09. Mobile Devices and Safety-Critical Systems

Blase Ur, April 30th, 2019
CMSC 23210 / 33210
Mobile Devices
Authentication
Permissions Model for Apps

This application can access the following on your phone:

- **Your location**
  - fine (GPS) location

- **Network communication**
  - full Internet access

- **Your personal information**
  - read contact data

- **Your accounts**
  - manage the accounts list, Picasa Web Albums, use the authentication credentials of an account

- **Storage**
  - modify/delete USB storage contents

- **Phone calls**
  - read phone state and identity

- **System tools**
  - prevent phone from sleeping, write subscribed feeds, write sync settings
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)
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
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

---

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

---

-- insulinpump.com

-- 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

-- Figures from Denning et al.
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?
Designing for Usability
What to do about hazards?
Best solution: remove hazard
If all else fails: warn
A better solution would be to add a spring so the door won’t slam
hole

70 H
Support users’ decisions

<table>
<thead>
<tr>
<th>High probability of danger</th>
<th>Might be dangerous</th>
<th>Very low probability of danger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block</td>
<td>User must decide</td>
<td>Don’t bother user</td>
</tr>
</tbody>
</table>

Improve warnings

Help user decide by asking question user is qualified to answer
Something happened and you need to click OK to get on with doing things.

Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegafroce.
Bad question

Your web browser thinks this is a phishing web site. Do you want to go there anyway?

Don’t go there  Go there anyway
People were confused until they posted instructions.
Design communicates function
How do you unplug the sink?
How do you turn on this shower?
Stove layout
Stove layout
Stove layout
Doors
Doors
Doors