Securing the Billions of Devices Around Us

Dr. Galen Hunt
Distinguished Engineer and Managing Director
Microsoft Azure Sphere
MCU
- 192Mhz Cortex-M4
- 256KB SRAM
- 1MB NOR FLASH
- GPIO, I2C, I2S, etc.
- RTOS (no kernel)

Radio Analog
- 2.4 & 5 GHz

Radio Digital
- WiFi
MCU (Microcontroller)
low-cost, single chip computer

9 BILLION new MCU devices built and deployed every year
How do you know if the compressor in your fridge needs to be replaced?

The Old Way
Melted ice cream

The New Way
Auto-diagnosis
Opportunity | Risk
What happens when you connect a device to the internet?

“The internet is this cauldron of evil.”
Dr. James Mickens, Harvard University
“Ransomware attacks will target more IoT devices in 2018”

“Huge IoT botnet may be used for Ukraine attack”

“When smart gadgets spy on you: Your home life is less private than you think”

“Industrial IoT to equip new era of corporate intruders coming in through devices”

“Security experts warn of dangers of connected home devices”

“Hacking these IoT baby monitors is child’s play, researchers reveal”

“Hackers infect 500,000 consumer routers all over the world with malware”

“Your smart fridge may kill you: The dark side of IoT”

“The Lurking Danger of Medical Device Hackers”

“Why the KRACK Wi-Fi mess will take decades to clean up”

“Hacking critical infrastructure via a vending machine? The IOT reality”

“Protecting Your Family: The Internet of Things Gives Hackers Creepy New Options”
Mirai Botnet attack

Everyday devices are used to launch an attack that takes down the internet for a day

100k devices

Exploited a well known weakness

No early detection, no remote update
Building a highly-secured device is difficult and costly.

Design and build a holistic solution

You’re only as secure as your weakest link.
You must have the technical expertise to stitch disparate security components into an gap-free, end-to-end solution.

Recognize and mitigate emerging threats

Threats evolve over time.
You must have the ongoing security expertise to identify and create the updates needed to mitigate new threats as they emerge.

Distribute and apply updates on a global scale

Update efficiency is critical.
You must have the infrastructure, logistics and operational excellence to deliver and deploy updates globally to your entire fleet of devices in hours.
How can we secure the 9 BILLION new MCU-based devices built and deployed every year?
Azure Sphere is an end-to-end solution for securing MCU powered devices.
Azure Sphere Certified Chips
with a built-in hardware root of trust
created from Microsoft’s learnings securing three generations of Xbox consoles.
Microsoft Pluton Security Subsystem

ARM Cortex-M for real time processing (2x)

SRAM ≥ 4MB

ARM Cortex-A optimized for low power

Internet Connection WiFi in first chips

FLASH ≥ 4MB

Multiplexed I/O

Firewalls

Certified Azure Sphere Chip
Highly-Secured & Internet Connected

Guarded
No Internet Connection

Microsoft Pluton IP Block Only

ARM Cortex-M for real time processing (1x)

SRAM

Flash

I/O

Firewalls

SECURED with full Pluton Security Subsystem

CONNECTED with built-in Internet networking

CROSSOVER rich processing brought to MCUs

LOCKED with Pluton IP block

GUARDED by full Azure Sphere Chip

HARD-WIRED within device
The Azure Sphere OS

a multi-layer defense-in-depth OS that merges the best of Microsoft and OSS technologies to create a trustworthy platform for new IoT experiences.
The Azure Sphere OS is optimized for IoT, security, and agility

**Secure Application Containers**
Compartmentalize code for agility, robustness & security

**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 hardware resources

**Pluton Runtime**
Controls processing cores and access to crypto ops

---

### Azure Sphere OS Architecture

<table>
<thead>
<tr>
<th>OS Layer 5</th>
<th>Generic Containers (on Cortex-A)</th>
<th>Real-Time Containers (on Cortex-Ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Layer 4</td>
<td>On-chip Cloud Services</td>
<td></td>
</tr>
<tr>
<td>OS Layer 3</td>
<td>HLOS Kernel</td>
<td></td>
</tr>
<tr>
<td>OS Layer 2</td>
<td>Security Monitor</td>
<td></td>
</tr>
<tr>
<td>OS Layer 1</td>
<td>Pluton Runtime</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>Azure Sphere MCUs</td>
<td></td>
</tr>
</tbody>
</table>
The Azure Sphere Security Service guards every Azure Sphere device; it brokers trust for connectivity through certificate based authentication, detects emerging threats through online failure reporting, and renews device security through software updates.
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.
Device Security is like a stool; it requires three legs:
How do we think about device security?
Microsoft has more than 25 years experience protecting customers and their devices.
SECURITY IS FOUNDATIONAL

It must be built in from the beginning.
The 7 properties of highly secured devices

Is your device highly secured or does it just have some security features?

- **Hardware Root of Trust**: Is your device’s identity and software integrity secured by hardware?
- **Defense in Depth**: Does your device remain protected if one of its security mechanisms is defeated?
- **Small Trusted Computing Base**: Is your device’s security-enforcement code protected from bugs in other code?
- **Dynamic Compartments**: Can your device’s security enforcement improve after deployment?
- **Certificate-Based Authentication**: Does your device use certificates instead of passwords for authentication?
- **Failure Reporting**: Does your device report back failures and anomalies?
- **Renewable Security**: Does your device’s software update automatically?

https://aka.ms/7properties
“Supply chains are not friendly territory.”

- Andrew “bunnie” Huang, BlueHat IL 2019

https://www.youtube.com/watch?v=RqQhWitJ1As
Some properties depend only on hardware support

Hardware Root of Trust

Unforgeable cryptographic keys generated and protected by hardware

• Hardware to protect device identity
• Hardware to secure software boot
• Hardware to attest system integrity
Some properties depend on hardware and software

**Dynamic Compartments**

Internal barriers limit the reach of any single failure

- Hardware to create barriers
- Software to configure into compartments
Some properties depend on hardware, software and cloud.

Renewable Security

Device security renewed to overcome emerging and evolving threats

- Cloud to provide updates
- Software to apply updates
- Hardware to prevent rollbacks
Meeting the 7 properties is difficult and costly

- Design and build a holistic solution
- Recognize and mitigate emerging threats
- Distribute and apply updates on a global scale

You’re only as secure as your weakest link.
You must have the technical expertise to stitch disparate security components into an gap-free, end-to-end solution.

Threats evolve over time.
You must have the ongoing security expertise to identify and create the updates needed to mitigate new threats as they emerge.

Update efficiency is critical.
You must have the infrastructure, logistics and operational excellence to deliver and deploy updates globally to your entire fleet of devices in hours.
Context Matters:
Hackers attack casino

Attackers gain access to casino database through fish tank

Entry point was a connected thermometer

Once in, other vulnerabilities were exploited

Gained access to high-roller database
Let’s secure the future.

SECURED FROM THE SILICON UP

@galen_hunt
/in/galenh