

Trust Goes Mobile:
Creating Trustworthy Mobile Devices

Janne Uusilehto
TCG Mobile Platform Working Group co-chair – Microsoft

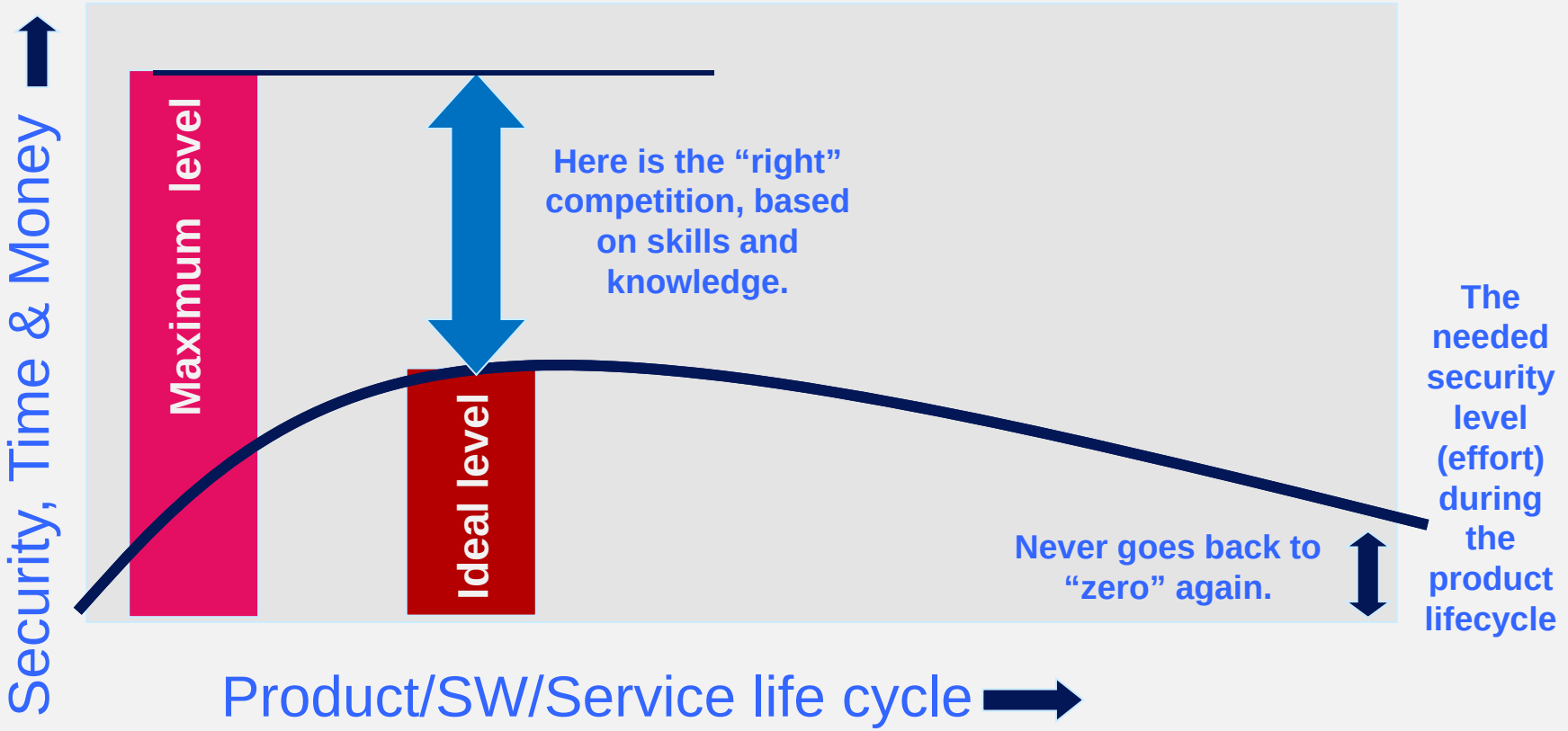
Copyright 2014 Trusted Computing Group

Some main principles

Copyright 2014 Trusted Computing Group

What is ”Secure enough” ?

How the competition works in the consumer product industry



Copyright 2014 Trusted Computing Group

HW security is matter of choice: an example



- **Virtual credentials protected by on-board trusted HW.**
- **Secure due to the use of hardware security, unlike in software-only credentials.**
- **Inexpensive to deploy because of already deployed generic secure hardware.**
- **Open in spirit to multi-application smartcards, but without issuer control.**

Copyright 2014 Trusted Computing Group

Security is not revolution, it's evolution

Copyright 2014 Trusted Computing Group

1998: The first “smart phone”, Nokia Communicator e-payment system



Hardware security protected peer-to-peer electronic payments over the Internet. Downloadable application from Nokia ”app store”. Device HW security was based on proprietary design.

2000: The first Nokia phone with digitally signed 3rd party apps



Applications were digitally signed by Nokia SW signing certificate. Signature was checked offline (by default) during the install phase. Online checking was user controllable. Application sideloading was possible.

2004: Trusted Execution Environment in action

- In addition to 3rd party application verification, the device had a Nokia proprietary secure execution environment in the baseband chip.
- This additional security was used in device production, integrity checking of firmware images, and with care-related services security.



2014: Full set of security features

- Firmware TPM
- Boot integrity / Secure boot
- Firmware integrity
- Application integrity
- Protected execution environment
- User data encryption
- OS Security features
- Remote wipe & location
- VPN connection
- Etc.



Nokia Lumia 930

TCG Mobile Platform Working Group

Copyright 2014 Trusted Computing Group

Mobile Platform Work Group

- **The Mobile Platform Work Group (MPWG) defines common functionality, interfaces, and a minimum set of implementation-agnostic requirements in specifications for basic mobile platforms that use TCG components to establish their root of trust**

- **MPWG's charter is to specify industry-standardised TPM functionality to improve mobile cross-platform security consistency and interoperability, to standardize logical TPM functionality for mobile device protected environments, to enable TPM support for legacy mobile security services, and to provide essential TPM security services for a broad range of mobile use cases and trusted applications, for basic mobile platforms**

- **MPWG enhances TCG as needed to address specific features of mobile devices like their untethered connectivity and limited capability as analyzed through various usage scenarios that may demonstrate the added value of mobile devices in TCG**

- **MPWG has broad mobile ecosystem representation amongst its membership including top players**

Copyright 2014 Trusted Computing Group

MPWG :: Ten Years Adding Trust

First industry-wide standardisation of mobile platform security; a lot has been done:

- Call for mobile security standardization at various industry conferences (2005 & 2006)
- Securing Mobile Devices on Converged Networks (White Paper September 2006)
- Mobile Trusted Module Overview Document (White Paper June 2008)
- Mobile Reference Architecture (Specification June 2008)
- Selected Use Case v1 Analysis Specification & Executive Summary (January 2009)
- Mobile Reference Architecture v1.0, Revision 5: Normative Requirements Check-list (June 2009)
- Mobile Trusted Module v1.0 Specification V1.0 R7.02 (June 2009)
- Mobile Reference Architecture v1.0 R5 (Specification April 2010)
- TCG Mobile Abstraction Layer (Specification April 2010)
- Mobile Trusted Module Specification (April 2010)
- Mobile Trusted Module FAQ (November 2010)
- Mobile Trusted Module 2.0 Use Cases & FAQ (May 2011)
- TPM Mobile with TEE for Comprehensive Mobile Device Security (White Paper June 2012)
- TPM 2.0 Mobile Reference Architecture Specification (April 2014) [review]
- TPM 2.0 Mobile Command Response Buffer Interface Specification (April 2014) [review]
- www.trustedcomputinggroup.org/developers/mobile

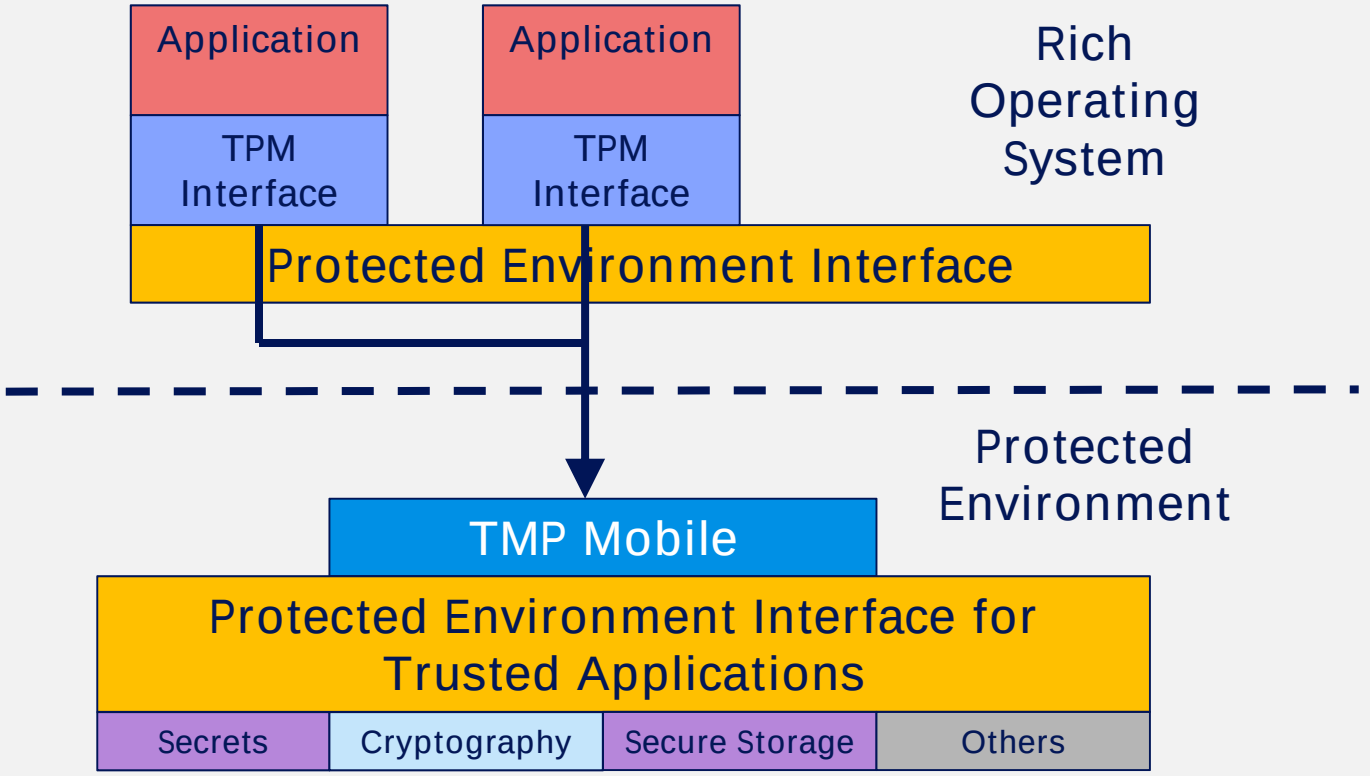
Copyright 2014 Trusted Computing Group

Mobile Use Cases

- **Consolidated collection of selected mobile usage scenarios where trusted computing principles strengthen mobile device security for the benefit of the end user and the service being used**
- **To guide subsequent technical requirements & specification work done by MPWG & to ensure that output meets real industry needs**
- **MTM 1.0 use cases (published 2005)**
  - **Platform Integrity**, **Device Authentication**, Robust DRM, SIMLock / Device Personalisation, **Secure SW Download**, Secure Channel between Device & UICC, Mobile Ticketing, **Mobile Payment**, Software Use, **User Data Protection and Privacy**
- **Selected Use Case Analyses (published January 2009)**
  - More detailed examination of most of the above-mentioned use cases
- **TPM 2.0 Mobile use cases (published 2011)**
  - **Mobile Banking**, Mobile Payment, Mobile Enterprise, **eHealth**, **Mobile Device Security & Identity**, App store, Automotive (latter now the focus of another TCG work group)

Copyright 2014 Trusted Computing Group

TPM Mobile & Protected Environment



Copyright 2014 Trusted Computing Group

TPM 2.0 Mobile Reference Architecture

- Core specification of security functional requirements
- Main concepts: Roots of Trust, Platform Integrity (Secure Boot & Measured Boot), Protected Environment (Secure Storage & Isolated Execution), Platform Configuration Registers (Measurement aggregation for eventual binding or attestation), Attestation (Device Identification & Device Authentication)
- Architecture described from perspective of implementation in a firmware-based protected execution environment
- Allows implementation choices - TPM in separate ASIC, TPM in separate processor on same ASIC, TPM on same processor using a TrustZone-like mechanism, TPM in a virtual machine
- Was in TCG member & public review until 3 June 2014
- www.trustedcomputinggroup.org/resources/tpm_20_mobile_reference_architecture_specification

Copyright 2014 Trusted Computing Group

Conclusions

Copyright 2014 Trusted Computing Group

Conclusions

- **Security is a business decision (for developers and platforms)**
- **One size does not fit all, but you can get pretty close**
- **Smart phone security is not only one thing, idea or ”security level”**
- **TPM Mobile a is versatile solution for mobile platform security**
- **Mobile industry has a great variety of choices for application developers**
- **Application security is also the developers’ choice**

Copyright 2014 Trusted Computing Group



Thank You

janne.uusilehto@microsoft.com