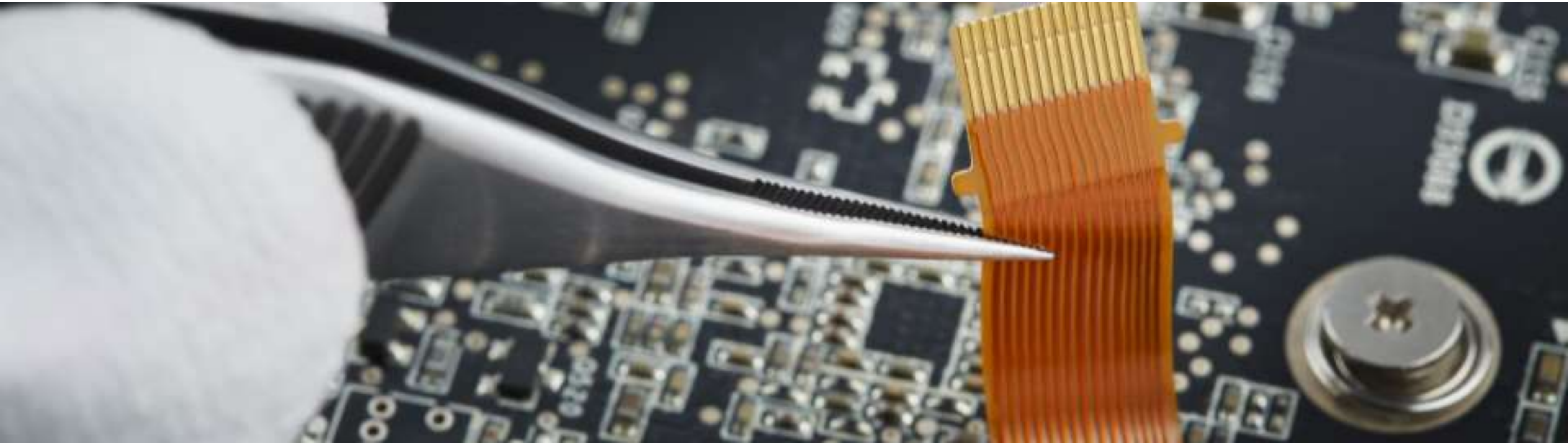
Avnet Integrated Solutions
Secure AI Edge solutions

April 2018

Tim Jensen – Software Director

AVNET®
Reach Further™



What is Security?

- Physical security: on “board elements”
- Bootloader S/W best practices
- Change & application control
- O/S lockdock
- IoT infrastructure
- Virtualised security on cloud

AVNET
Reach Further™

McAfee™

Microsoft

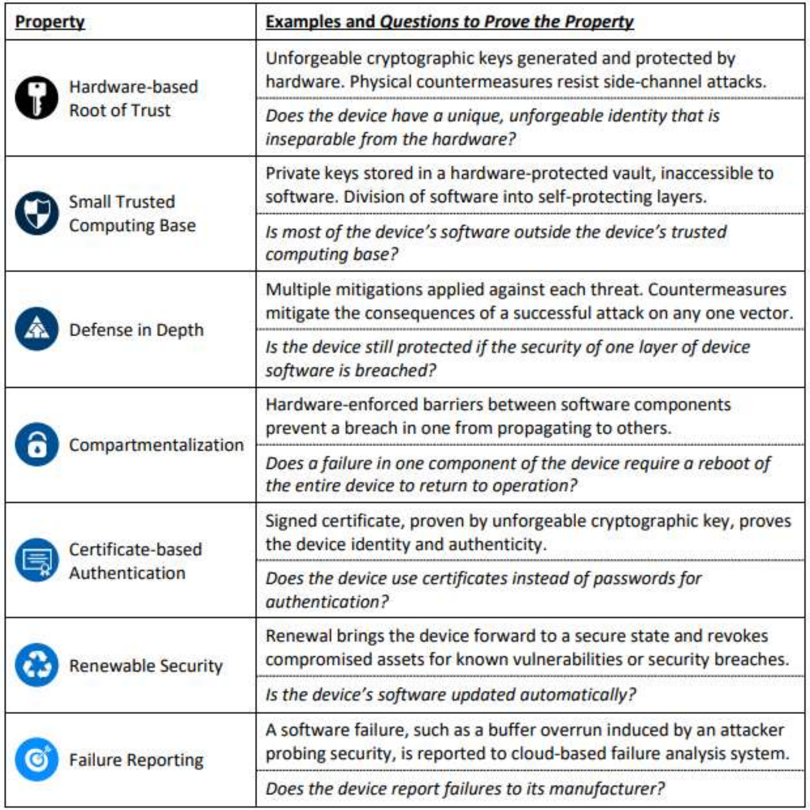
Security thinking

- Traditional players and solutions
  - Hardware security
  - OS Lockdown
  - Black & whitelisting

- New players & new thinking
  - AI is becoming a big part of Security

Microsoft Sopris

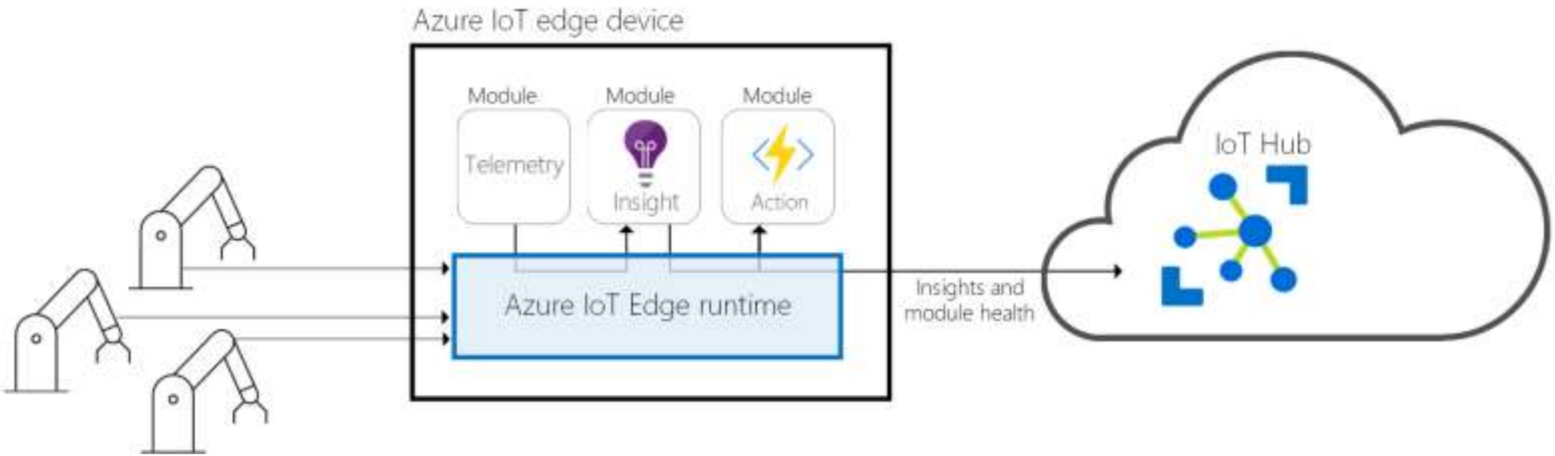
- By Microsoft Research
- 7 Properties of highly secure devices
- Both a HW and Software solution



Property	**Examples and *Questions to Prove the Property***
Hardware-based Root of Trust	Unforgeable cryptographic keys generated and protected by hardware. Physical countermeasures resist side-channel attacks. *Does the device have a unique, unforgeable identity that is inseparable from the hardware?*
Small Trusted Computing Base	Private keys stored in a hardware-protected vault, inaccessible to software. Division of software into self-protecting layers. *Is most of the device's software outside the device's trusted computing base?*
Defense in Depth	Multiple mitigations applied against each threat. Countermeasures mitigate the consequences of a successful attack on any one vector. *Is the device still protected if the security of one layer of device software is breached?*
Compartmentalization	Hardware-enforced barriers between software components prevent a breach in one from propagating to others. *Does a failure in one component of the device require a reboot of the entire device to return to operation?*
Certificate-based Authentication	Signed certificate, proven by unforgeable cryptographic key, proves the device identity and authenticity. *Does the device use certificates instead of passwords for authentication?*
Renewable Security	Renewal brings the device forward to a secure state and revokes compromised assets for known vulnerabilities or security breaches. *Is the device's software updated automatically?*
Failure Reporting	A software failure, such as a buffer overrun induced by an attacker probing security, is reported to cloud-based failure analysis system. *Does the device report failures to its manufacturer?*

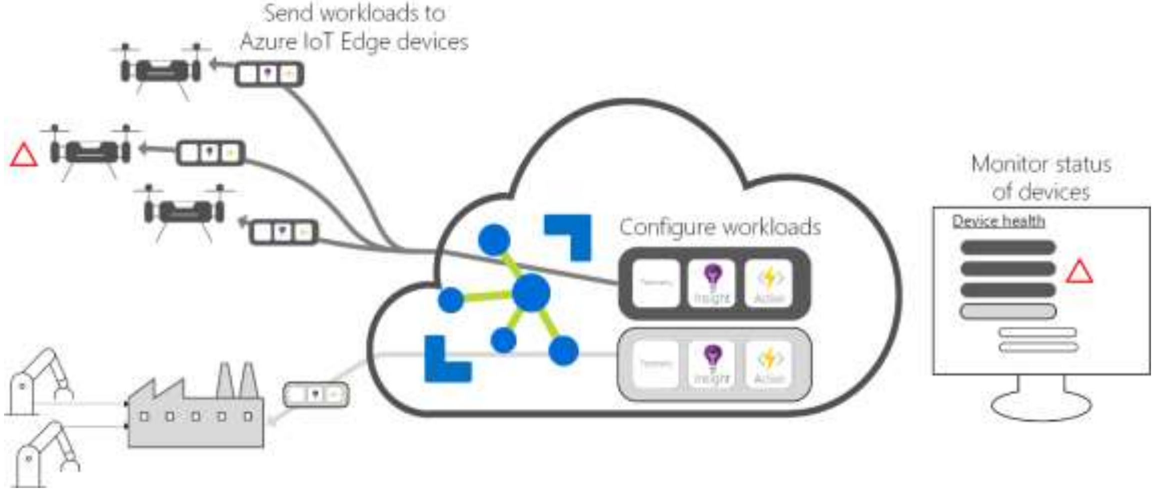
AI at the Edge

- Edge AI is rapidly expanding
- Driver are Availability, latency and Bandwidth
- Many solutions, Software and HW based



Microsoft Azure IoT edge

- Configure workloads in the cloud and push to Edge
- Fully compatible with Microsoft Azure cloud and IoT hub
- Your choice of edge AI:
  - Microsoft services like Machine learning / AI
  - 3rd party solutions
  - Your own solution



Send workloads to Azure IoT Edge devices

Configure workloads

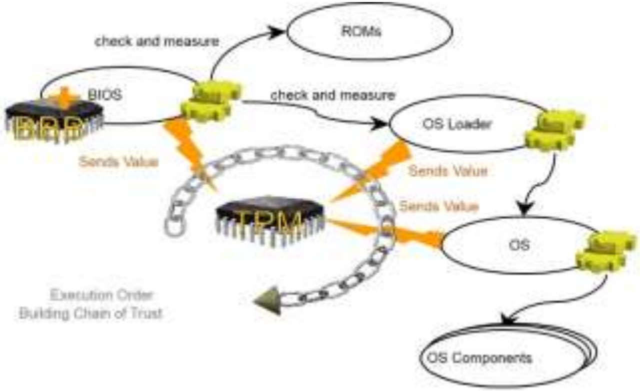
Monitor status of devices

Secure Computing Hardware

UEFI

SECURE BOOT

TRUSTED COMPUTING GROUP®



AVNET®
Reach Further™

BIOS Tools

OS security

Linux

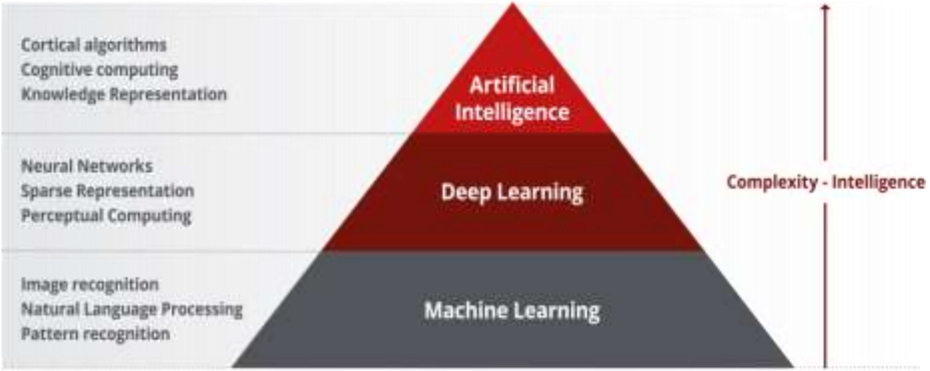
- By default more secure
- Small base = more secure
- Free = your responsibility

Microsoft Windows

- Paid OS – Microsoft responsible
- Recent version (Win 10 IoT) pretty good
- Patching is crucial when connected

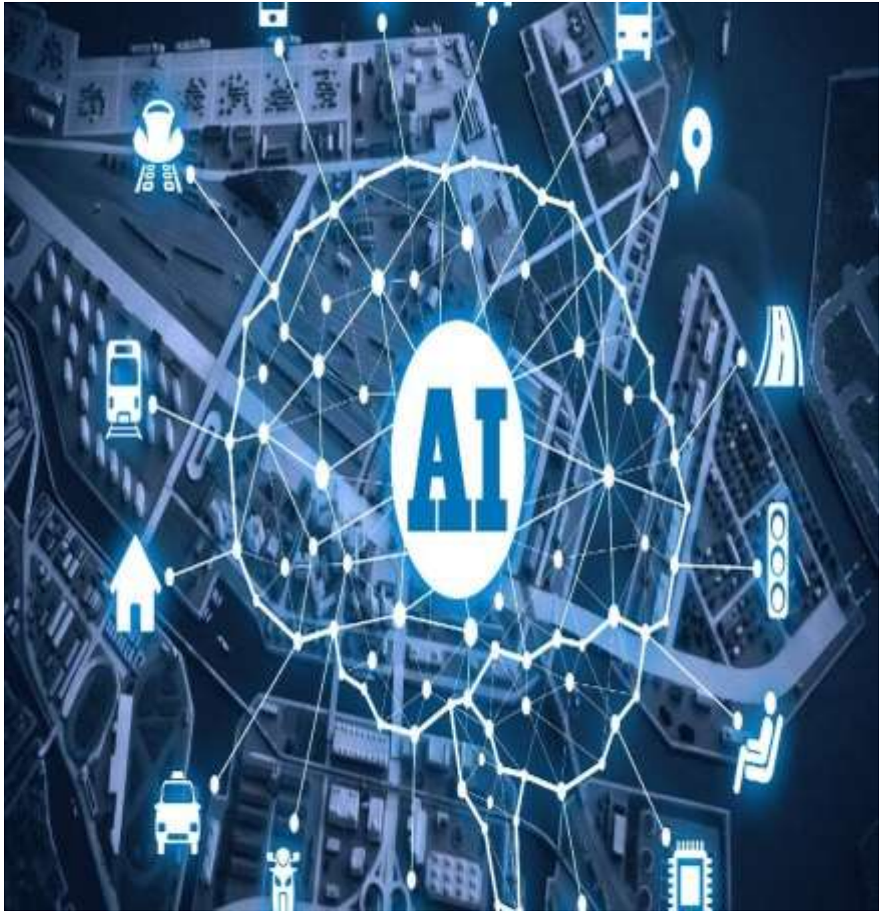
Security Software

- Big change towards machine learning & AI
- Both cloud based and edge based
- Best “secure patient Zero” defense



Summary

- AI at the edge is growing fast
- Security is ever more important
- Consider the full system when thinking about security
- Standard platforms deliver flexible solutions



Reach Further™

AVNET®