Security in IoT

DAT159 – IoT/Cloud Module

Tosin Daniel Oyetoyan
13.11.2018

Practical Information

- Lecture until 11:10
- Explain Assignment 3 (5-10mins)
- Assignment 2: Help, Demonstrate and Approve

Resources for further reading

- Fink, G. A. et al.(2015). **Security and privacy grand challenges for the Internet of Thing**s. In IEEE International Conference on Collaboration Technologies and Systems (CTS), (pp. 27-34). (pdf available on Canvas)
- Zhang, Z. K. et al. (2014). **IoT security: ongoing challenges and research opportunities**. In 7th IEEE International Conference on Service-Oriented Computing and Applications (SOCA), (pp. 230-234). (pdf available on Canvas)
- Khalil, I. M., Khreishah, A., & Azeem, M. (2014). **Cloud computing security: A survey**. *Computers*, *3*(1), 1-35.
- Faruki, P., et al. (2015). **Android security: a survey of issues, malware penetration, and defenses**. IEEE communications surveys & tutorials, 17(2), 998-1022.
- Brundage, M., et al. (2018) **The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation**

Content

- Motivation
- IoT properties
- Security requirements for IoT
- Challenges of IoT Security
- Security Threats
- Inspirational video

Security & Privacy issues

- CIA Chief: We'll Spy on You Through Your Dishwasher

How to Hack a Cisco IP Phone:

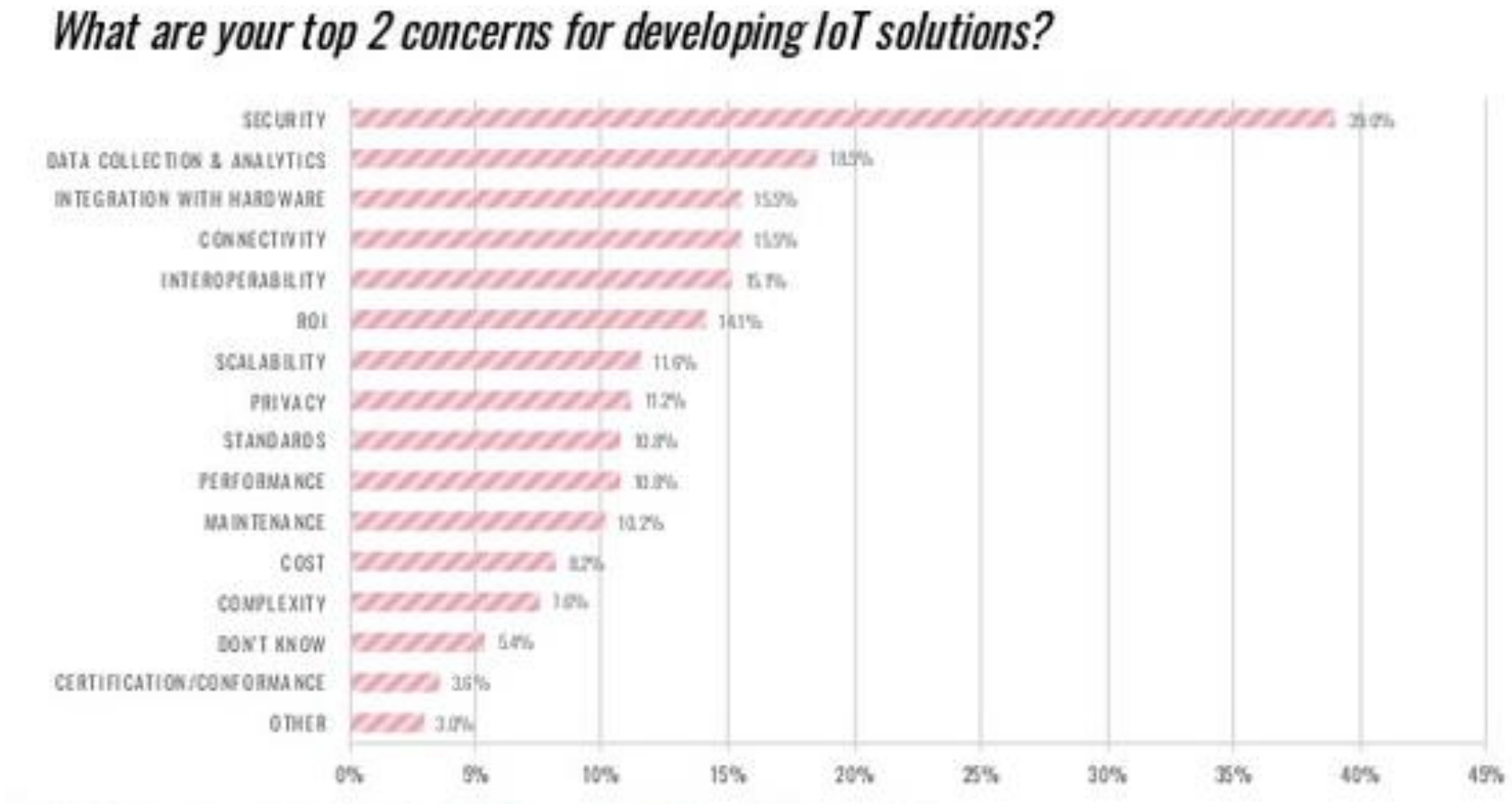
Columbia computer scientist Ang Cui helped uncover a weakness in Cisco IP phones that can let a hacker take complete control of them

BMW ConnectedDrive hack sees 2.2 million cars exposed to remote unlocking

With the rise of the "smart home," you'd be sending tagged, geolocated data that a spy agency can intercept in real time when you use the lighting app on your phone to adjust your living room's ambiance

“Embedded devices, generally speaking, are very poorly secured, if they are secured at all” - Kurt Stammberger (V.P. Monaco, San Francisco)

Security in IoT – A Major Concern



Eclipse IoT Developer Survey 2018
https://www.slideshare.net/kartben/iot-developer-survey-2018

Lots of Reconnaissance & Analysis Tools

- shodan.io – IoT vulnerability scanner
- https://binary.ninja/ - disassembler/decompiler
- https://github.com/greatscottgadgets/ubertooth/wiki - bluetooth sniffer
- https://github.com/ReFirmLabs/binwalk - Reverse engineering
- https://www.qemu.org/ - processor emulation
- https://www.ettercap-project.org/ - MiTM Attacks
- https://www.wireshark.org/ - Packet inspection/protocol analyzer
- https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project - HTTP protocol analyzer (Proxy)
- https://www.kali.org/ - Penetration framework
- https://www.metasploit.com/ - Penetration framework

Attacker and Attacker Goal

Attacker

- Script-kiddies
- Disgruntled or sacked employees
- Activists
- Terrorists and politically-motivated groups
- State Actors

Attacker Goal

- Theft
  - Steal and acquire resources to use extort money (Anonymous crime-as-a-service)
  - Steal confidential information to extort money
- Vandalism
  - Cause harm ()
- Sabotage
  - Undermine credibility, disable operation, force out business

IoT Potentials and Security

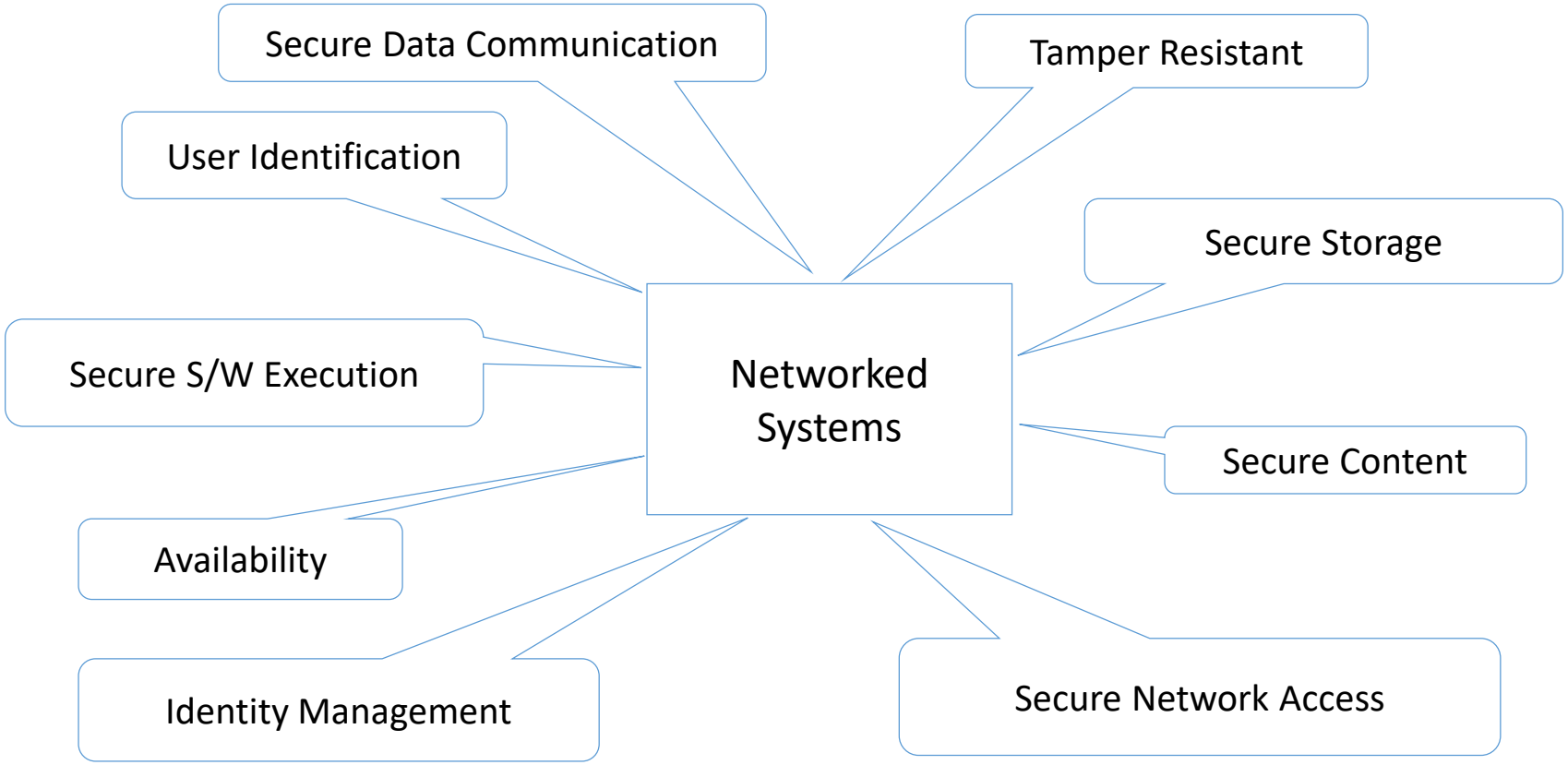
IoT will create many possibilities for services and values for

- Users (smart cities, smart energy, smart ocean, smart transport,)
- Criminals
  - Cybercrime (Crime as a Service (botnets, DDoS, cryptocurrency mining,)
    - Selling your information for profit
    - monetizing and offering DDoS services
    - botnet rentals in underground markets
      - e.g. renting 100 bots in the Chinese underground is pegged at US$24 in 2015;
      - in the French underground in 2016, botnet rental of 100-150 bots per day is at €95 (or US$102.19).
      - https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/securing-routers-against-mirai-home-network-attacks
  - Breaches of privacy (Organisations, Governments, etc)
  - Physical safety in the home, across the city and within businesses
  - Threats to national infrastructure (Power Grid, Transport, Defense)
- App platforms in the cloud or at the network edge will be targets for attacks

Critical Infrastructures & Others

- Energy Sector
  - DDoS
  - Smart met**er**: Monitor home user consumption patterns (user profiling)
  - Smart-Home: Linux Worm targets Internet-enabled Home appliances to Mine Cryptocurrencies
    - https://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html
- Transportation system
  - Single Connected Car Can Trick Smart Traffic Lights Into Causing Intersection Clogging
    - https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/connected-car-can-trick-smart-traffic-lights-causing-intersection-clogging
- Environmental system
  - https://www.cnet.com/news/hacker-says-he-broke-into-texas-water-plant-others/
- Privacy
  - https://www.cnet.com/news/smart-toys-have-big-security-flaws-consumer-report-finds/
  - https://www.cnet.com/news/your-smart-camera-may-have-been-spying-on-you/

Security Requirements



IoT Property

- Heterogenous components
  - Systems
  - standards and protocols
  - O/S
  - Programming languages
- Connectivity
  - Systems of systems

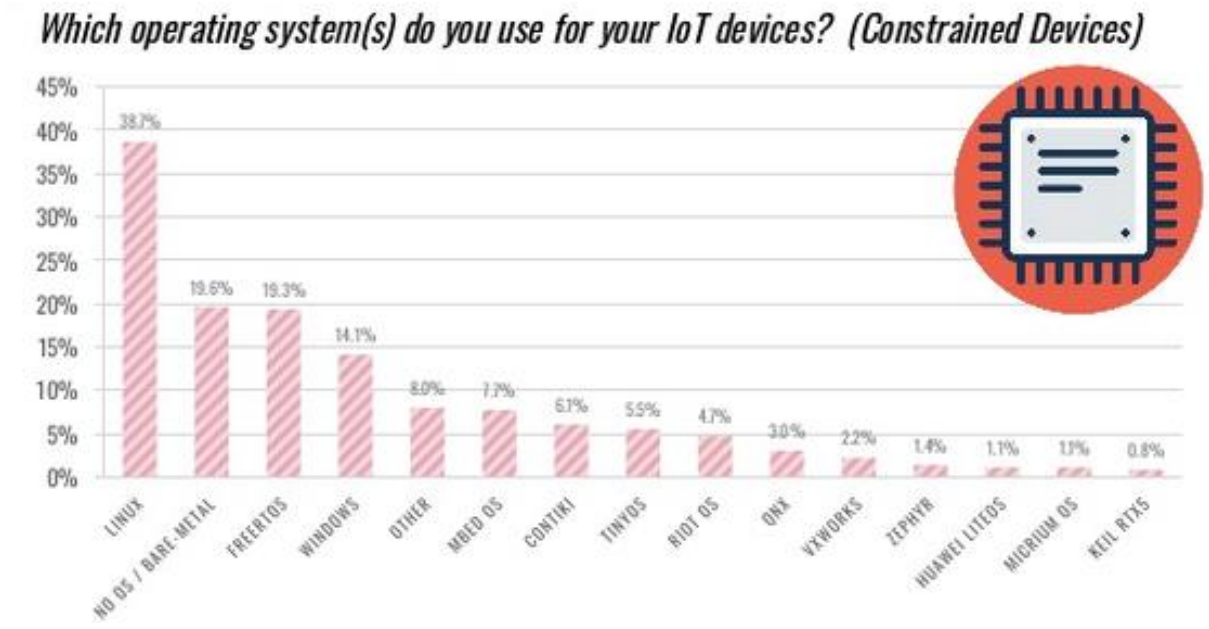
Property #1 - Heterogenous components

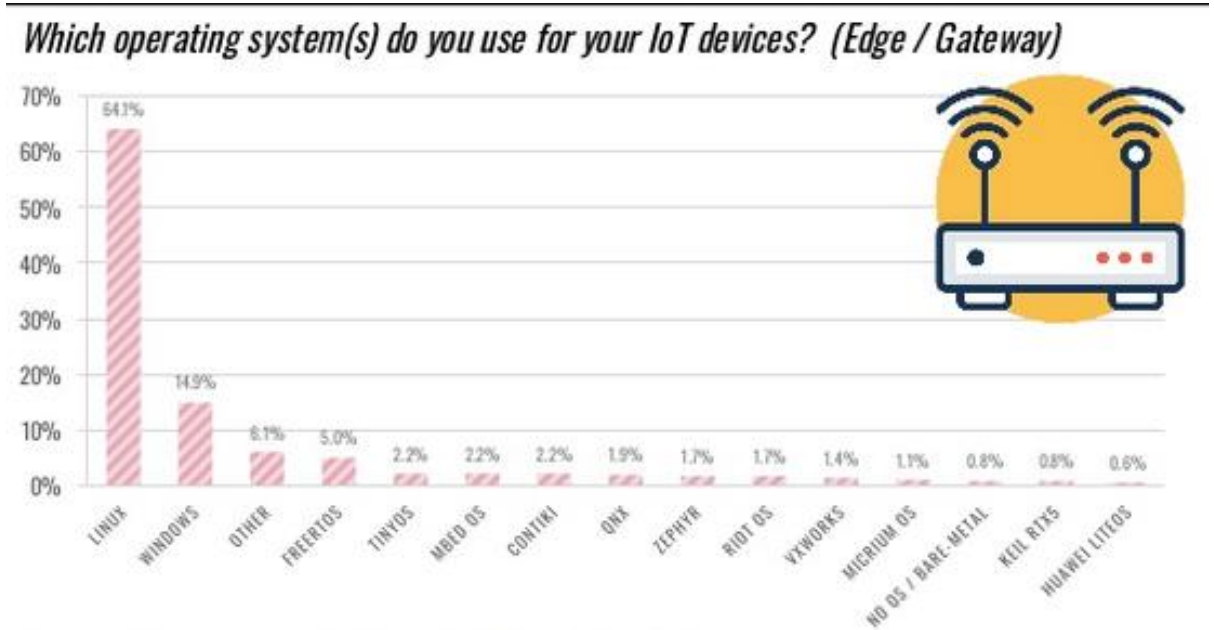
- Tiny sensors, Hardware or Embedded devices
- Firmware
- Web applications
- Mobile applications
- Cloud assets
- Communication technologies

Property #1 – Many Standards and protocols

- **Infrastructure** (ex: 6LoWPAN, IPv4/IPv6, RPL)
- **Identification** (ex: EPC, uCode, IPv6, URIs)
- **Comms / Transport** (ex: Wifi, Bluetooth, LPWAN)
- **Discovery** (ex: Physical Web, mDNS, DNS-SD)
- **Data Protocols** (ex: MQTT, CoAP, AMQP, Websocket)
- **Device Management** (ex: TR-069, OMA-DM)
- **Semantic** (ex: JSON-LD, SensorML, Web Thing Model)
- **Multi-layer Frameworks** (ex: Alljoyn, IoTivity, Weave, Homekit)

Property #1 – Many OS

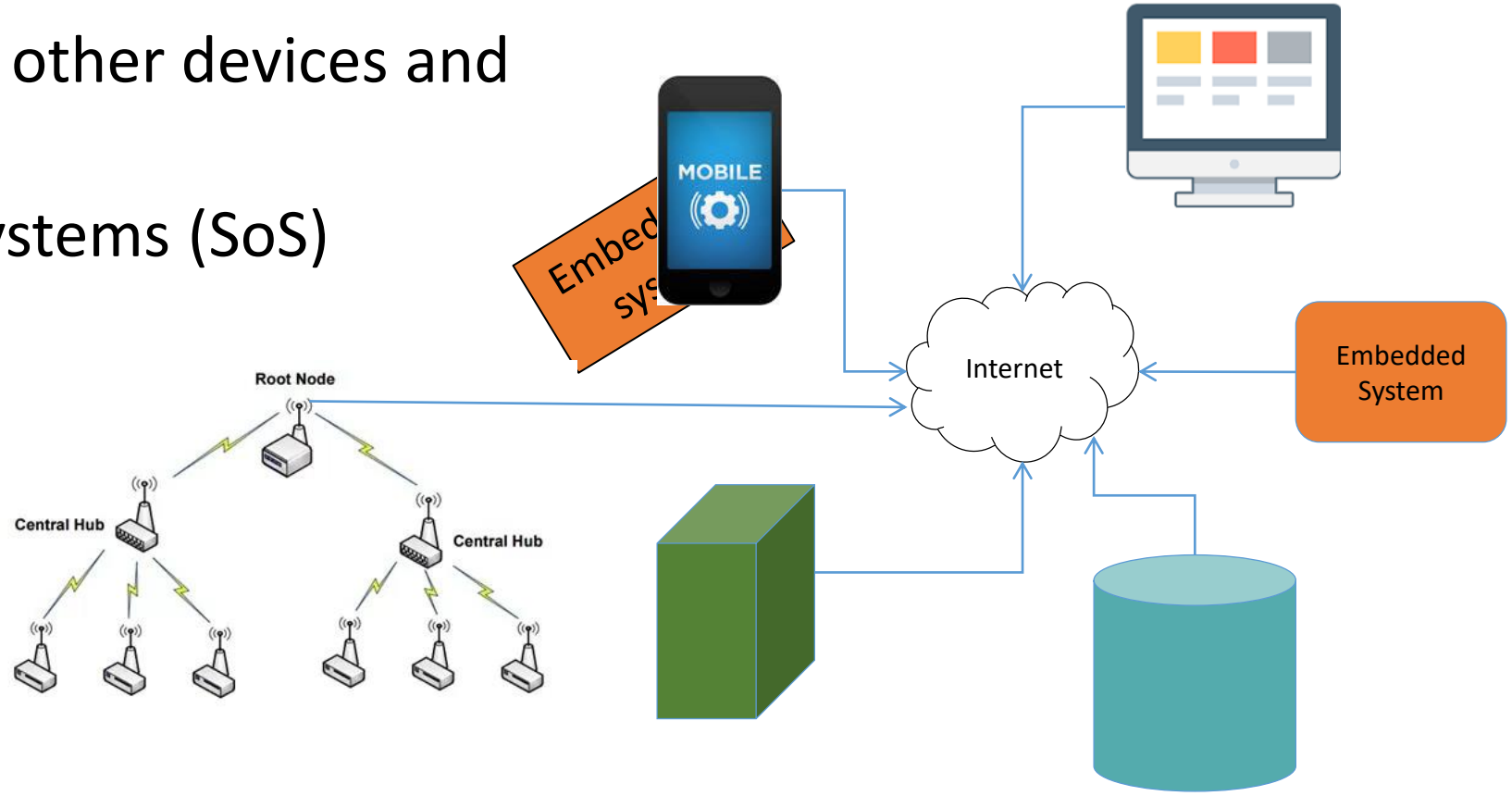




e.g. Linux Worm targets Internet-enabled Home appliances to Mine Cryptocurrencies
https://thehackernews.com/2014/03/linux-worm-targets-internet-enabled.html

Property #2 - Connectivity

- Connected to other devices and systems
- Systems-of-Systems (SoS)



Security Challenges – Standards/Protocols

- Protocols differ according to manufacturer choices
- Unexpected combination of standards in a IoT ecosystem
- Subtle differences between protocols are excellent places to find cyber exploits

Security Challenges – Data Privacy

- Location data
- Audio data
- Video data
- Vehicles
- Digital Identity
- Other personal data
- How are you connected to IoT?
  - Wearable technologies
    - Smart watch

Security Challenges – Insecurity by design

- Constrained devices
  - Memory
  - Power
  - Computation
- Security solutions with traditional computers are too heavy
  - e.g. Cryptography algorithm – computationally intensive

Security Challenges – Difficulty to patch

- IoT devices in hard-to-reach locations
  - Human body (Pacemaker)
  - Remote desert
  - Underground
- Fixing, Upgrading, Patching
  - Anything that is exposed to the Internet must be securely software upgradable

https://www.networkworld.com/article/3222651/internet-of-things/fixing-upgrading-and-patching-iot-devices-can-be-a-real-nightmare.html

Security Challenges - Very Large Attack Surfaces

- Every components of IoT is a potential attack surface
  - Cloud
  - Iot device
  - Thin/Thick clients
  - Communication

Security Challenges - Very Large Attack Surface

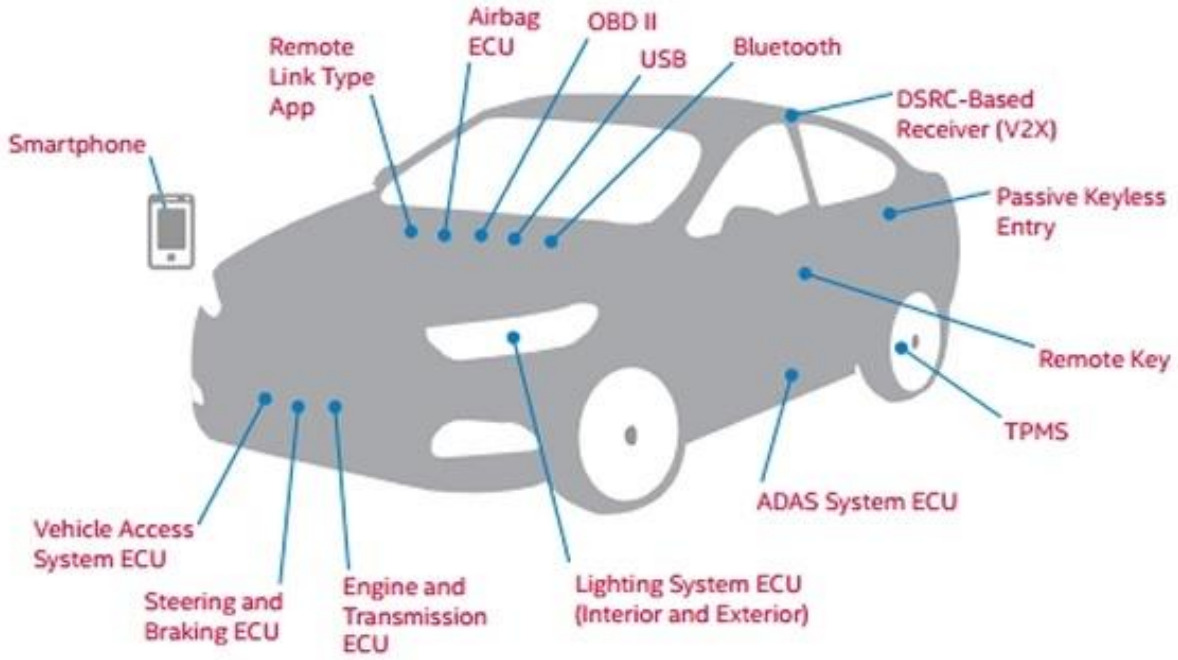
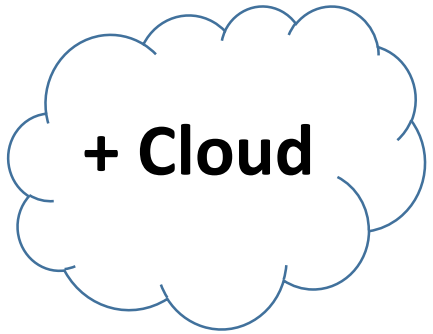


Figure 2. Fifteen of the most hackable and exposed attack surfaces on a next-generation car.

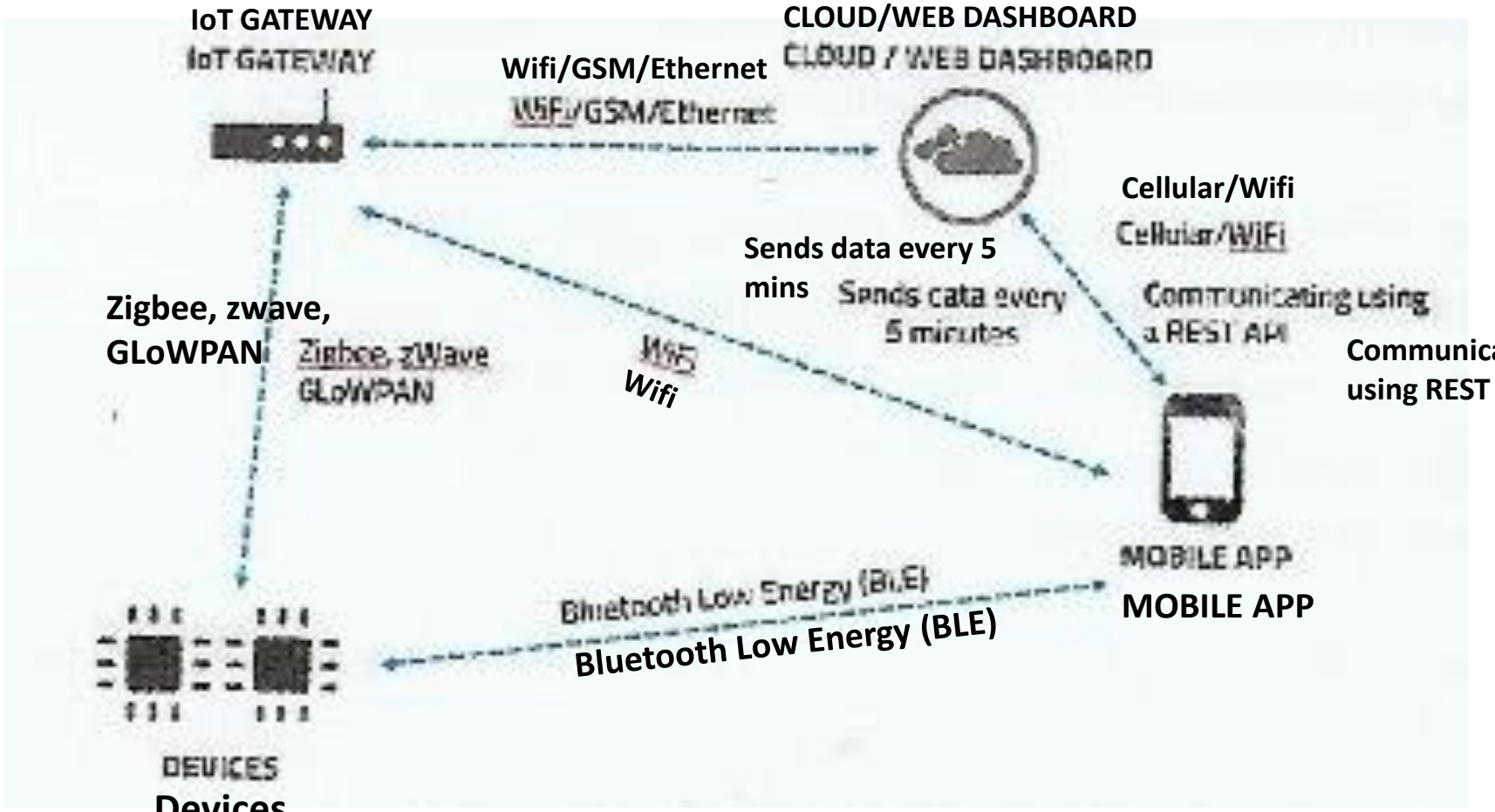
Source: http://www.wheels24.co.za/News/Cyber-threat-15-ways-your-car-can-be-hacked-20150915



Smart Car Example

Charlie Miller and Chris Valasek. "Remote Exploitation of an Unaltered Passenger Vehicle". August 10, 2015

Security Challenges - Very Large Attack Surface

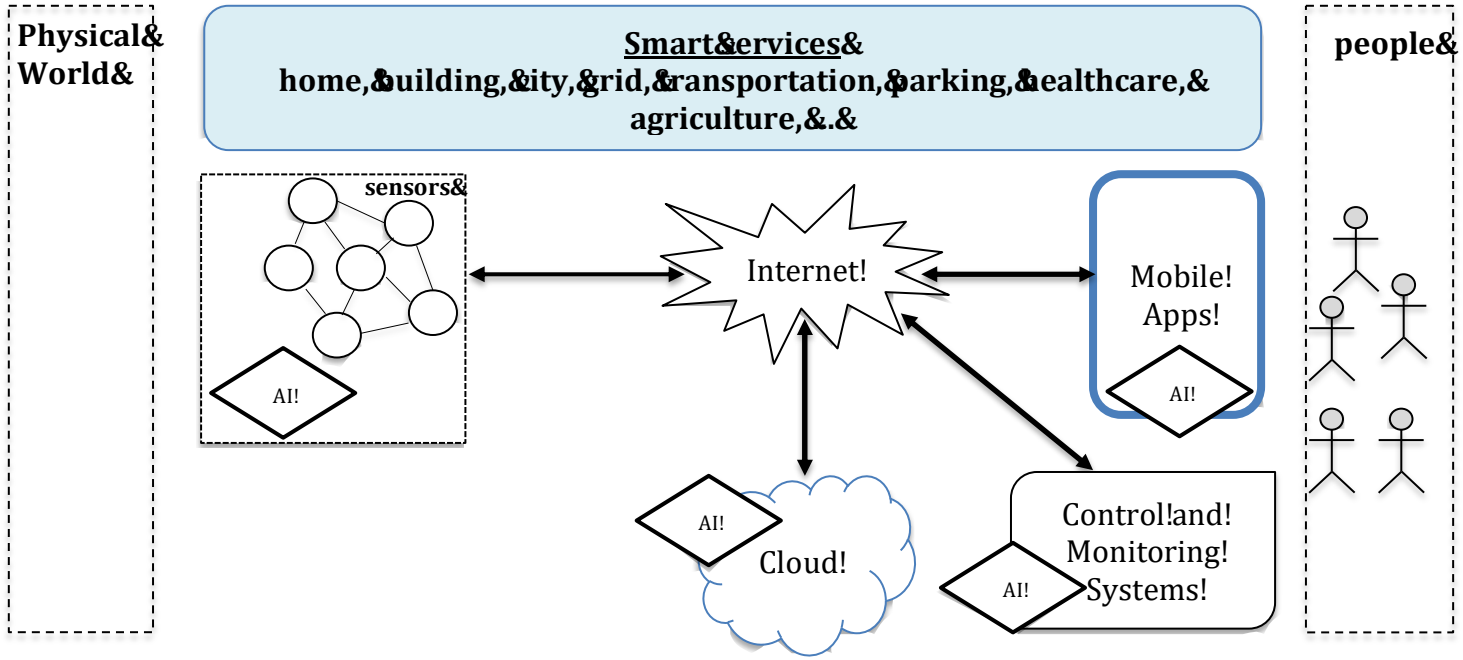


Source: Hacking IoT Devices

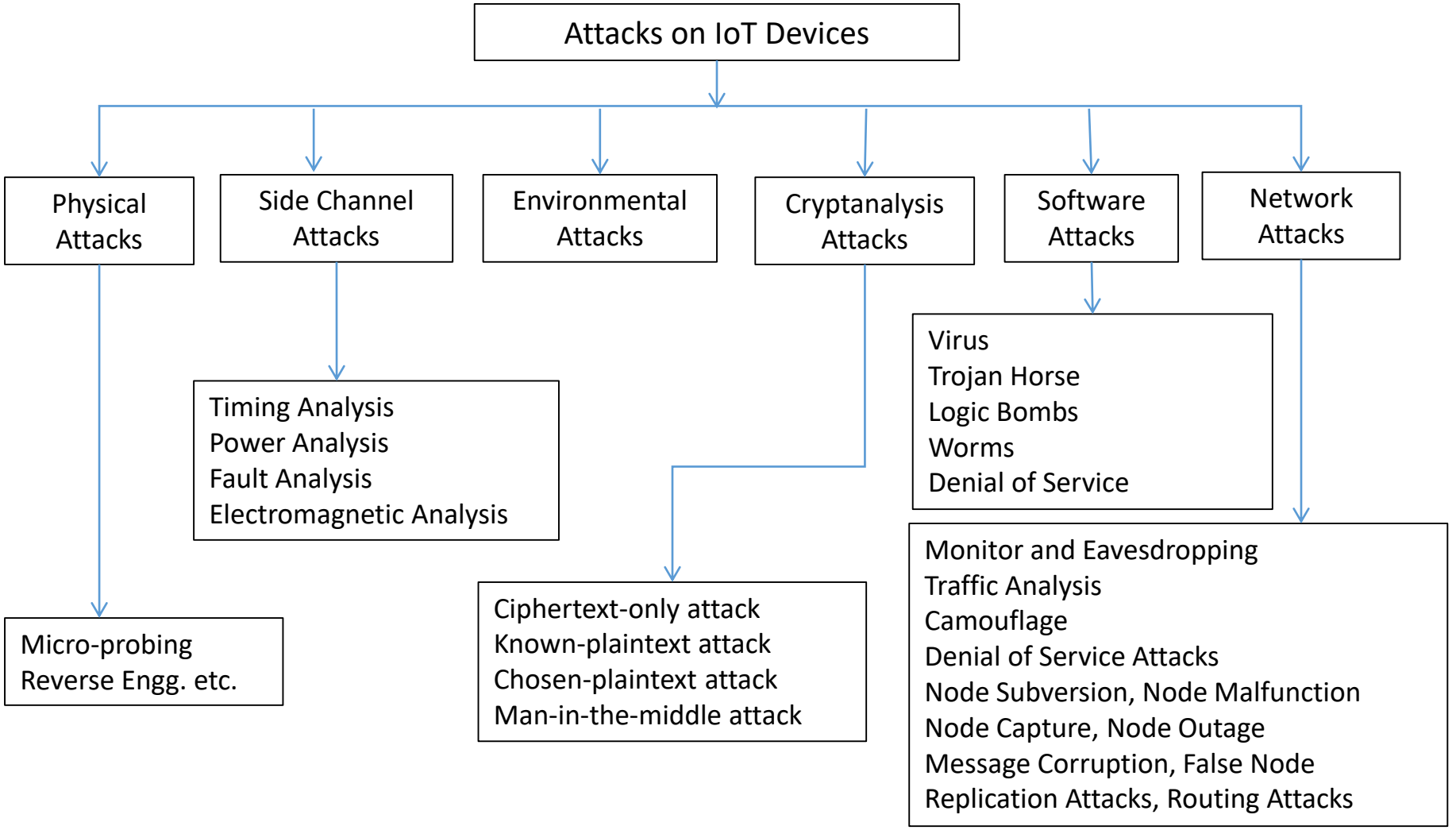
Smart Home Example

Attacks/Threats Dimensions

- IoT/Gateway Devices
- Cloud systems
- Smartphones
- AI-enabled
  - 'smartness'
- Communications



Threats to IoT Devices



Security in Cloud Computing

- Affected by typical Web vulnerabilities (e.g. OWASP Top 10)
- In addition to weaknesses in
  - Cloud infrastructure implementation

2017 OWASP Top-10 Risks

Risk	Description
A1:2017-Injection	SQL, NoSQL, OS, and LDAP injection), -untrusted data is sent to an interpreter as part of a command or query. Unauthorized execution
A2:2017-Broken Authentication	Incorrect implementation of authentication and session management -compromise passwords, keys, or session tokens
A3:2017-Sensitive Data Exposure	Improper protection of sensitive data, such as financial, healthcare, and PII -encryption (weak) rest/transit
A4:2017-XML External Entities (XXE)	evaluate external entity references within XML documents (XML Parsers).
A5:2017-Broken Access Control	access unauthorized functionality. Restrictions on what authenticated users are allowed to do are often not properly enforced
A6:2017-Security Misconfiguration	insecure default configurations -incomplete or ad hoc configurations

OWASP Top-10 Risks

Flaw	Description
A7:2017-Cross-Site Scripting (XSS)	**untrusted data**. execute scripts. hijack user sessions, deface web sites, or redirect
A8:2017-Insecure Deserialization	remote code execution. including replay attacks, injection attacks, and privilege escalation attacks
A9:2017-Using Components with Known Vulnerabilities	libraries, frameworks, and other software modules, run with the same privileges as the application
A10:2017-Insufficient Logging&Monitoring	ineffective integration with incident response. Most breach studies show time to detect a breach is over 200 days. Detected by external parties

Example of Attacks on Cloud

Denial-of-service	Service/Hardware unavailable (http-based/xml-based ddos)
Cloud malware injection	Service instance of victim is infected. Credential information leakage, user data leak
Cross VM side channels	VMs on same physical machine. Data/info/resource leak (Computation Time of certain processes/Energy consumption side channels)
Botnets	Unauthorized access to cloud resources, steal sensitive data
VM rollback attack	Brute force attack, damage cloud infrastructure, leak sensitive information

Khalil, I. M., Khreishah, A., & Azeem, M. (2014). Cloud computing security: A survey. *Computers*, *3*(1), 1-35.

Security in Smartphones

- Personalized services
- Smartphones will be central for most utility services around IoT
  - Will be used for monitoring/sending control signals

Threats to Smartphones

- **Dangerous apps**
- **Exploiting weaknesses in legitimate apps**

- Accidental exposure of functionalities
- Send data to wrong recipients
- Validation problems

CVE-2016-6256 XML External Entity(XXE) attack
SAP Business One Android Application

Examples of Attacks on Smartphones (Android)

Privilege elevation	Exploiting kernel vulnerabilities to gain root access
Privacy leakage/PI theft	Users grant dangerous permissions to malicious apps
Spying/Sniffing	Monitoring voice calls, sms, transactions, unauthorized recording audio/video
Botnet	Remote control and exploitation
Colluding attack	Set of apps signed with same certificates causing them to share UID

Faruki, P., et al. (2015). Android security: a survey of issues, malware penetration, and defenses. IEEE communications surveys & tutorials, 17(2), 998-1022.

Known Attacks on Smartphones (Android)

Denial of service

Design to overuse resources: CPU, memory, battery, bandwidth to deny users from normal operations

Threats from Artificial Intelligence

- Expansion of existing threats.
  - Enable large scale attacks
  - The costs of attacks may be lowered by the scalable use of AI systems to complete tasks that would ordinarily require human labor, intelligence and expertise.
- Introduction of new threats.
  - New attacks may arise through the use of AI systems to complete tasks that would be otherwise impractical for humans.
  - Malicious actors may exploit the vulnerabilities of AI systems deployed by defenders.
- Change to the typical character of threats.
  - Growing use of AI is projected to be especially effective, finely targeted, difficult to attribute, and likely to exploit vulnerabilities in AI systems.

- Brundage, M., et al. (2018) The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation
- Allen, G., & Chan, T. (2017). Artificial Intelligence and National Security. Belfer Center for Science and International Affairs.

Threats from Artificial Intelligence

- data poisoning attacks
  - introducing training data that causes a learning system to make mistakes
- adversarial examples
  - inputs designed to be misclassified by machine learning systems
- exploitation of flaws in the design of autonomous systems' goals
- Trained features could be removed/replaced if systems are compromised
- Single point of failure

Inspiration

- https://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked
- https://www.nist.gov/video/what-internet-things-iot-and-how-can-we-secure-it

Assignment 3

- https://github.com/lmkr/dat159/blob/master/week3.md

Practice questions

- Why do you think security is challenging with IoT revolution?
- Explain 2 challenges that make security complex in IoT landscape
- Mention and discuss briefly 3 security threats to IoT systems
- Explain 3 ways you know to secure IoT systems