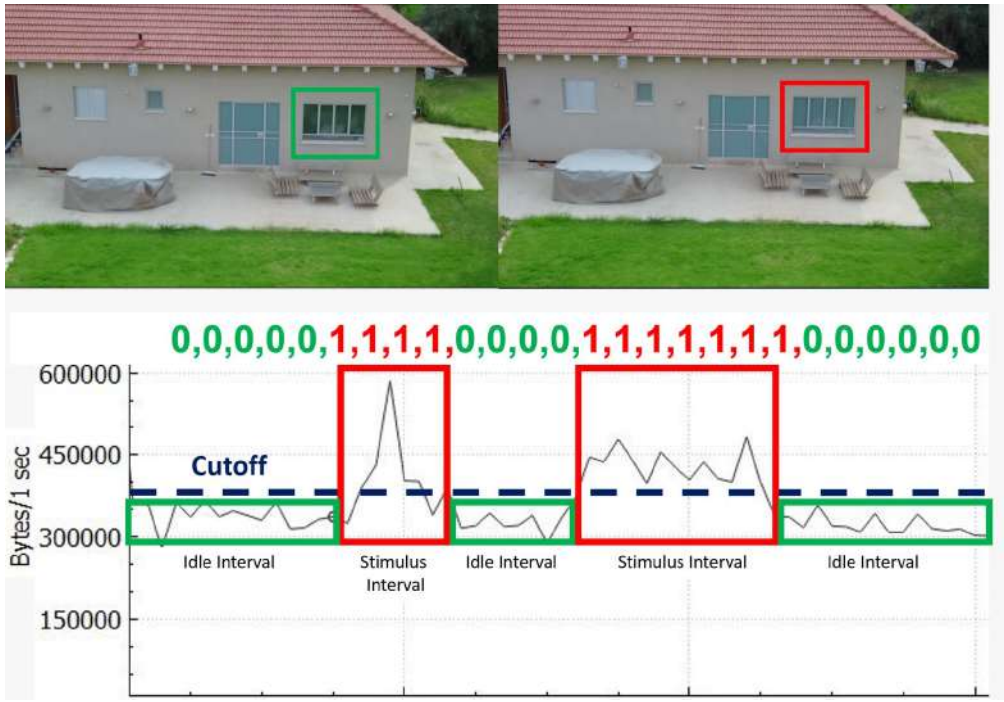


[1] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, and W. Xu, "Dolphinattack: Inaudible voice co mmands," in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communicat ions Security, CCS '17, (New York, NY, USA), pp. 103–117, 2017.

Signal level attack –Dolphin Attack

Defense using Side-Channel

- Check the network traffic of a drone to detect whether it is watching you.



https://www.wired.com/story/a-clever-radio-trick-can-tell-if-a-drone-is-watching-you/

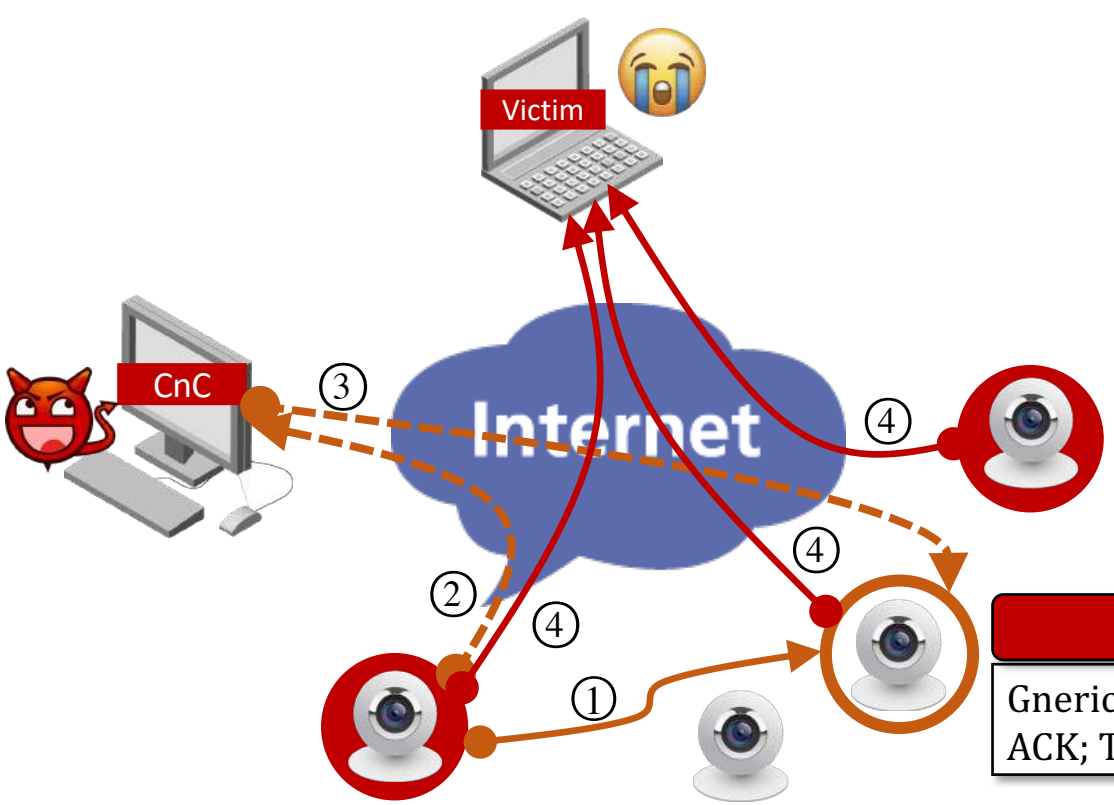
OTA Integrity

- Over the air updates
  - Strictly checked on desktop OS and mobile phones
    - E.g. Apple's online validation of iOS versions
  - Much weaker checking in IoT devices
    - Some vendor has no signature validation at all, over HTTP download
    - Risk of firmware injection/replacement

IoT Security Problems – Network Layer

- Heterogeneous Network
- Traditional network attacks, e.g., DDoS attack, utilize huge amounts of IoT devices –Maria.
- New techniques always have two sides.
  - E.g., SDN, etc.
- Data security – non-encryption, side-channel

Maria Attack



Attack steps

1. Existing BOT discovers new open devices
2. Details are sent to CnC
3. CnC copies virus in new devices
4. CnC commands the BOTs to attack a vicitm

Miria attack vectors

Gneric UDP; VSE; DNS; Plain UDP; TCP SYN; TCP ACK; TCP STOMP; GRE IP; GRE Ethernet; HTTP

IoT Security Problems – Application Layer

- Web security – Phishing, XSS, SQLi
- Cloud security – data integrity, confidentiality
- Android Security
  - Least privilege
  - Separation of privilege
  - Malware
- Information leakage from Big DATA
- Security risks introduced by AI
- Access control - Over privilege problem

Future of Web

What is after Web 1.0 and Web 2.0?

- Web 1.0
  - Web 1.0 is a retronym referring to the first stage of the World Wide Web's evolution, from roughly 1991 to 2004
- Web 2.0
  - Web architecture, from 2004 to 2010
- Web 3.0, or Web3?
  - What is the difference between Web3 and Web 3.0?
    - Java to JavaScript?
  - *Submit your questions for an open discussion next week*