Microsoft Azure Sphere Overview

Martin Grossen, Line Manager Microsoft Embedded / IoT Europe
martin.grossen@avnet.eu

5. June 2018
Prepare for the 2nd wave of Digital Transformation…

Wave 1: The Microcontroller (MCU)

Wave 2: Internet Connectivity
Manufacturers have a compelling desire to build connected MCU-based devices

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

<table>
<thead>
<tr>
<th>Option 1</th>
<th>Option 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Melted ice cream</td>
<td>Message that a technician</td>
</tr>
<tr>
<td>and spoiled milk</td>
<td>with replacement compressor</td>
</tr>
<tr>
<td></td>
<td>will arrive tonight</td>
</tr>
</tbody>
</table>

Connected devices create profoundly better customer experiences
Observations

Device Security is a socioeconomic concern

DAY 1 the attack is Technology headline in NY Times
DAY 2 the attack is Politics headline

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 industry response to date is inadequate

For example, network vendors offer to turn off network ports

The attack exploited well-known weaknesses

Weak common passwords, no early detection, no remote update, etc
The danger is real, especially for IoT devices

The Mirai Botnet (aka Dyn Attack), Oct 2016: Largest IoT DDoS attack. Large portions of the internet going down, including Twitter, the Guardian, Netflix, Reddit and CNN. Affected devices: Webcams and DVR players.

The Jeep Hack, July 2015: A team of researchers was able to take total control of a Jeep SUV by exploiting a firmware update vulnerability.

The TRENDnet Webcam Hack, Jan. 2012. Access to camera and microphone over TCP/IP.

The Hackable Cardiac Device from St.Jude, Jan. 2017: The vulnerability provided access to drain the battery, change heartbeat pace and to trigger shocks.

The Printer Hack to catch fire, Nov. 2011: Made the fuser overheat, causing the paper in the printer to catch fire.
The internet security battle

Microsoft has been fighting it for decades so they have some experience to share. Also on hardware side!

Example X-BOX:

XBOX: Hacked within weeks
  -> Standard Intel x86 system

XBOX 360:Hacked within 3,5 month
  -> HW hack to compromise the bus:

XBOX One: Not hacked until today
  -> also thanks to in-chip bus firewalls
Highly-secured connected devices require 7 properties

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

= Silicon support required  
= OS support required  
= Cloud Service support required  

http://aka.ms/7properties
Azure Sphere is an end-to-end solution for creating highly-secured, connected MCU devices.

**Secured MCUs**
A new class of crossover Azure Sphere MCUs, from our silicon partners, with built-in Microsoft security technology provide connectivity, high performance, and a secured hardware root of trust.

**Secured Operating System**
The highly-secured Azure Sphere IoT OS combines the best of Microsoft and OSS technologies to create a trustworthy platform for new IoT experiences.

**Secured by our Cloud Service**
The Azure Sphere Security Service guards every Azure Sphere device; it protects your devices and customers, detects emerging threats, and proactively responds.
Azure Sphere: Technology and Solution Overview
So what is Azure Sphere exactly?

Azure Sphere is not a single chip but a security solution / technology built with a combination of a special microcontroller, a special operating system and the corresponding cloud services.

Azure Sphere is a high-value, cost-effective solution, secured by Microsoft.

The solution today contains:
- **Azure Sphere Chip** MT3620
- **Azure Sphere Security Services** for 10 years
- **Azure Sphere IoT OS** with 10 years of on-device updates
Today, only Azure Sphere provides all 7 Properties for secured IoT

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MT3620</td>
<td>Azure Sphere</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Espressif ESP32</td>
<td>RTOS &amp; ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Marvell 88MW300/2</td>
<td>RTOS &amp; ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualcomm QCA4010</td>
<td>RTOS &amp; ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Broadcom BCM43907</td>
<td>RTOS &amp; ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TI CC3220x</td>
<td>RTOS &amp; ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Full, Partial, or No Silicon support
- Full, Partial, or No OS support
- Full, Partial, or No Cloud Security Service support
Azure Sphere History

- Project started in 2014 in Microsoft Research, now part of AI&R division
- Started working on prototype chip and OS in 2015
- Established “seven properties of highly secured devices”
- Ran a “security challenge” based on prototype chip and OS in 2017
- Actively working with partners and customers for production in 2018
Azure Sphere:
The chip MT3620
Azure Spheres MCU’s - Create a secured foundation for intelligent edge devices

- **Secured**
  - With built-in Microsoft security technology, i.e. I/O bus firewalls
  - Including the Pluton Security Subsystem

- **Performance**
  - With built-in Cortex-A7 processors
  - Delivers significantly greater performance vs. similar traditional MCU

- **Connected**
  - With built-in networking
Device Development using the MT3620
Device Development Options

Use a module

Use the chip directly and solder to PCB
Microsoft is working with other suppliers to implement the Azure Sphere Pluton Security Core into their HW:

<table>
<thead>
<tr>
<th>ARM</th>
<th>Hilscher</th>
<th>LitePoint</th>
<th>LongSys</th>
<th>MediaTek</th>
<th>Nordic</th>
<th>Nuvoton</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXP</td>
<td>Qualcomm</td>
<td>Seeed Studio</td>
<td>Silicon Labs</td>
<td>STMicroelectronics</td>
<td>Toshiba</td>
<td>VeriSilicon</td>
</tr>
</tbody>
</table>

[AVNET SILICA]
Azure Sphere: The Operating System
Azure Sphere IoT OS: Unequalled security and 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**
  - Secure HLOS Kernel

- **OS Layer 1**
  - Security Picovisor

- **Hardware**
  - Azure Sphere MCUs

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

**On-chip Cloud Services**
Provide update, authentication, and connectivity

**Secured HLOS Kernel**
Empowers agile silicon evolution and reuse of code

**Security Picovisor**
 Guards integrity and access to critical resources
Azure Sphere: The Cloud Services
The Azure Sphere Security Service guards every Azure Sphere device. It renews security, identifies emerging threats, and brokers trust between device, cloud, and other endpoints.

- Protecting devices with certificate-based authentication
- Guaranteeing device authenticity and running only your genuine software
- Getting insight into device and application failure and visibility into emerging threats
- Deploys app updates to your Azure Sphere powered devices
Azure Sphere: The Software Development
Azure Sphere and Visual Studio enhance your productivity

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

**Accelerate Deployment**
Bring the power of automation to your development experience

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

**Connect your Developers**
Apply tool-assisted collaboration across your entire development organization
Azure Sphere development tools
Azure Sphere:
The Development Board
MT3620 Development Board

MT3620

Micro USB socket

FT4232HQ
Azure Sphere: Live Demo
Azure Sphere Live Demo Prerequisite

You need following prerequisite to run this live demo on the Azure Sphere development board:

- Installed Visual Studio 2017 version 15.3 or later
- Installed Azure Sphere SDK and Tools version 4.0.1
- Configured all drivers and network settings per description in SDK/Tool documentation
- Updated Azure Sphere development board with firmware 4.0.1
- Claimed and assigned Azure Sphere development board under your AAD (cutil.exe)
- Configured WiFi (dutil.exe)
- Connected Azure Sphere development board via USB to Computer
- Connected Azure Sphere development via WiFi
- Azure Subscription with a running IoT Hub in
Azure Sphere Live Demo: Visual Studio 2017

Start Visual Studio 2017, create new project: File -> New -> Project
Azure Sphere Live Demo: Visual Studio 2017

Select: Visual C++ -> Cross Platform -> Azure Sphere
In Solution Explorer, add a new connected service with right mouse click on References.
Under Connected services choose Azure IoT Hub
Under Connect, select your Azure subscription running the IoT Hub
Under Connect, select your Azure subscription running the IoT Hub.
Under IoT Hub, select the running IoT Hub you want to use for this demo.
Azure Sphere Live Demo: Visual Studio 2017

Under Device, select your device
If the device was never connected, you have to create a new device with a new name.
Azure Sphere Live Demo: Visual Studio 2017

Under Summary, click Finish
This has added the azure_iot_hub.h and azure_iot_hub.c into your solution
In main.c, find the #error tag and delete this comment out of the code (line 60, 61 & 62)
Azure Sphere Live Demo: Visual Studio 2017

Under Debug, Start Debugging or press F5. If never built before, you will be asked to build first.
In Device Output Windows, you will see the output from the GPIO-, WiFi- and AzureIoTHub API.
Azure Sphere Live Demo: Visual Studio 2017

AzureIoTHub API is submitting states every 10 seconds
Azure Sphere Live Demo: Visual Studio 2017

Log into the Azure Portal where the IoT Hub is running and click on the IoT Hub resource.
Azure Sphere Live Demo: Visual Studio 2017

In the IoT Hub, click on IoT devices
In IoT devices, click on the name of the Azure Sphere development board
In Device Details, click on Device Twin
Scroll down in the device twin JSON file and find the reported blink rate and version number.
Azure Sphere Live Demo: Visual Studio 2017

Press button A on the device and Refresh the Device Twin: Rate and Version has changed
Back in Device Details, click on Message To Device
Azure Sphere Live Demo: Visual Studio 2017

Type in a message to the device in the Message Body and click Send Message
Azure Sphere Live Demo: Visual Studio 2017

AzureIoTHub API is prompting message from IoT Hub in the Visual Studio Output Window
Azure Sphere: The new security technology
Azure Sphere is Open

Open Chips
MCU manufacturer are free to license (without royalty) the security chip kernel “Pluton” for use in any chip whether or not it uses our OS or cloud *

Open Kernel
MCU manufacturers are free to innovate with our GPL’d HLOS kernel code base

Open Cloud
Azure Sphere devices are free to connect to Azure or any other cloud, proprietary or public

Open Data
Your data belongs to you. Azure Sphere secures your data connections, but we never see your data

Open Development
Device manufacturers are free to use Visual Studio or any other development tools with Azure Sphere

* Azure Sphere branding requires a Azure Sphere chip with an Azure Sphere OS and Azure Sphere Security Services
What is the value add from AVNET Silica?

AVNET was selected on a worldwide base as the exclusive distributor for the Azure Sphere technology. AVNET Silica is driving Azure Sphere in Europe.

What we offer

- Advisory services
- Product & solution design
- Embedded / IoT licensing
- Technical trainings
- Integration services
- Cloud & digital services
- Supply chain services
- Logistics

Azure Sphere document package:

http://bit.do/AzureSphere

You have to register first to get the document links by email
What is the Advantage from AVNET Silica on the Azure side?

- AVNET Silica is a Microsoft CSP (Cloud Solution Provider) for industrial applications

- No credit card needed: AVNET Silica will standard invoice Azure consumption over SAP every month

- AVNET Silica will help to set up the Azure subscriptions, set the consumption limit and the access credentials / levels

- AVNET Silica will provide a detailed monthly Azure consumption report per service and per day

- AVNET Silica is supporting together with Microsoft Azure architects the projects on industrial OEM level
AVNET: Contact us!

- For Azure Sphere topics worldwide:
  
  Azure.Sphere@Avnet.com
  
- For Microsoft Embedded / IoT topics in Europe:
  
  Microsoft@Silica.com
Microsoft Azure Sphere Overview
Martin Grossen, Line Manager Microsoft Embedded / IoT Europe
martin.grossen@avnet.eu

5. June 2018