mHealth Panel: Trusted Sensors

Alec Wolman
Microsoft Research
Observation #1

- Smartphones will play a major role in healthcare
  - Lots of simple healthcare apps already
    - Patients Know Best: Manage your personal medical records
    - Foodwiz: Avoid allergies with barcode scanning
    - Medication reminders
  - And a few sophisticated ones …
    - iBGStar: FDA-approved blood glucose monitoring app for iphone
  - New sensors will enable many new health apps
    - BLE (BT 4.0) provides energy-efficient extension of sensing capabilities
Observation #2

- Malware is coming to smartphones
  - Juniper study showed 155% rise in 2011
  - Most of the focus on Android
  - Malware installs through vulnerabilities, and through social engineering
- App stores help, but they don’t eliminate the problem
Problem

• We don’t have a good track record for securing general-purpose platforms
• For health-critical apps & services, need isolation from malware

• Can Trusted Computing hardware help?
  • At MSR, we’ve been investigating mobile platform support for “trusted sensors”
Trusted Sensors

- Trusted Sensors: use trusted computing primitives to preserve the integrity & authenticity of sensor readings
  - Sensors use digital signatures to sign their readings
  - Verification of sensor readings performed by a cloud service

- Observation: trusted computing is coming to mobile
  - Many laptops already have TPM chip
  - Many smartphones already have ARM’s TrustZone
## Trusted Sensors Architecture

### Mobile Device

<table>
<thead>
<tr>
<th>Layer</th>
<th>Components</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Purpose Operating System</td>
<td>Applications</td>
</tr>
<tr>
<td>Isolated Execution Environment (per-app)</td>
<td>App-Specific Trusted Sensor Transformations</td>
</tr>
<tr>
<td>Secure Execution (TCB)</td>
<td>Signing Service / Trusted Sensor APIs, Sensor Device Drivers, Policy Object Interpreter</td>
</tr>
</tbody>
</table>

#### Isolation Boundaries

- Sensor-based Attestations
- Web Services

---

The Trusted Sensors Architecture diagram illustrates the layers and components of a mobile device, including the general purpose operating system, isolated execution environment (per-app), and secure execution (TCB). Each layer contains various components such as applications, app-specific trusted sensor transformations, signing service, trusted sensor APIs, sensor device drivers, and policy object interpreter. The diagram also highlights the isolation boundaries, indicating the secure execution environment for each application to prevent unauthorized access and ensure data integrity.