12. Mobile Devices and the Internet of Things

Blase Ur, May 3rd, 2017
CMSC 23210 / 33210

THE UNIVERSITY OF CHICAGO
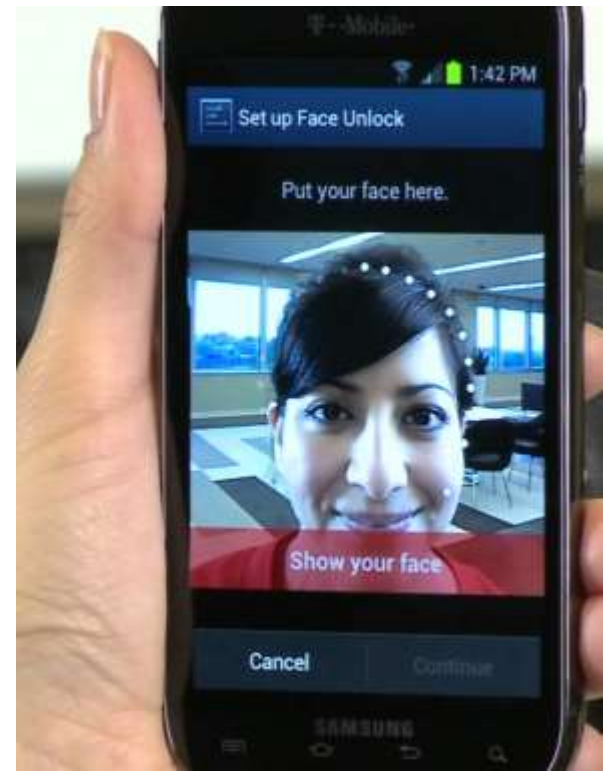
SUPER GROUP
UCHICAGO

Security, Usability, & Privacy
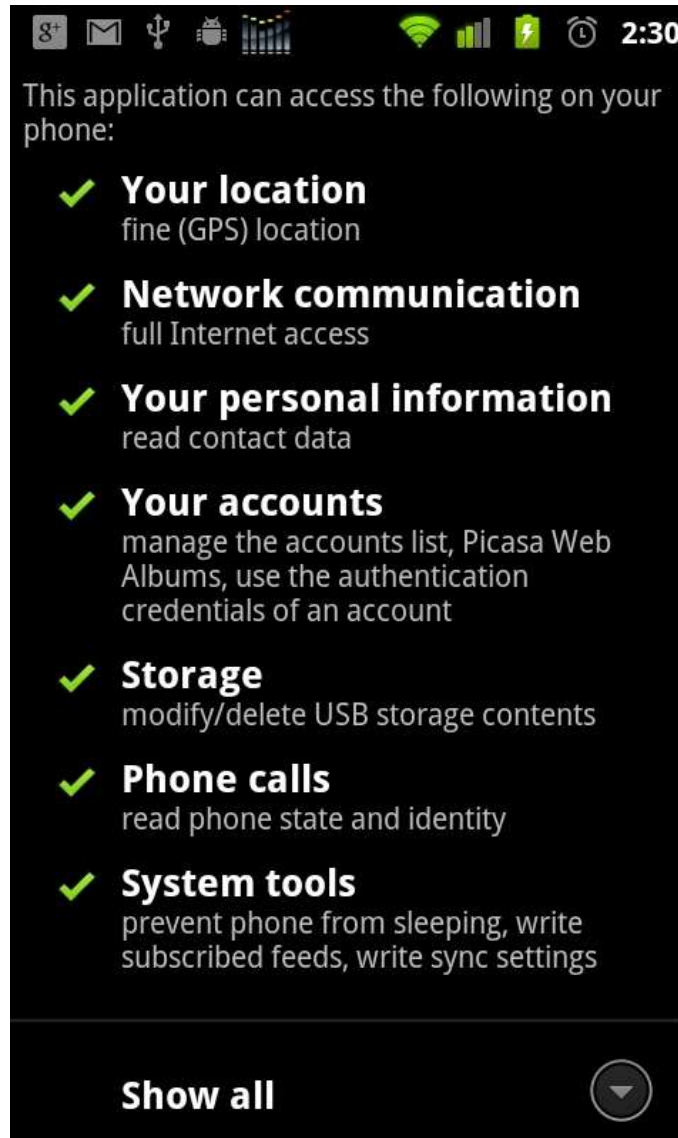Education & Research

Today's class

- Security and privacy for:
  - mobile devices
  - the IoT
  - safety-critical devices
- Discuss midterm

Mobile Devices

Authentication

Permissions Model for Apps

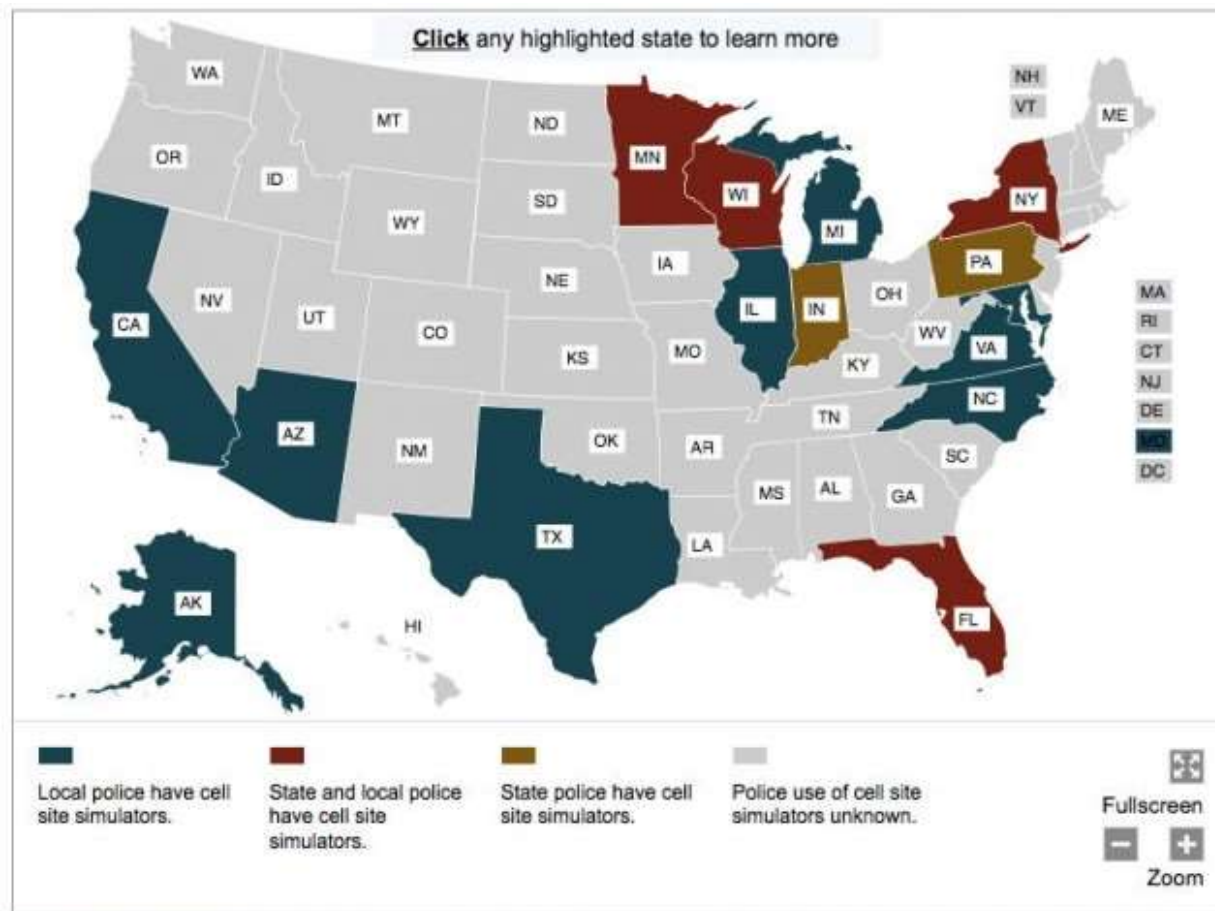# Phones in the Legal System

- Riley v. California
  - SCOTUS 2014

- Unanimous ruling that **warrantless** search of a phone during an arrest is unconstitutional

Mobile Devices

- What are some other key security and privacy challenges for mobile devices?
    - Tracking for advertising
    - Tracking using MAC address
    - Tracking using accelerometer
    - Lack of desktop-based tools
    - Authentication of telephone networks

Mobile Devices

- Stingrays (cell site simulator)

Click any highlighted state to learn more

Local police have cell site simulators.	State and local police have cell site simulators.	State police have cell site simulators.	Police use of cell site simulators unknown.

Fullscreen

Zoom

Display a table of the map data.

Internet of Things

What is the IoT?

What is the IoT?

What is the IoT?

Security Issues in Homes

- Sharing data
  - Many users
  - Many devices
  - Sensitive data

- Access to networks (e.g., wifi)

- Device pairing

Compare the passcodes

Does the passcode on Windows Phone match this one?

374105

EightForums.com

Yes   No   Cancel

Considerations in the Home

- Home as "castle"

- Occupants with social relationships

- Visitors; guests

- Surveillance

- Patching devices

- Side channels

Safety-critical devices

Cars

https://www.youtube.com/watch?v=oqe6S6m73Zw

https://www.youtube.com/watch?v=3jstaBeXgAs

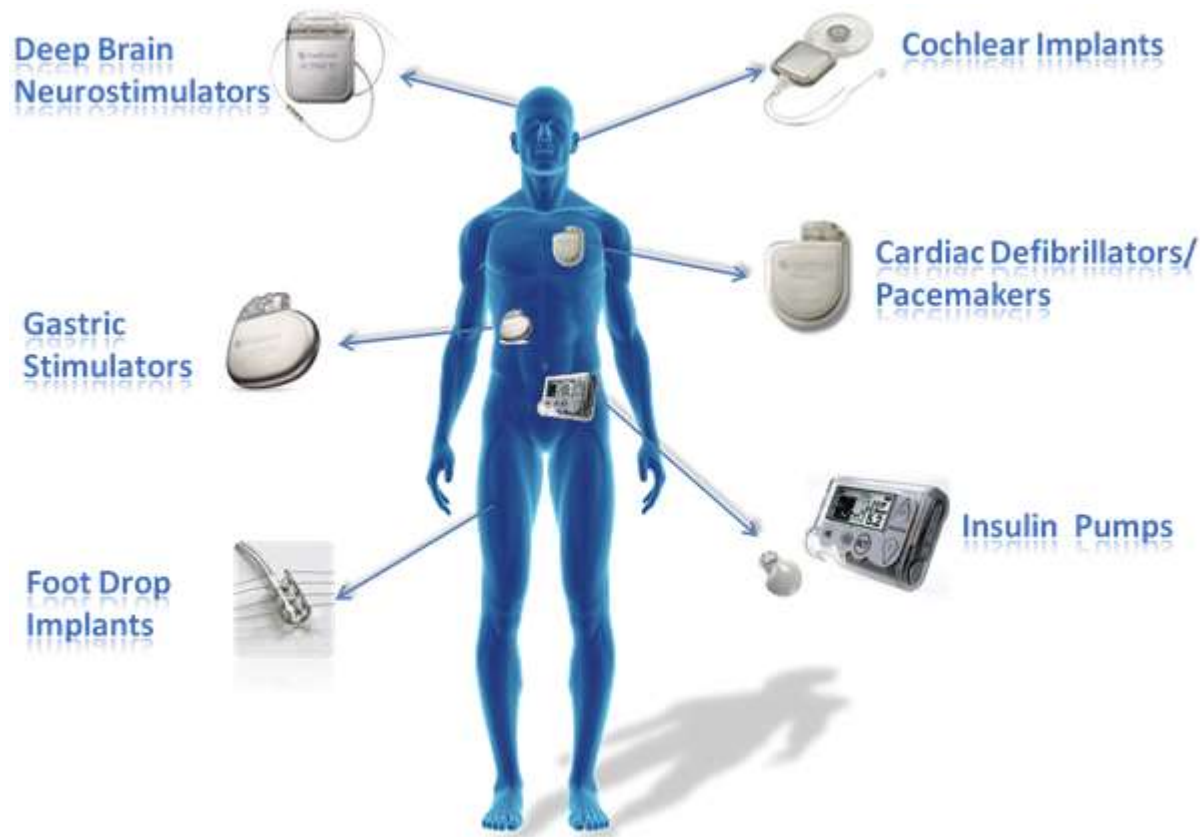# Meta-issues with car privacy/security

- Why are our cars run by computers?

- Why are we connecting our cars to the Internet?
  - Rich media content
  - Real-time traffic and safety info
  - OTA updates
  - Self-driving cars
  - (Surveillance)

- Are privacy/security issues the same?

Meta-issues with privacy/security

- Let's answer the same questions for medical devices

Implantable Medical Devices (IMD)

- Embedded computers

- 350K Pacemakers & 173K Cardiac Defibrillators in 2006

Deep Brain Neurostimulators

Cochlear Implants

Cardiac Defibrillators/ Pacemakers

Gastric Stimulators

Insulin Pumps

Foot Drop Implants

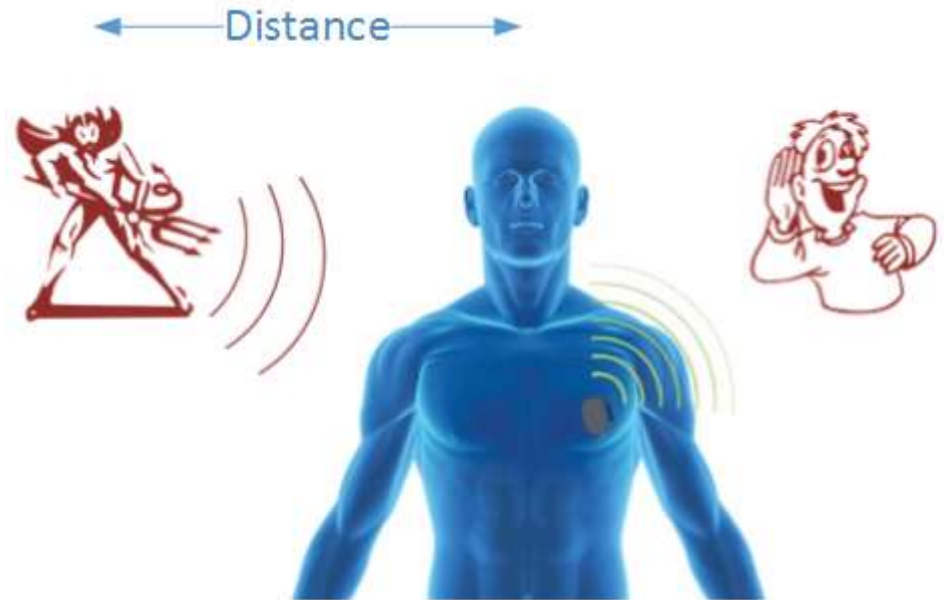healthcareitsystems.com

Operational Requirements

- Possible goals

  - Collect information (diagnostics)
  - Provide information (medical history)
  - Perform medical function

- Disable IMD before conducting surgeries

- Access in emergency situations

- Constraints

  - Limited capacity of battery (replacement = surgery)

Risks in Medical Devices

- Vulnerabilities
  - Authentication
- Attack Vectors
  - Passive
  - Active
- Risks / threats
  - DoS
  - Changes in configuration
  - Replace medical records -- someone having a different operation
  - Injuries, death

Hacking Tests (1)

- **2008:** wireless access to a combination heart defibrillator and pacemaker (within two inches of the test gear)

- Disclose personal patient data

- Reprogram IMD to shut down and to deliver jolts of electricity that would potentially be fatal

Hacking Tests (2)

2011-2012-2013

- **Hacking Insulin Pumps**

-- insulinpump.com

2013 -- Black Hat /Defcon:

- **"Implantable medical devices: hacking humans"**
  - At 30 feet by compromising their pacemaker
  - Transmitter to scan for and interrogate individual medical implants
  - Security techniques for manufacturers

-- ioactive.com

Defense Approaches

- How do we achieve resistance to attacks?

  – What are the classes of attacks?

- What can go wrong?

- How do we balance utility and security/privacy?
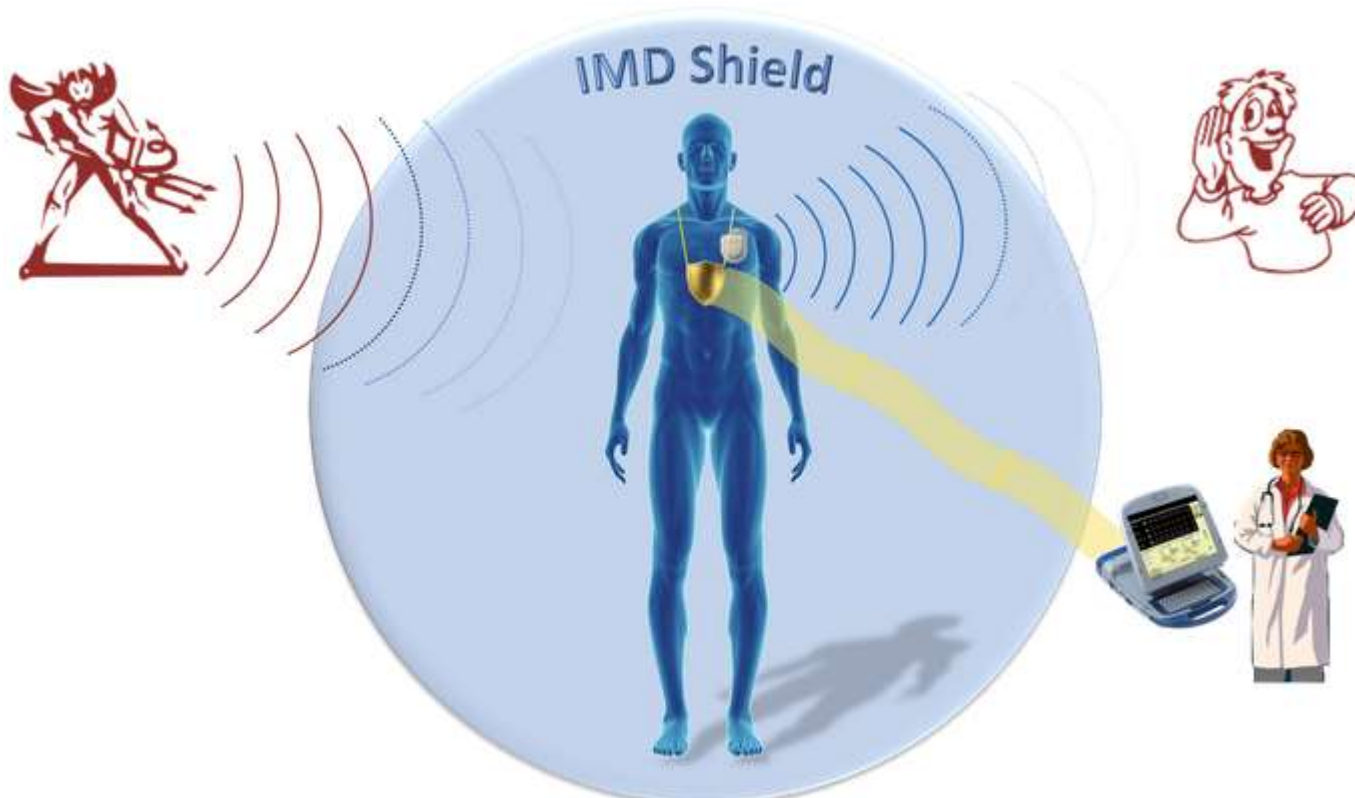
Authentication Methods

- Passwords: how to make them available?
  - Tattooed passwords (visible, UV visible)
  - Bracelet

- Biometrics (face recognition)

- Smart Cards

- Touch-to-access policy

- Key-based systems

- Shields
  - Necklace
  - Computational wristband

IMD Shield

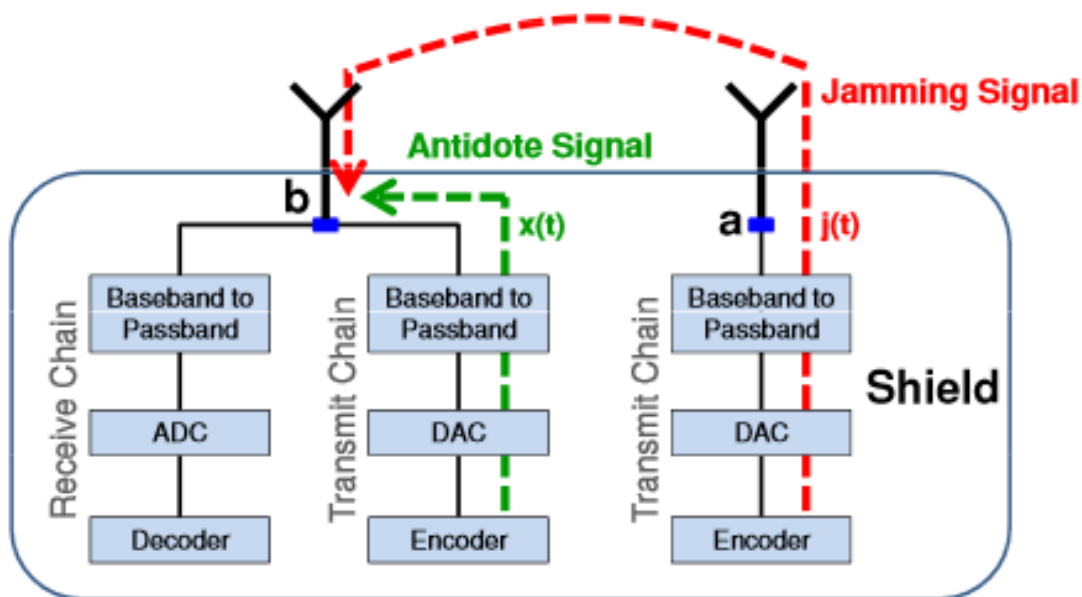- Proxy (messages exchanges)

- Authentication + encryption (channel)

- IMDShield -mit.edu

IMD Shield - Implementation

- Jammer design (full duplex radio)

- S. Gollakota et al. MIT

Wristbands / Alert Bracelets

- Safety in emergencies

- Security & Privacy under adversarial conditions

- Battery life

Wristbands / Alert Bracelets

- Protection is granted while wearing the bracelet.

- Remove to gain access to the IMD

- Inform patients about malicious actions – But not preventive

- Authentication + symmetric encryption

- Disadvantages
  - Relies on the patient wearing the bracelet
  - Reactive
  - Cognitive effects on patients

--Denning et al.

Usability Considerations

- Hospitals not having correct equipment

- Visual indicator of patients condition (something is wrong). Personal dignity.

- Carrying one more device

- Aesthetics
  - Wristbands (especially). "Mockups are unaesthetic"
  - Tattoos

- Mental and physical inconvenience

- Cultural and historical associations

Electronic Medical Records

- Why do we want *electronic* medical records?

- What are privacy/security concerns about electronic medical records?

- How do we mitigate those concerns?