

Trust in Mobility: A New Standards-Based Approach to Securing Mobile Computing Devices, Software, and Applications

June 28, 2011

Janne Uusilehto

Chairman, TCG Mobile Working Group

Director, Head of Nokia Product Security

Janne.uusilehto@nokia.com

Mobile device facts

It is estimated that by 2015 the total number of global mobile subscribers will be close to 5 billion.*)

Mobile security is vital for many applications due need to protect the user assets (privacy), corporate assets (confidentiality), service provider assets (availability & authenticity).

How to make sure your business is having feasible reliability and adequate share of the responsibilities?



*) Source: Informa Strategic Market Report, Telecoms & Media, January 2011

There are many definitions for the product security

A product does what it is designed to.

Security is a process, not a product.

Product security is the incorporation into anything that Nokia productizes via security-related design, architecture, process, development, testing, release and maintenance.

Product security requires extra robustness and resistance for attacks against all parts of the architecture and functionality.

What security are you ?

- -Corporate Security – corporate physical assets & people
- -IT Security – corporate information assets and IT systems
- -Product & Services security – products, services & engineering
- -Security response – incident management & response

What is the key for trusted service?

Perfect HW security?

Application security?

Full encryption of the data?

Trusted UI?

State of the art usability?

Operating system security?

Access control systems?

Device/service management?

Excellent user manual?

Reactive processes for vulnerabilities?

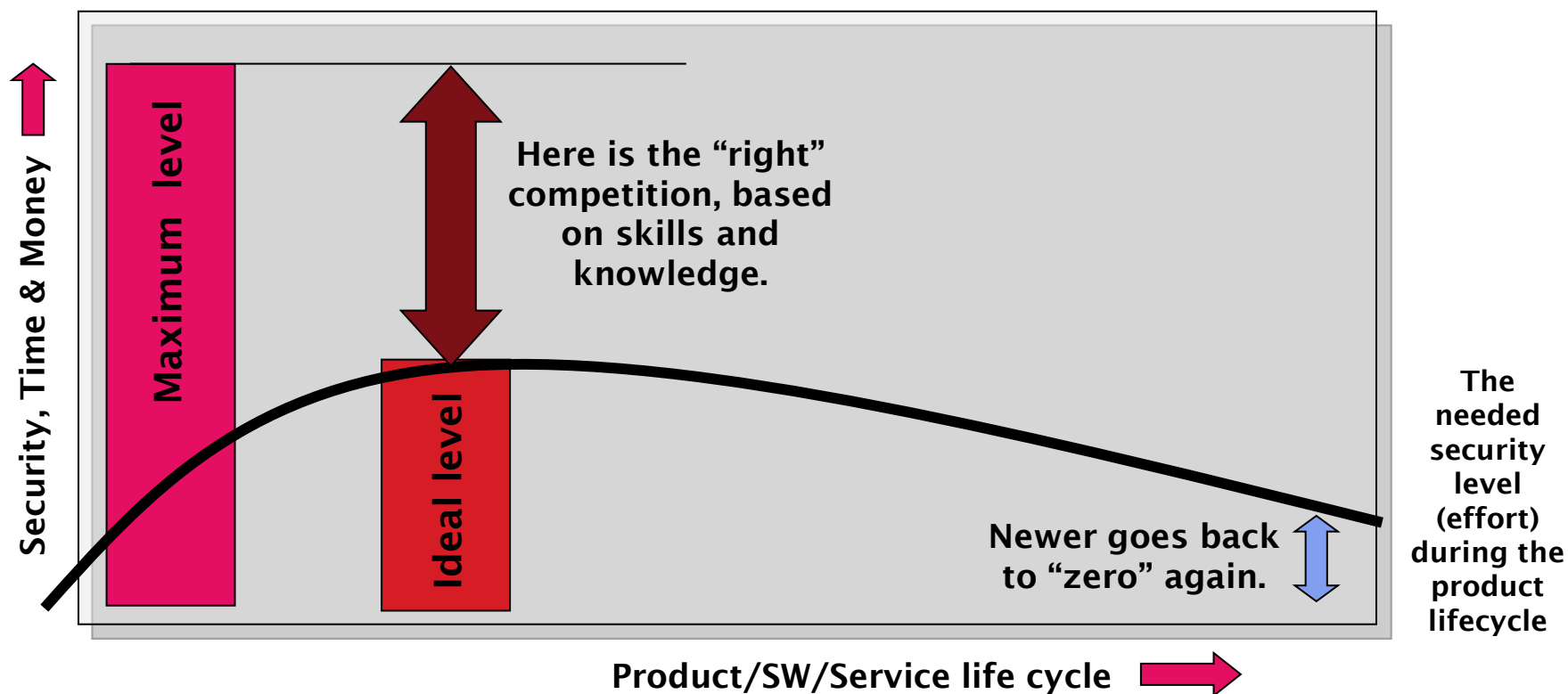
SW update capability?

Standardized security?



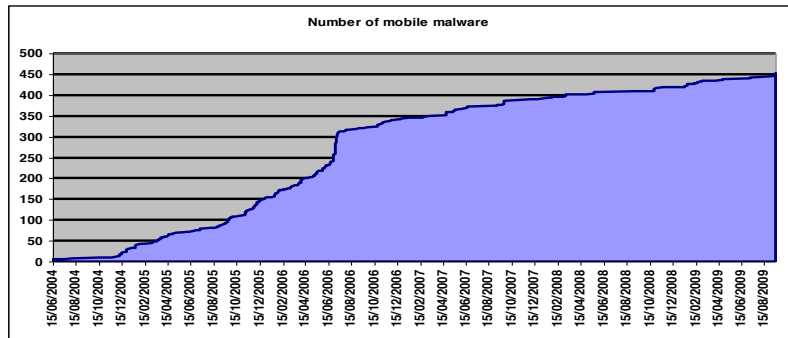
Matching security levels with product life cycle – the business case

How the competition is working in consumer product industry



Mobile malware status – Year 2009

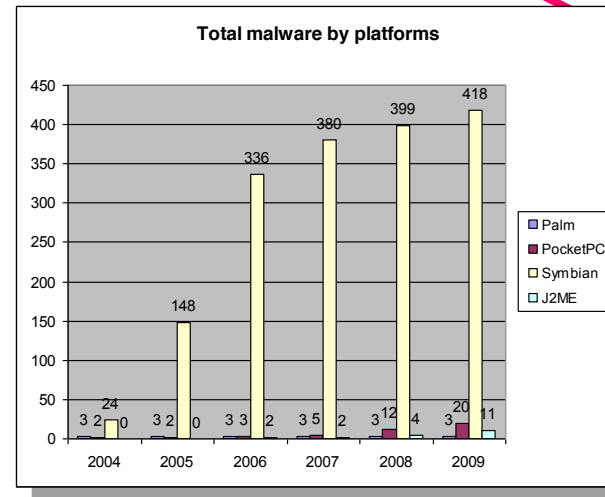
Total: amount of mobile malware (all mobile platforms): 454



Mobile Malware Development

Source: F-Secure Thu 26.11.2009, 20:2

Getting mobile malware statistics is currently not feasible as increase is so small.
ATTN: Web applications breakthrough may change this situation rapidly !!



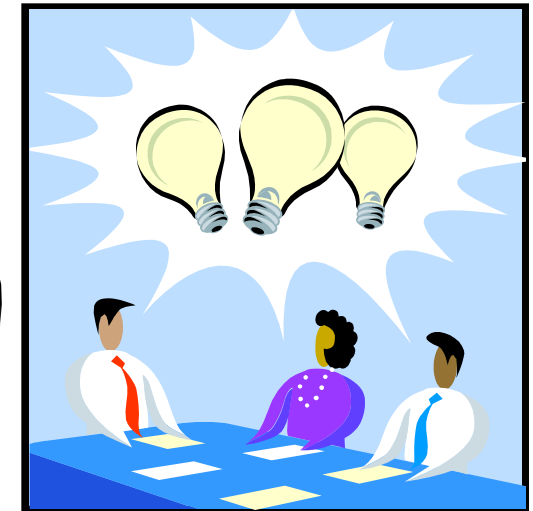
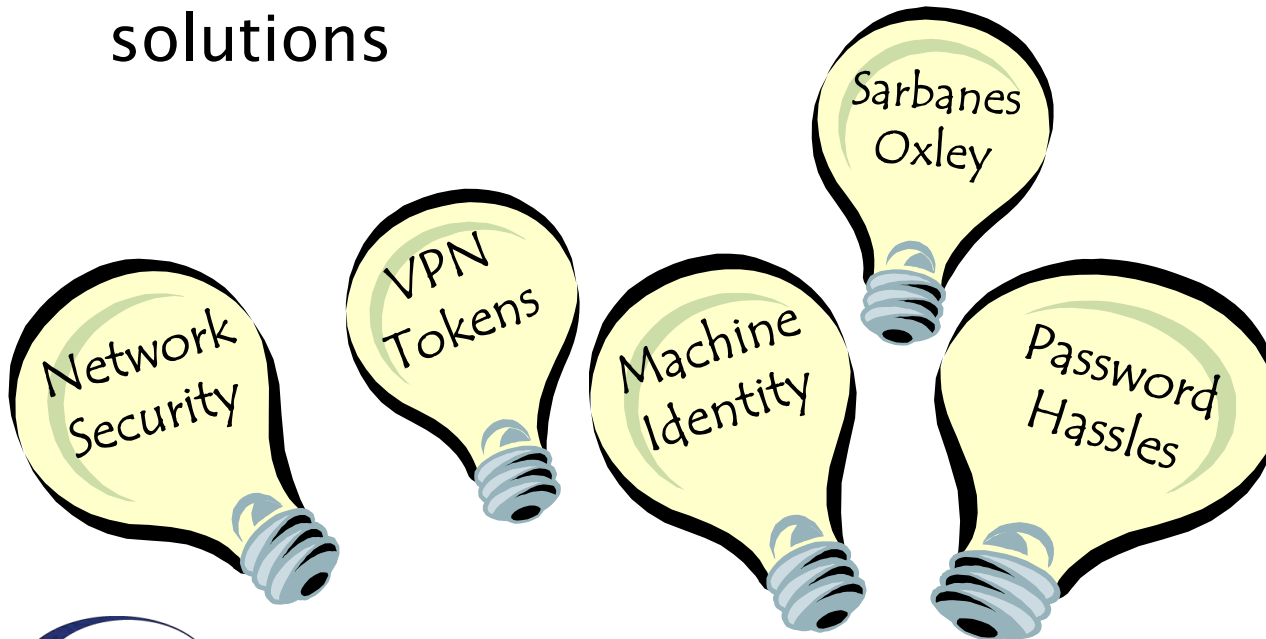
Note: According F-Secure they get about 200.000 malware samples every day. About 5000-6000 of them are real malware and few thousand of those completely new ones.

TOTAL CUMULATIVE AMOUNT over last 10 years of mobile malware for all mobile platforms is around 500.

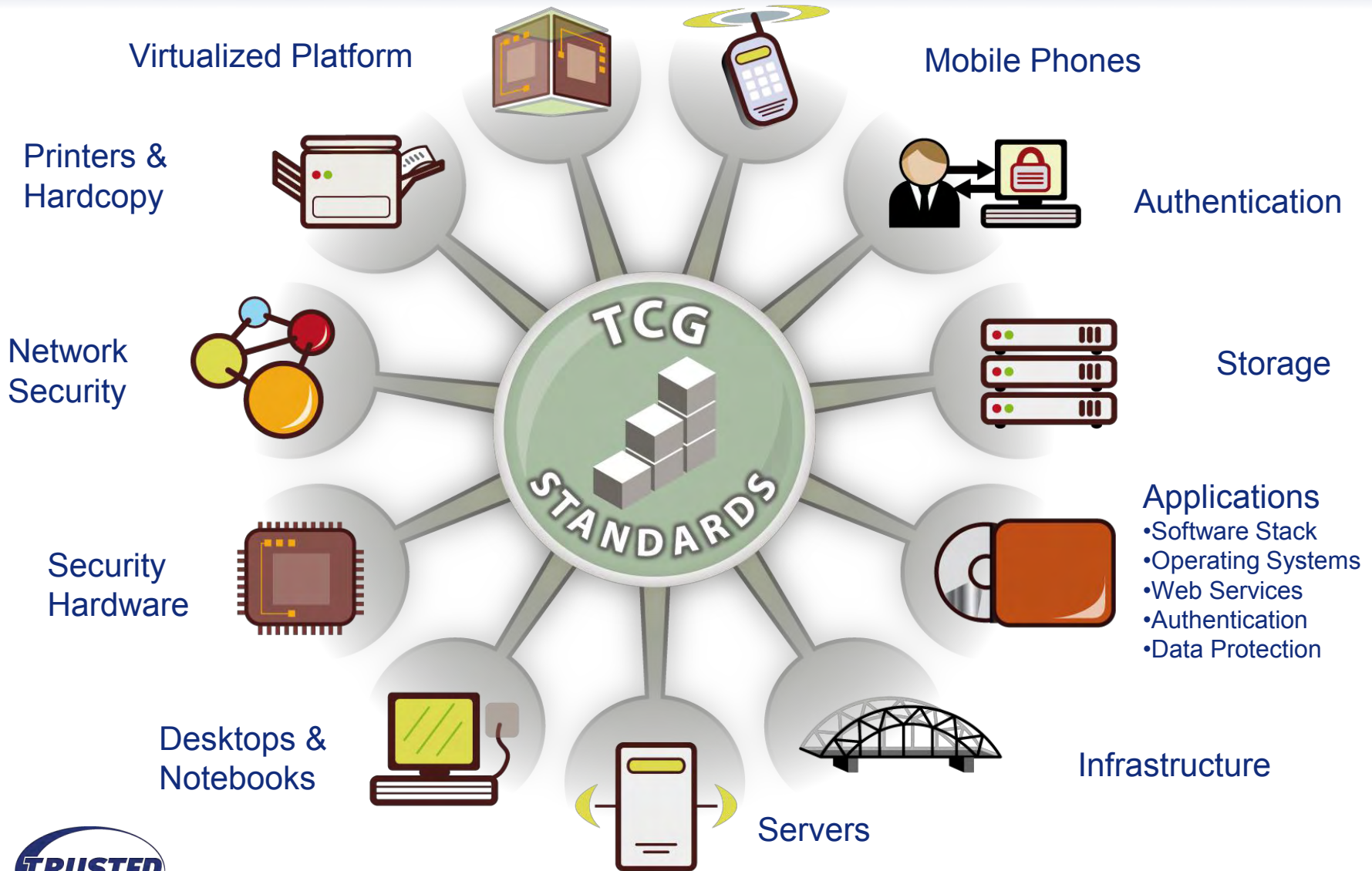
A Trusted Computing Foundation

Trusted Computing is:

- An Open, Vendor Neutral solution
- Interoperable across hardware vendors
- Significantly more efficient than existing security solutions



TCG: Standards for Trusted Systems



TCG - Mobile Working Group

Focusing on trusted computing for mobile devices with optimized HW security solution having multiple ownership model by default, but also architecture to support strong end user protection.

Is aiming for next generation of Mobile Trusted Device (MTM 2.0) in order to enable some security critical mobile applications on multiple platforms by transparent and standard way.



Rationale for use cases

- They are narratives that describe a context of related interactions between stakeholders in an ecosystem to enable a user to achieve a specific goal
- They suggest to developers what kind of functionalities might be needed to support certain applications that rely on e.g. security
- They identify threats to usage & propose countermeasures
- They provide a basis for extrapolating requirements & subsequently for deriving a specification
- The following MTM 2.0 use cases intend to outline the application of contemporary TCG techniques to mobile devices

MTM 2.0 use cases

- **e-Wallet: Mobile Banking**
- **e-Wallet: Mobile Payment**
- **Strong Mobile Authentication of Enterprise Employees**
- **e-Wallet: e-Health Application**
- Media Lending
- Device Management
- Identity Management
- **Vending Machines with Trusted Execution Environment**
- Application Store
- Device Interconnectivity in Vehicles



e-Wallet: Mobile banking, mobile payment

- How to protect mobile financial service (MFS) credentials & apps using a standardised secure element (SE) such as the MTM?
- MFS industry is seeking ways to secure mobile payments at a comparable level to chipcards
- Mobey Forum's "Alternatives for Banks to offer Secure Mobile Payments" white paper (April 2010), outlines opportunities for SEs like the MTM
- Multiple "White" SEs & collaborative mobile banking & payment business models are possible with standardised MTMs in conjunction with a Trusted Execution Environment (TEE) , MTM API, and remote attestation to services
- Besides the MTM and Trusted Execution Environment (TEE), it requires linking the ecosystem stakeholders, not least the end user, together to pass a transaction end-to-end
- Gartner's Dataquest Insight puts mobile payment amongst the Top Ten consumer mobile applications in 2012

Enterprise mobile user authentication

- How to enforce robust & scalable mobile user authentication in enterprise environments using the MTM as an enabler?
- Most enterprise breaches are attributed to weak or even absent user authentication
- Many sorts of tokens are in use & their maintenance is cumbersome and expensive
- An enterprise user authentication certificate can be enrolled into the MTM to enable logical (and optionally physical) access to the corporate environment
- MTM-facilitated user authentication can reinforce an enterprise's defense-in-depth

e-Health

- How to leverage the ubiquity of mobile devices to securely support healthcare monitoring (data to/from GP, local clinic, regional hospital, pharmacy)?
- Mobile devices with standardised MTMs, a TEE, MTM API, and attestation capability, can facilitate mobile e-Health, i.e. associated apps are stored on the device
 - The user's health credentials are secured in the MTM, are securely processed in a TEE, and communications to health services are attested
- Benefits of increased health monitoring frequency, cost savings, improved quality of care
- Mobile health monitoring is in its infancy & has generated a lot of interest from care deliver organisations (CDOs) & government healthcare agencies, e.g. an Austrian MOBITEL e-Health trial
- Gartner's Dataquest Insight puts mobile health amongst the Top Ten consumer mobile applications in 2012

Vending machines

- Is there a market for online and secure vending machine?
- The physical security of vending devices is a well-known problem, but as these devices get more sophisticated, the scope for electronic attacks widens
- With RFID-based payment systems, the back-end settlement service provider may require a minimum level of security within the software and hardware
- With a vending device certified to a standardised Protection Profile, the robustness of the vending machine can be demonstrated
- According to the EVA, NAMA and JVMA, in 2004 in the EU there were just over 3 million vending machines, Japan had almost 5 million, and the USA about 6 million

TCG: Design Objectives

- **TCG standards are designed with following considerations**
 - To promote worldwide interoperability and compatibility between implementations, through standard interfaces
 - To reduce costs for both suppliers and consumers
 - To drive development efficiency through standard protocols and mechanisms
 - To adopt standard publically available and internationally recognized security protocols and cryptography, which has been vetted through peer review, collaboration and other methods
 - To leverage a combination of hardware and software to create a safer computing environment

More about MTM and mobile security

<http://www.trustedcomputinggroup.org/developers/mobile>

