IoT Security Platform

Andrey Doukhvalov
Head of Future Tech

Industrial Cybersecurity: Safeguarding Progress
Saint Petersburg, Russia
September, 2017
IoT Malware in Action

- In 2016 one million devices have been infected with **BASHLITE**.
- 96% are IoT devices (cameras and DVRs),
- 4% are home routers
- 1% are compromised Linux servers.

**Remaiten** is a Malware which infects Linux on embedded systems by brute forcing using frequently used default username and passwords combinations from a list in order to infect a system.

**Linux.Darlloz** is a worm which infects Linux embedded systems. It targets the internet of things and infects routers, security cameras, set-top boxes by exploiting a PHP vulnerability.

- 900,000 customers of German ISP Deutsche Telekom
- 2,400 home routers across the UK
IoT Security Landscape

Root-of-Trust, Strong Authentication, Verification

- **Edge**
  - Authentication (verified)
  - Service discovery / provisioning / pairing
  - Trusted execution environment
  - Network security / firewall
  - Secure Boot

- **Gateways / Smart Devices**
  - Authentication (verified)
  - Encryption
  - Message integrity
  - MitM protection
  - DNS spoofing protection

- **Network**
  - Authentication (verified)
  - PKI / certificate management
  - Trusted execution environment
  - Network security / firewall
  - Access control (role based)

- **DataCenter / Cloud**
  - Authentication (verified)
  - PKI / certificate management
  - Trusted execution environment
  - Network security / firewall
  - Access control (role based)

---

**IoT Device Security**

**Communication Security**

**Cloud Security**
The Eclipse IoT Working Group, IEEE IoT, AGILE IoT and IoT Council co-sponsored an online survey to better understand how developers are building IoT solutions.

The survey was open from February 7 until March 17, 2017. A total of 713 individuals participated in the survey. Each partner promoted the survey to their communities through social media and web sites.
### Key Industries / Trends 2016-2017

<table>
<thead>
<tr>
<th>Industry</th>
<th>2016</th>
<th>2017</th>
</tr>
</thead>
<tbody>
<tr>
<td>IoT platform / middleware</td>
<td>41.6%</td>
<td>41.1%</td>
</tr>
<tr>
<td>Home automation</td>
<td>41.1%</td>
<td></td>
</tr>
<tr>
<td>Industrial automation</td>
<td></td>
<td>36.4%</td>
</tr>
<tr>
<td>Connected / smart cities</td>
<td></td>
<td>33.4%</td>
</tr>
<tr>
<td>Energy management</td>
<td></td>
<td>33.3%</td>
</tr>
<tr>
<td>Building automation</td>
<td></td>
<td>26.1%</td>
</tr>
<tr>
<td>Agriculture</td>
<td></td>
<td>25.5%</td>
</tr>
<tr>
<td>Healthcare</td>
<td></td>
<td>22.7%</td>
</tr>
<tr>
<td>Automotive</td>
<td></td>
<td>21.4%</td>
</tr>
<tr>
<td>Transportation</td>
<td></td>
<td>20.1%</td>
</tr>
</tbody>
</table>

Participation of other industries is growing...
Hardware Components in IoT Solutions

What hardware components are included in your IoT solution?

- Sensors: 86.8%
- Actuators: 50.8%
- Gateway / hub device: 50.2%
- Edge node device: 36.2%
- Camera / video capture: 35.1%
- LCD display: 33.5%
- Touch screen: 25.4%
- Audio playback / speaker: 17.4%
- None: 4.5%
- Other: 4.1%
Security is the N1 IoT Developers’ concern

<table>
<thead>
<tr>
<th>Topic</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>46.7%</td>
</tr>
<tr>
<td>Interoperability</td>
<td>24.4%</td>
</tr>
<tr>
<td>Connectivity</td>
<td>21.4%</td>
</tr>
<tr>
<td>Integration with hardware</td>
<td>19.3%</td>
</tr>
<tr>
<td>Standards</td>
<td>15.0%</td>
</tr>
<tr>
<td>Return on investment (ROI)</td>
<td>14.8%</td>
</tr>
<tr>
<td>Cost</td>
<td>14.7%</td>
</tr>
<tr>
<td>Scalability</td>
<td>14.1%</td>
</tr>
<tr>
<td>Privacy</td>
<td>13.7%</td>
</tr>
<tr>
<td>Performance</td>
<td>12.3%</td>
</tr>
<tr>
<td>Data analytics</td>
<td>12.3%</td>
</tr>
<tr>
<td>Complexity</td>
<td>9.0%</td>
</tr>
<tr>
<td>Maintenance</td>
<td>8.2%</td>
</tr>
<tr>
<td>Certification / conformance</td>
<td>4.4%</td>
</tr>
<tr>
<td>Other</td>
<td>3.8%</td>
</tr>
<tr>
<td>I don't know</td>
<td>2.4%</td>
</tr>
</tbody>
</table>
What can we learn from mobile & apply to IoT?

Lifecycle Security

Communications Security

Device Security
IoT Security should be integrated

Situation

- Most IoT developers are not security experts
- Little to no knowledge of hardware
- Prior experience in mobile app development
- Time to market & functionality beat security

Strategy

- Ease of use requirements on tools & IoT platform providers
- Hide complexity of hardware based security
- Provide built-in security functions
- Use standard methods and building blocks
How much security you need?

- **Physical access to device**
  - JTAG, Bus, IO Pins
  - Time, money & equipment

- **Software Attacks & lightweight hardware attacks**
  - Buffer overflows
  - Interrupts
  - Malware

- **Communication Attacks**
  - Man In The Middle
  - Weak RNG
  - Code vulnerabilities

- **Secure Element**
  - SW & HW Attacks
    - Physical access to device
    - JTAG, Bus, IO Pins
    - Time, money & equipment

- **Security Subsystem**
  - TEE/SP

- **Hardware isolated TEE/SP M**

- **Традиционные TLS/S SL**

- **Security Cost**

---

*Trusted Execution Environment / Secure Partitioning Manager*
В 2010, под эгидой GlobalPlatform был запущен проект Trusted Execution Environment (TEE). Инициатива была запущена в ответ на изменения на рынке мобильности: требования к безопасности существенно возросли по мере того как потребители начали использовать мобильные устройства для финансовых и платежных транзакций. Кроме того, по мере роста потребления контента (видео, музыка) на разных типах устройств, старые методы защиты контента оказались недостаточны. Для защиты премиального контента его владельцы традиционно использовали Digital Rights Management (DRM), Conditional Access (CA) и др. подобные схемы часто использовали аппаратно-усиленную защиту контента, в то время как теперь они столкнулись со средой где взаимодействует множество разных агентов. Кроме того, изменение путей доставки контента (3G, 4G, Wi-Fi, WiMAX, Bluetooth, NFC) предъявляет повышенные требования к коммуникационным каналам.
Global Platform Trusted Execution Environment

- TEE became the global standard for embedded security
TEE Platform in action

Merchant

- Register Account: 15 Seconds...
- Enter Address: 59 Seconds...

Payment

- Input Card Details: 78 Seconds...
- Authenticate: 7 Seconds...

32 Keystrokes
56 Keystrokes
23 Keystrokes
9 Keystrokes

Select Address:
1 Second...
Select Account
Enter PIN:
6 Seconds...

1 Keystroke
5 Keystrokes

2.5 Minutes
120 Keystrokes

7 Seconds
6 Keystrokes
Global Platform TEE Management Framework

- The newly emerging TEE MF standard lays ground to the remotely controlled embedded security

The goals of the security model for administration are:

- to provide means to manage the Trusted Execution Environment (TEE), Security Domains (SD), and Trusted Applications (TA),

- to ensure the security and the integrity of these entities,

- to enable the confidentiality of the data,

- to provide a scalable model allowing deployments involving a unique Actor or multiple Actors,

- and to enforce the security policy of each Actor while preserving its assets.

To ensure the security and integrity of these entities, the TMF code implementation on the device is a Trusted OS Component (see [TEE Arch]), or composed from a group of such components. As such it inherits the same security requirements as other Trusted OS Components.
### Kaspersky IoT Security Platform - proposal

#### Security Operation Center
- Security Services Mngmnt
- KATA
- Security Center

#### Gateway
- KSN, DPI
- TMS/TFS, KICS
- FW
- AV
- VPN

#### Edge
- Logging Inspection

---

### System
- Cloud security services
- Systems Management
- Policy Management

---

### Applications
- General
- Security
- Applications

### TEE MF
- Lifecycle Security
- Comm Security
- Device Security

---

### Hypervisor
- TEE Services
- KOS

### TEE Services
- KOS TEE + SE on trusted SoC
- KOS TEE on trusted SoC

---

### Security Center

---

<table>
<thead>
<tr>
<th>Integrated Security</th>
<th>ARM</th>
<th>Intel</th>
</tr>
</thead>
<tbody>
<tr>
<td>HV Non-TEE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3rd-party TEE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KOS TEE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KOS TEE + SE on trusted SoC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

### Security Services
- FW
- AV
- VPN
- Logging Inspection

---

### TEE
- Trusted Boot
- Trusted Channel
- OTA
- Trusted Storage
- Crypto

---

### Policy Management
- Cloud security services
- Systems Management
- Policy Management
## Platform Roadmap

<table>
<thead>
<tr>
<th>Services</th>
<th>KL Core Assets</th>
<th>Ecosystem</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Operation Center</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Anomaly Detection</td>
<td>MLAD/KATA</td>
<td>Industrial Modules</td>
</tr>
<tr>
<td>Malware Protection</td>
<td>KSN/CF/AV</td>
<td>Security Services</td>
</tr>
<tr>
<td>IoT Platform Connectors</td>
<td>KSC for IoT (TEE MF)</td>
<td>Trusted IoT Platform</td>
</tr>
<tr>
<td><strong>Gateway/Networking</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Monitoring</td>
<td>KSN/CV/AV/TMS/KICS</td>
<td>Industrial Protocols</td>
</tr>
<tr>
<td>Lifecycle Security</td>
<td>Firmware Update</td>
<td>Add-Ons</td>
</tr>
<tr>
<td>Communication Security</td>
<td>Trusted Channel</td>
<td>Devices (Router, STB)</td>
</tr>
<tr>
<td>Device Security</td>
<td>Device Pairing</td>
<td>Devices (Router, STB)</td>
</tr>
<tr>
<td><strong>Device Level</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Security</td>
<td>KSS (Lib -&gt; Agent)</td>
<td>KSS Linux</td>
</tr>
<tr>
<td>Trusted Hypervisor</td>
<td>KSH</td>
<td>TEE functions</td>
</tr>
<tr>
<td>Integrated Security</td>
<td>KOS</td>
<td>SoC (Elvis)</td>
</tr>
</tbody>
</table>
IoT Security Platform

Let's discuss it

Andrey Doukhvalov
Head of Future Tech

Industrial Cybersecurity: Safeguarding Progress
Saint Petersburg, Russia
September, 2017