msp

CONCURRENT TECHNOLOGIES

Secure Intel Processor Boards

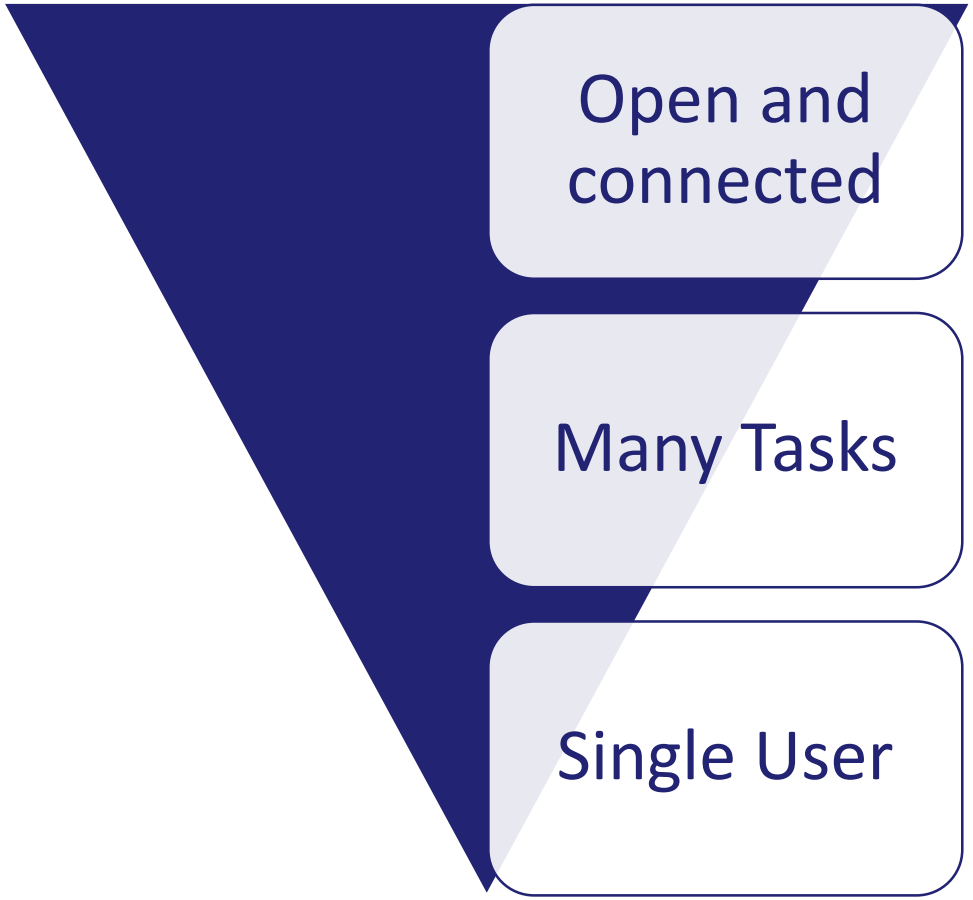
Security Progression

- Security has always been a big issue for Defense Applications

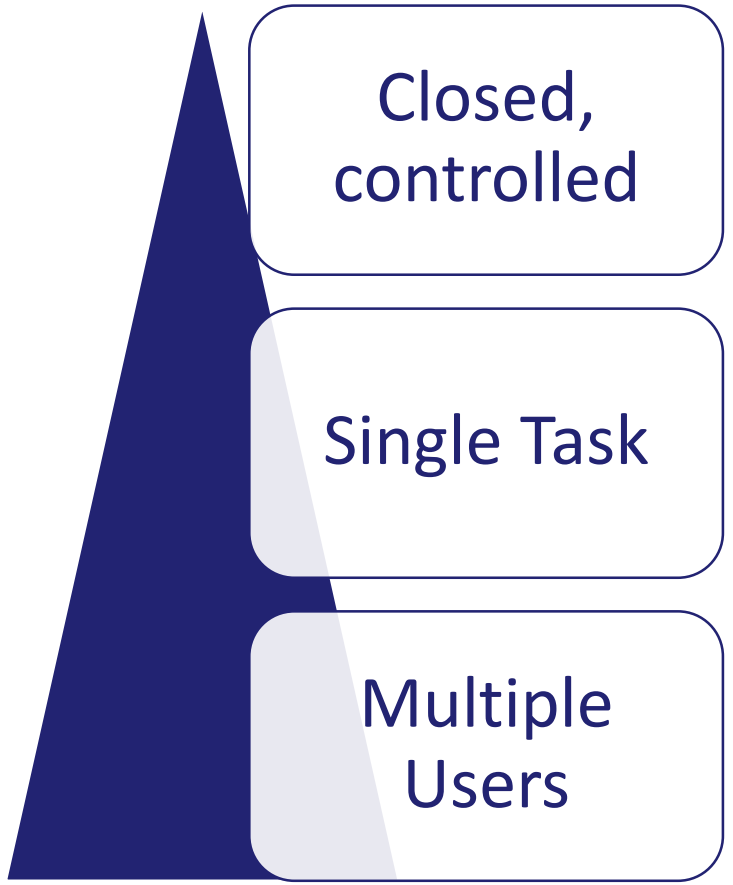
- Recently, other industries have become more security conscious

Security Risks depend on the Environment

Consumer Use



Embedded Use



Embedded users can leverage some consumer technologies

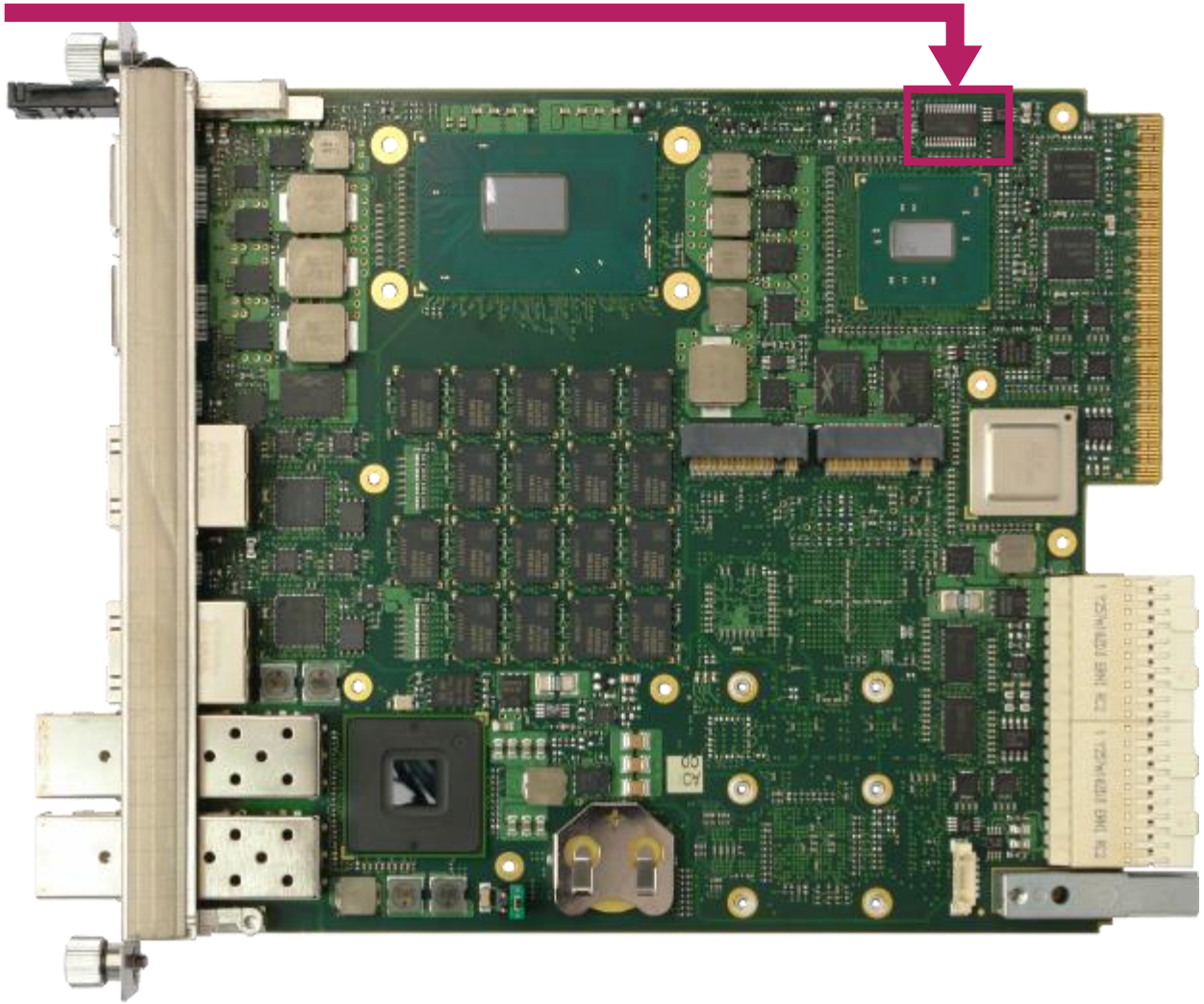
Security Timeline in the context of Windows OS

1993	2002	2009	2012	2015
Microsoft Windows NT	Microsoft Windows xp	Windows 7	Windows 8	Windows 10
User access permissions	IPv6 using IPSec	**TPM 1.2** Bitlocker, User Account Control, Defender	UEFI Secure Boot	**TPM 2.0** Device Guard, Credential Guard, Boot Guard

TPM – Trusted Platform Module

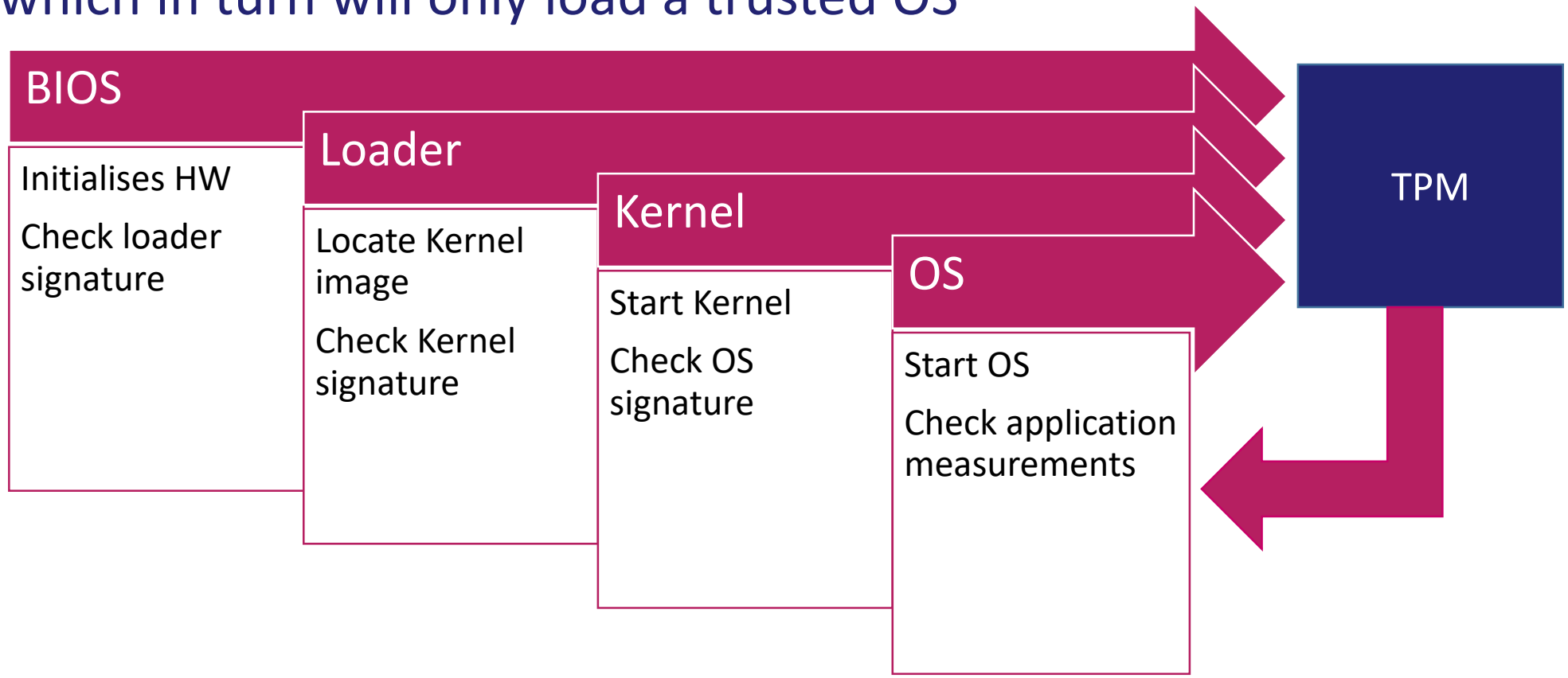
What is a TPM?

- A tamper-resistant integrated circuit
- Enables:
  - Cryptographic key generation
  - Safe storage of small amounts of sensitive information, such as passwords and cryptographic keys
  - Generation of random numbers



TPM can help ensure image security

- The TPM can record hashes that measure the images for later validation
- Secure Boot only loads trusted (signed) operating system bootloaders, which in turn will only load a trusted OS



Guards utilizing TPMs

- Microsoft® Credential Guard prevents against ‘credential creep’ in large organizations:
  - User credentials are isolated from the operating system kernel using virtualization and TPM measurements
- Intel® Boot Guard is a hardware based scheme that prevents boot block takeover

TPM 2.0 Improvements

- Support for additional cryptographic algorithms, i.e. SHA256, SHA384, SHA512, and SM3_256
- Enhancements to the availability of the TPM to applications
- Enhanced authorization mechanisms
- Simplified TPM management

- All new boards from Concurrent Technologies come with TPM 2.0 and it is now an option on boards announced since 2014

Security Timeline

1993	2002	2009	2012	2015
Microsoft Windows NT	Microsoft Windows xp	Windows 7	Windows 8	Windows 10
User access permissions	IPv6 using IPSec	TPM 1.2 Bitlocker, User Account Control, Defender	UEFI Secure Boot	TPM 2.0 Device Guard, Credential Guard, Boot Guard

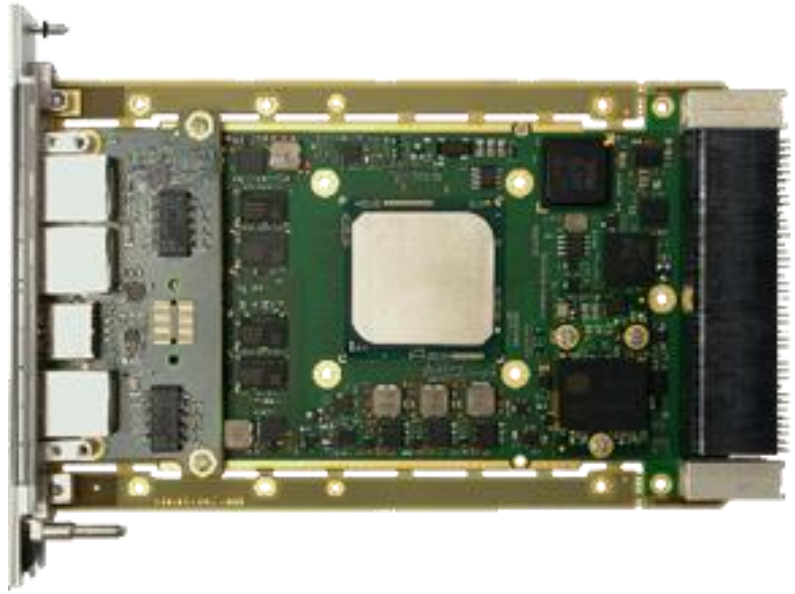
What if you can't use the latest OS?

Use a Hypervisor

- Run a legacy OS and application in a Virtual Machine
- Can utilize native hypervisor or OS based
- Has an impact on real time performance
- Boot method more secure but legacy OS and application concerns

Virtual Machine

Hypervisor



Use a Board based Security Solution

- Guardian Security Package
  - Available since 2012
  - Processor boards are available with the option of additional hardware, firmware and software components for holistic security

Three Key Goals of Guardian

- Preventing unauthorized use:
  - To prevent an unauthorized person from interfering with or operating the equipment
- Preventing unauthorized access:
  - To prevent an unauthorized person from gaining access to sensitive data when they have access to the equipment
  - To prevent a person with legitimate access to the hardware from gaining access to sensitive data
- Allowing sensitive data to be purged on-demand:
  - To ensure that all sensitive data can be deleted rendering the hardware inoperable or returning it to the original factory configuration

Guardian protects against:

- Physical intrusion
- Booting from non-secure sources
- Accessing classified data
- Retrieving sensitive Intellectual Property
- Modifying non-volatile memory
- Executing non-trusted software
- Unauthorized modification of system configuration
- Bypassing low level firmware
- Reverse engineering

Testing and Deployment

- Board is configured:
  - Enables extensive testing without lock activating
- Security Lock enabled:
  - A breach of any selected measure will lock a board permanently
  - Boards are suitable for deployment
- Remove from Service:
  - Sanitization option to scrub and securely erase devices

Conclusions

- Improved security has now (finally) become more important to many customers than backwards compatibility:
  - TPM 2.0 and Windows 10
  - Secure Boot
  - Boot Guard
- Even tightly controlled, closed solutions need security options
- Be flexible - one solution doesn't fit every customer
- Nothing is 100% secure

MSP www.msp.ch

Concurrent Technologies www.gocct.com

Thanks for listening