IoT – Identity of Things Perspective

Dipto Chakravarty
CTO, Exostar
IoT - Gaps in Design

- Identity of smart Things
- Disruptive technology trends
- Accidental architecture leaves gaps
- Resulting “Swiss cheese” solution is often full of holes

Source: http://iotslam.com/session/securing-trust-mobile-communication-smart-things/
## IoT - Gaps in Architectural Patterns

<table>
<thead>
<tr>
<th>Endpoint structure</th>
<th>Device Location</th>
<th>Device Integrity</th>
<th>Device (Edge)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mgmt structure</td>
<td>Virtualize</td>
<td>Enterprise Mgmt</td>
<td>Client Mgmt</td>
</tr>
<tr>
<td>App structure</td>
<td>Web apps</td>
<td>Mobile apps</td>
<td>VDI/Desktop apps</td>
</tr>
<tr>
<td>Identity structure</td>
<td>Cloud Identity</td>
<td>Identity as-a-Svc</td>
<td>Enterprise Identity</td>
</tr>
<tr>
<td>Infrastructure</td>
<td>Public Cloud</td>
<td>Private Cloud</td>
<td>Virtualized</td>
</tr>
</tbody>
</table>
Summary ...

- Challenges in architecting solutions for IoT / IIoT
- Patterns to use for designing your new IoT apps
- Identity of IoT and IIoT will be pervasive

**Evolution**
- Mobile → IoT
- SaaS → Mobile
- Enterprise → SaaS

**Solution**
- IoT ← Mobile
- Mobile ← SaaS
- SaaS ← Enterprise
IoT – Manufacturer’s Perspective

Andrew Girson
CEO, Barr Group
Building secure IoT devices is not easy...

• No “One-Size-Fits-All” Solution
  • Many markets, from aero to consumer to medical to auto
  • Many types, from low-power to ruggedized to low-cost
  • Many generations, from pre-Internet retrofits to near-past legacy designs to future designs
  • Many threats, from physical device tampering to close-range wireless snooping to remote Internet-based infiltration

• An engineer designing a low-cost IoT widget can’t add in a crypto-chip or advanced crypto software
...especially when security is ignored

Internet-based Device?

Yes 60%

No 22%

...especially when security is ignored

and Dangerous?

Yes 25%

In Denial!

Is Security a Design Requirement?

Source:
Barr Group 2017 Embedded Systems Safety & Security Survey
(~2000 respondents)
Do we care about the right issues?

60% of engineers overall do consider security, but note the topics of concern:

- IoT manufacturers will bolster the security in their products when the market tells them to do so.
IoT – Privacy Perspective

Joe Klein
CTO, Disrupt6
# Licensed-High Speed (Mobile Carriers) Wireless Generations

<table>
<thead>
<tr>
<th>Physical Layer</th>
<th>Voice</th>
<th>0G</th>
<th>1G</th>
<th>2G</th>
<th>3G</th>
<th>4G + LTE</th>
<th>5G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Analogue</td>
<td>Voice</td>
<td>Analogue</td>
<td>GSM</td>
<td>WCDMA</td>
<td>OFDM</td>
<td>MIMO/mWave</td>
<td>MMAwave</td>
</tr>
<tr>
<td>Digital Voice</td>
<td>WAP</td>
<td>Digital Voice</td>
<td>WAP</td>
<td>IMS</td>
<td>IMS</td>
<td>IMS</td>
<td>IoT/OT</td>
</tr>
</tbody>
</table>

- **Performance**:
  - 0G: ~9,600bk/s
  - 1G: <200kb/s
  - 2G: <100mb/s
  - 3G: <1gb/s
  - 4G + LTE: <1gb/s
  - 5G: <1gb/s

<table>
<thead>
<tr>
<th>Network Layer</th>
<th>Application Layer</th>
<th>Privacy &amp; Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>No-IP</td>
<td>FAX &amp; Modem</td>
<td>Eavesdropping</td>
</tr>
<tr>
<td>IPv4/NAT</td>
<td>SMS</td>
<td>SMS, Voice &amp; Data Intercept</td>
</tr>
<tr>
<td>IPv6</td>
<td>Web</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Video/Chat</td>
<td></td>
</tr>
</tbody>
</table>

## Physical Layer
- **Analogue**: Analogue
- **GSM**: Global System for Mobile Communications
- **WCDMA**: Wideband Code Division Multiple Access
- **OFDM**: Orthogonal Frequency-Division Multiplexing
- **MIMO/mWave**: Multiple Input Multiple Output/mMillimeter Wave
- **Digital Voice**: Digital Voice
- **WAP**: Wireless Application Protocol
- **IMS**: IP Multimedia Subsystem
- **IoT/OT**: Internet of Things/Operational Technology

## Network Layer
- **No-IP**: No Internet Protocol
- **IPv4/NAT**: Internet Protocol Version 4/Network Address Translator
- **IPv6**: Internet Protocol Version 6

## Application Layer
- **FAX & Modem**: Facsimile & Modem
- **SMS**: Short Message Service
- **Web**: World Wide Web
- **Video/Chat**: Video Chat

## Privacy & Security
- **Eavesdropping**: Eavesdropping
- **SMS, Voice & Data Intercept**: SMS, Voice & Data Intercept
Internet Generations

- ArpaNet
- US Government
- NCP
- 256
- E-Mail, FTP
  - Server/Server
  - No Security or Privacy
- InterNET
  - InterNAT
- Public Internet
- IPv4/NAT
- 4 Billion
- WWW, Client/Server
  - Cloud
  - Streaming Media (1:1)
  - Bolt on Security
- Tourists
  - Dial-Up
- New InterNET
- Global Internet
- IPv6
- 3.4x10^38
- P2P, M2M, V2V, V2I, IPFS
  - Computing at the Edge
  - Streaming Media (1:M)
  - Security & Privacy
- Residents
- Always On

IoT & OT Zone
## IoT Privacy & Security Recommendations

<table>
<thead>
<tr>
<th>What</th>
<th>Why</th>
<th>How</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption</strong></td>
<td>Manage Keys Not Data</td>
<td>Key Management, Remote Attestation</td>
</tr>
<tr>
<td><strong>Tokenization</strong></td>
<td>Reduce Value of Data</td>
<td>Data Sovereignty/Residency/Privacy</td>
</tr>
<tr>
<td><strong>Containment</strong></td>
<td>Block movement</td>
<td>Decomposition into Containers &amp; Firewalls</td>
</tr>
<tr>
<td><strong>Immutability</strong></td>
<td>Avoid Changes to code</td>
<td>Power up, power cycle, Secure Boot</td>
</tr>
<tr>
<td><strong>Flux</strong></td>
<td>‘Make it moving’</td>
<td>Frequency/IP/Application/Reboots/Patching</td>
</tr>
<tr>
<td><strong>Speed</strong></td>
<td>‘The New Stealth’</td>
<td>DevOps, ‘Serverless computing’</td>
</tr>
<tr>
<td><strong>Diversity</strong></td>
<td>Increases effort</td>
<td>Processors, Networks, Hardware</td>
</tr>
<tr>
<td><strong>Decentralization</strong></td>
<td>Decrease value in any one location (Cloud!)</td>
<td>P2P networks, Analytics at the edge, Distributed Files and Processing (IPFS)</td>
</tr>
<tr>
<td><strong>Disinformation</strong></td>
<td>Slows attackers</td>
<td>Deception Systems</td>
</tr>
<tr>
<td><strong>Identity</strong></td>
<td>Raise the trust of communications</td>
<td>Human Identity, Device Identity</td>
</tr>
<tr>
<td><strong>Open Systems and Standards</strong></td>
<td>Avoid backdoor lock in</td>
<td>Avoid older standards &amp; preparatory systems</td>
</tr>
<tr>
<td><strong>Maximize Vendor Trust</strong></td>
<td>Avoid claims without delivery and short EOL</td>
<td>ANSI/NIST Supplier Declaration of Conformity (SDOC)</td>
</tr>
<tr>
<td><strong>Supply Chain</strong></td>
<td>Dependencies bring extraordinary risk. Hardware is the new software.</td>
<td>Testing, SDOC requirements</td>
</tr>
</tbody>
</table>
The 7 Principles of Privacy (and Security)

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, Not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric

Source: https://blog.varonis.com/privacy-design-cheat-sheet/