The Seven Properties Of Highly-Secure IoT Devices

Dr. David Tarditi
Principal Software Engineer Lead
Microsoft Azure Sphere
MCU (Microcontroller) low-cost, single chip computer

9 BILLION new MCU devices built and deployed every year
Many will be connected to the Internet

Radio Analog
2.4 & 5 GHz

Radio Digital
WiFi

MCU from 2014 with radios on die

192Mhz Cortex-M4
256KB SRAM
1MB NOR FLASH
GPIO, I2C, I2S, etc.
RTOS (no kernel)
How does a consumer or business know the compressor in their refrigerator needs to be replaced?

The Old Way
Melted ice cream/spoiled food

The New Way
Auto-diagnosis

Connected devices create profoundly better experiences.
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"

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

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

"The Lurking Danger of Medical Device Hackers"

"Hacking critical infrastructure via a vending machine? The IOT reality"

"Security experts warn of dangers of connected home devices"

"Hacking these IoT baby monitors is child's play, researchers reveal"

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

"Protecting Your Family: The Internet of Things Gives Hackers Creepy New Options"

"Huge IoT botnet may be used for Ukraine attack"

"Industrial IoT to equip new era of corporate intruders coming in through devices"
Mirai Botnet attack
October, 2016

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
Internet risks highlighted by Mirai 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-known 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 have much worse effects.  
Hackers could “brick” an entire product line in a day  
Actuating devices could cause property damage or loss of life

The New York Times
Hackers Used New Weapons to Disrupt Major Websites Across U.S.

A New Era of Internet Attacks Powered by Everyday Devices
How do you build a secured device?

What are best practices?
Microsoft has more than 25 years experience protecting customers and their devices.
Some lessons learned

YOUR CODE HAS BUGS

NIST security vulnerability causes from 2008-2017

(The top blue line is out-of-bounds memory errors)
YOUR DEVICE WILL BE HACKED.

Hackers are smart.
Hackers are creative.
Hackers are persistent.
SECURITY IS FOUNDATIONAL

It must be built in from the beginning.
The 7 properties of highly secure IoT devices
Is your device highly secured or does it just have some security features?

1. Hardware Root of Trust
2. Defense in Depth
3. Small Trusted Computing Base
4. Dynamic Compartments
5. Certificate-Based Authentication
6. Failure Reporting
7. Renewable Security

White paper: https://aka.ms/7properties
Hardware Root of Trust

Hardware to protect device identity
• Unforgeable cryptographic keys generated and protected by hardware
• Hardware holds private key.
• Public key establishes identity with others.

Hardware to secure software boot
• Boot ROM ensures loader integrity

Hardware to attest system integrity
• Is only your code running?
Small Trusted Computing Base

- Be as small as possible (less code = fewer bugs).
- Reduce the attack surface.
- Have a security monitor or hypervisor sitting underneath kernel.

Trusted computing base is the software that ensures security of system.

Linux kernel

Security monitor
Compartments limit the reach and impact of any single security breach.

- Hardware and software support for memory protection + processes.

**Defense-in-depth**

- Multiple layers of defense
- Multiple mitigations: internal firewalls on buses, network firewall, no-execute, ASLR, ...
Certificate-Based Authentication

• Passwords for devices have problems: can be stolen or hacked, require administration

• We know who the device is and that it is in a good state.

• Can issue certificates to device allowing access to services.
Failure reporting

Renewable Security

Failure reporting
Gather reports across devices at scale to detect software flaws, probing, and attacks.

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 challenging

- 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.
Case study: realizing the 7 properties with Azure Sphere
Azure Sphere is an end-to-end solution for securing connected devices.

The Azure Sphere OS

The Azure Sphere Security Service

Azure Sphere Certified Chips
Azure Sphere Certified Chips

with a built-in hardware root of trust
created from Microsoft’s learnings as we secured
three generations of Xbox consoles.
Azure Sphere defines a template for secured chips

First chip: MediaTek MT3620
Highly-Secured & Connected

- **Microsoft Pluton** Security Subsystem
- **FLASH** 16 MB
- **Internet Connection** WiFi in first chips
- **ARM Cortex-M** for real time processing (2x)
- **SRAM** 4 MB
- **ARM Cortex-A** optimized for low power
- **Multiplied I/O**
  - GPIO
  - PWM
  - TDM
  - I2S
  - UART
  - DC
  - SPI
  - ADC

**CONNECTED** with built-in networking

**SECURED** with Pluton Security Subsystem

**CROSSOVER** rich processing even on MCUs

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 Architecture

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
The Azure Sphere Security Service guards every Azure Sphere device; it brokers trust, detects emerging threats, and upgrades device security.
The Azure Sphere Security Service

**Protects** your devices with certificate-based authentication for all communication

**Detect** emerging security threats through automated reporting of on-device failures

**Respond** to security threats/issues with
- Fully automated on-device updates of OS
- Hands-free deployment of updates to applications.
Device Security is like a stool; it requires three legs:

1. Secured OS
2. Secured Cloud Service
3. Secured Chips
Key take-aways

Security is foundational. Design and build it from the start.

Use the 7 properties when evaluating security claims. Is your device really secure? How will it stand up over time?

Read the white paper. https://aka.ms/7properties.

Check out Azure Sphere. An example of realizing the properties: https://azure.microsoft.com/en-us/services/azure-sphere/.

Microsoft @ Booth #9.
Let’s secure the future.

SECURED FROM THE SILICON UP