Ch. 14 - IoT Security and Privacy

Sec 1 – Introduction

COMPSCI 244p

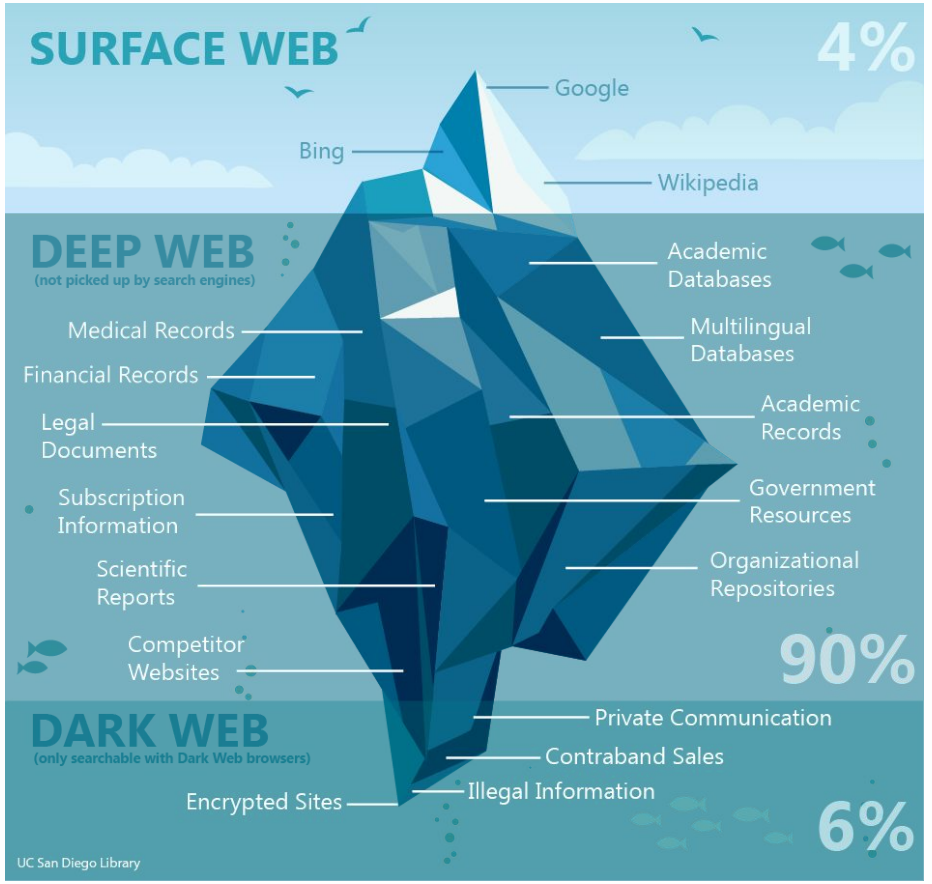
Internet-of-Things; Software and Systems

CONTENT

- Intro to Web and IoT Security and Privacy
- IoT Security Challenges
- IoT Security Requirements
- IoT Domain Architecture
  - Cloud Domain
  - Fog Domain
  - IoT Sensing Domain

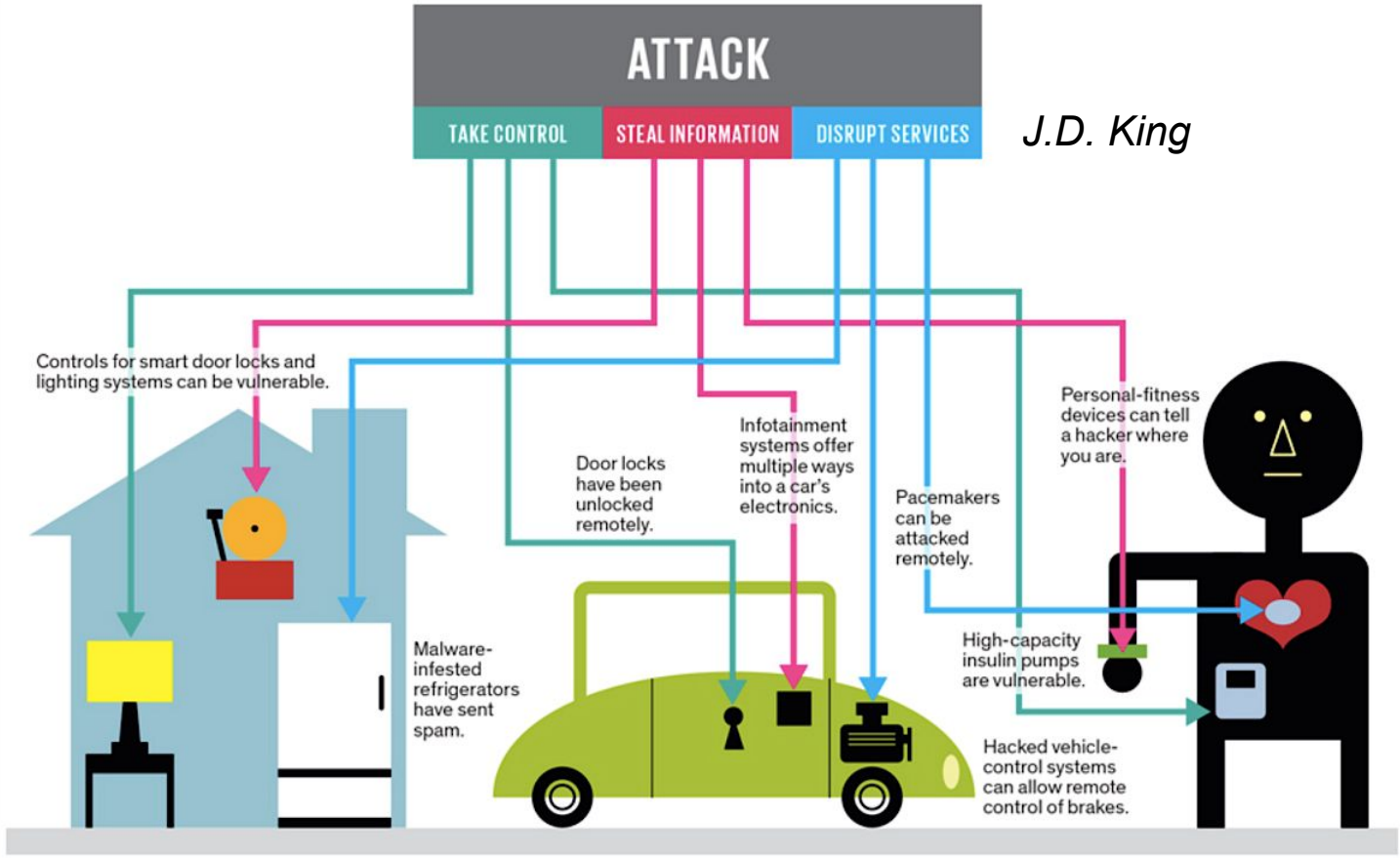
Intro to IoT Security and Privacy

- The benefits that IoT brings are associated with **new security risks and privacy** issues



Intro to IoT Security and Privacy II

- The damage caused by cyber-attacks in the IoT era will have a **direct impact** on all the **physical objects** that you use in your daily life.
  - E.g., controlling the door lock, the brakes and the steering wheel of your car
  - E.g., controlling remotely the implantable and wearable health devices
    - Doctors disabled the wireless capability of **Dick Cheney**'s pacemaker.



J.D. King

Intro to IoT Security and Privacy III

- Privacy in IoT is crucial
  - **Learning** about **people's life** by **eavesdropping** on the sensed data
    - E.g., from smart house appliances and wearable devices
  - Facial, speech, and human activity recognition amplify the amount of information that the sensed data can reveal
  - An outsider can even learn about your personal life when aggregating the **metadata from multiple hacked objects**
    - IoT Metadata aggregation examples projects:

The Energy Channel

IoT Security Challenges

- Multiple Technologies
  - IoT combine multiple technologies (e.g., RFID,WSN, cloud computing, virtualization).
  - Each having its own vulnerabilities.
  - The chain of all these technologies needs to be secured.
  - **Security is judged based on the weakest point (i.e., Achilles' heel)**
- Multiple Verticals
  - Numerous applications (i.e., verticals).
    - eHealth, industrial, smart home gadgets, smart cities
  - Security requirements of each vertical are quite different.

IoT Security Challenges II

- Scalability
  - Billion of devices
  - **Centralized** defensive frameworks cannot work anymore
- Big Data
  - The generated data will be also enormous
  - Each smart object will be supplied by numerous sensors
  - Secure large streams of data
- Availability
  - Continuously operational for a desirably long period of time
  - "**five 9s**" availability (99.999 % of the time in a given year)
  - Network **administrators** hesitate to use needed threat response technology functions
  - Add **redundancy** to systems may help

IoT Security Challenges III

- Resource Limitations
  - Recourse-constrained devices are low-hanging fruits for denial-of-service (DoS) Attacks
    - **Overwhelming** the limited resource capabilities of these devices or sending data to crash the system.
  - Traditional cryptography techniques are **computationally expensive**
- Remote Locations
  - Some IoT devices may be installed in unmanned locations
  - **Cyber** and **physical** security monitoring systems must be installed in safeguarded location
- Mobility
  - Extra difficulties when developing defensive mechanisms in dynamic environments
- Delay-Sensitive Service
  - Many IoT applications are expected to be delay-sensitive
  - Protection against degrading the service time

IoT Security Requirements I

- Confidentiality
  - The exchanged messages can be **understood only** by the **intended entities**
- Integrity
  - The exchanged messages were not **altered/tampered** by **a third party**
- Availability
  - The service is not interrupted. **DoS** attacks target this requirement
- Authentication
  - Entities involved in any operation are indeed who they claim to be
- Authorization
  - Entities have the required **control permissions** to perform the operation they request to perform

IoT Security Requirements II

- Freshness
  - The data is fresh.
  - **Replay** attacks target this requirement where an old message is replayed in order to return an entity into an old state.
- Non-repudiation
  - An entity cannot deny an action that it has performed.
- Forward Secrecy
  - When an object leaves the network, it will not understand the communications that are exchanged after its departure.
- Backward Secrecy
  - Any new object that joins the network will not be able to understand the communications exchanged prior to joining.

IoT Three-Domain Architecture

- Cloud Domain
  - performing the heavy-computational processing operations.
- Fog Domain
  - performs operations on the collected data including aggregation, preprocessing, and storage.
- IoT Sensing Domain
  - smart objects that are expected to change their location over time.