Azure Sphere
为智能边缘保驾护航

施 佳
物联网解决方案架构师
IoT Solutions, Microsoft
2019年3月13日 苏州
The microcontroller (MCU) a low-cost, single chip computer

9 BILLION new MCU devices built and deployed every year
The MPU in your PC is 100x to 1000x more powerful than the MCU in your fridge.
Connected MCUs will change your customer relationships

How does a consumer know the compressor in their fridge needs to be replaced?

Option 1
Melted ice cream

Option 2
Predictive maintenance

Connected devices create **profoundly better** customer experiences.
And, expose your business to unequalled risks...

Observations on October 21, 2016 Botnet Attack

- **Device security is a socioeconomic concern**
  - Day 1 the attack is Technology headline in NY Times
  - Day 2 the attack is Politics headline

- **The attack exploited well-understood weaknesses**
  - Weak common passwords, no early detection, no remote update, etc.

- **Future attacks could be much larger**
  - This attack was small; just 100k devices
  - Imagine a 100M-device attack

- **Future attacks could create huge liability exposure**
  - Hackers could "brick" an entire product line in a day
  - Actuating devices could cause property damage or loss of life
The internet security battle. We’ve been fighting it for *decades*. We have experience to share.
Highly-secured connected devices require 7 properties

1. **Hardware Root of Trust**
   - Is your device’s identity and software integrity secured by hardware?

2. **Defense in Depth**
   - Does your device remain protected if a security mechanism is defeated?

3. **Small Trusted Computing Base**
   - Is your device’s TCB protected from bugs in other code?

4. **Dynamic Compartments**
   - Can your device’s security protections improve after deployment?

5. **Certificate-Based Authentication**
   - Does your device use certificates instead of passwords for authentication?

6. **Failure Reporting**
   - Does your device report back about failures and anomalies?

7. **Renewable Security**
   - Does your device’s software update automatically?

https://aka.ms/7properties

= Silicon support required  = OS support required  = Cloud Service support required
Some properties depend only on hardware support

- Hardware to protect **Device Identity**
- Hardware to **Secure Boot**
- Hardware to attest **System Integrity**

**Hardware Root of Trust**

Unforgeable cryptographic keys generated and protected by hardware

*Is your device’s identity and software integrity secured by hardware?*
Some properties depend on hardware and software

- Hardware to **Create Barriers**
- Software to **Configure Compartments**

**Dynamic Compartments**
Internal barriers limit the reach of any single failure

*Can your device’s security protections improve after it is deployed?*
Some properties depend on hardware, software and cloud

Renewable Security
Device security renewed to overcome evolving threats and security breaches.

Does your device’s software update automatically?

- Cloud to **Provide Updates**
- Software to **Apply Updates**
- Hardware to **Prevent Rollback**
Azure Sphere empowers manufacturers to create highly-secured, connected MCU devices

**SECURITY**
Every device built with Azure Sphere is secured by Microsoft. For its 10 year lifetime.

**PRODUCTIVITY**
The Azure Sphere developer experience shortens OEM time to market.

**OPPORTUNITY**
Azure Sphere empowers OEMs to create new customer experiences and business models.
Azure Sphere is an end-to-end solution for securing MCU powered devices

New Azure Sphere certified MCUs, from silicon partners, with built-in Microsoft security technology provide connectivity and a dependable hardware root of trust.

New Azure Sphere OS secured by Microsoft for the devices 10-year lifetime to create a trustworthy platform for new IoT experiences.

The Azure Sphere Security Service guards every Azure Sphere device; it brokers trust for device-to-device and device-to-cloud communication, detects emerging threats, and renews device security.
Azure Sphere certified MCUs create a secured root of trust for connected, intelligence edge devices

**CONNECTED** with built-in networking

**SECURED** with built-in Microsoft silicon security technology including the Pluton Security Subsystem

**CROSSOVER** Cortex-A processing power brought to MCUs for the first time
Our Silicon Partners
The Azure Sphere OS is optimized for IoT, Security and MCU agility

**Azure Sphere OS Architecture**

- **OS Layer 4**
  - App Containers for POSIX (on Cortex-A)
  - App Containers for I/O (on Cortex-Ms)

- **OS Layer 3**
  - **On-chip Cloud Services**

- **OS Layer 2**
  - **HLOS Kernel**

- **OS Layer 1**
  - **Security Monitor**

- **Hardware**
  - Azure Sphere certified MCUs

**On-chip Cloud Services**
- Provide update, authentication, and connectivity
- Custom Linux kernel empowers agile silicon evolution and reuse of code
- Security Monitor guards integrity and access to critical resources

**Secure Application Sandboxes**
- Compartmentalize code for agility, robustness & security

**HLOS Kernel**
- Product manufacturer's application
  - Runtime for applications (e.g., Base C API, Azure IoT, HTTP client, UART and GPIO APIs, etc.)

**Security Monitor**
- Networking management
  - Application management
  - OTA update client
  - Device Authentication client

**Custom Linux Kernel**
- User Mode
  - Supervisor Mode

© Microsoft Corporation
The Azure Sphere Security Service connects and protects every Azure Sphere device

**Protects** your devices and your customers with certificate-based authentication of all communication

**Detects** emerging security threats through automated processing of on-device failures

**Responds** to threats with fully automated on-device updates of OS

**Allows** for easy deployment of software updates to Azure Sphere powered devices
Modernize MCU development with Azure Sphere and Visual Studio

**Simplify development**
Focus your device development effort on the value you want to create

**Streamline debugging**
Experience interactive, context-aware debugging across device and cloud

**Collaborate across your team**
Apply tool-assisted collaboration across your entire development organization

**Simplify Azure connect**
Connect your Azure Sphere devices quickly and easily to Azure IoT
Three components.
One low price.
No subscription required.

An Azure Sphere certified MCU
The Azure Sphere Security Service for 10 years
The Azure Sphere OS with 10 years of on-device updates
Azure Sphere is open

Open to any MCU manufacturer
We are licensing our Pluton security subsystem royalty **free for use** in any chip*

Open to any cloud
Azure Sphere devices are free to connect to Azure or any other cloud, proprietary or public for application data

Open to any innovation
MCU manufacturers are free to innovate with our GPL’d OSS Linux kernel code base

* Azure Sphere branding requires an Azure Sphere chip with Azure Sphere OS and Azure Sphere Security Service
SECURITY

Peace of mind
Protect your products and customers with our turnkey, 7 property security solution that protects, detects and responds to threats dynamically so you’re always prepared.

PRODUCTIVITY

Faster time to market
Lower overhead and increase team efficiency with tools that deliver productivity and dramatically optimize development and maintenance of your device and experiences.

OPPORTUNITY

The future is now
Transform engagement your products and customer strategies, and enable new revenue streams with connected crossover chips powerful enough to create next generation experiences.
Demo 演示：
连接Azure Sphere到Azure IoT Hub
### Azure Sphere MCU and Module Application Scenarios*

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Module Use Case</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>complement existing MCU</strong></td>
<td>Upgrade existing devices by adding a Azure Sphere module to existing MCU, connected by serial, SPI etc.</td>
<td>Use a Azure Sphere MCU to provide connectivity in conjunction with an application-specific MCU.</td>
</tr>
<tr>
<td><strong>replace existing MCU</strong></td>
<td>Add connectivity to existing or new devices by wiring simple sensing, control and HMI to a Azure Sphere module.</td>
<td>Use a Azure Sphere MCU to implement all the on-device logic and provide connectivity.</td>
</tr>
</tbody>
</table>

* Hybrid combinations possible  † HMI: human-machine interface
非常感谢！