Brussels, 20 June 2012
Bibliothèque Solvay

EUROSMART
The Voice of the Smart Security Industry

Security and privacy in the digital world

Solutions from the Smart Security Industry

Security of Mobile Devices, Applications and Transactions

Jan EICHHOLZ

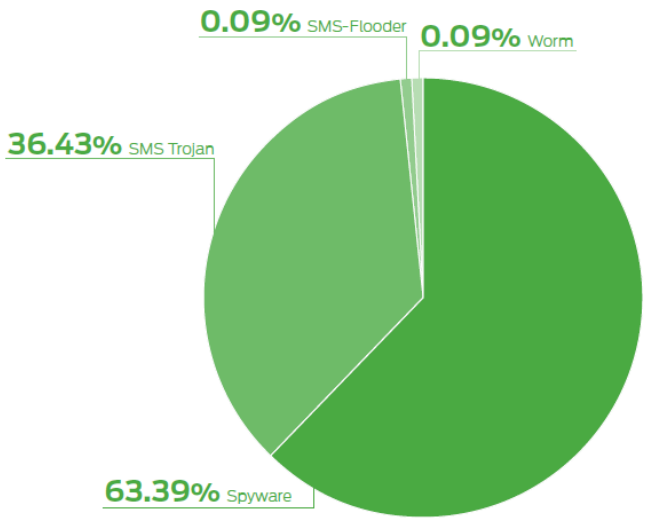
Authors
Daniel Borleteau
Nicolas Bousquet
Thierry Crespo
Xavier Dubarry
Jan Eichholz
Virginie Galindo

Agenda

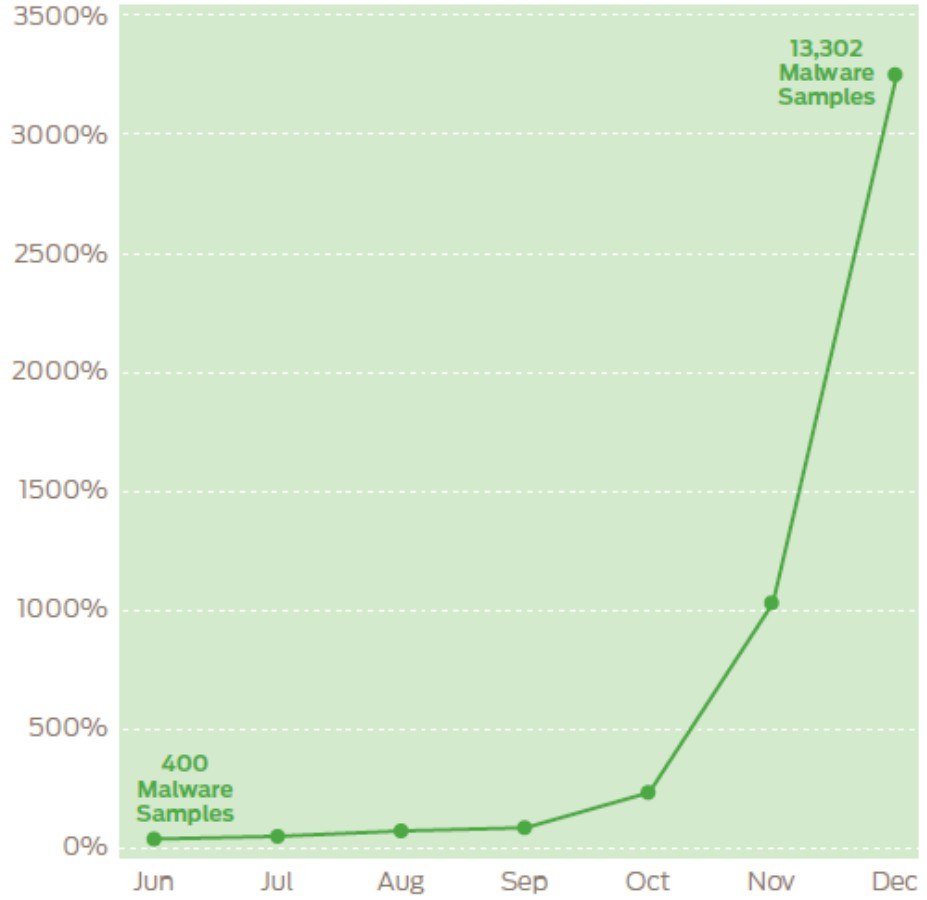
- **Mobile Devices and Security**
- **Government, Payment and other Services are going mobile**
- **Technologies for secure mobile devices**
  - The Trusted Execution Environment
  - The SIMAlliance Open Mobile API
  - Secure Elements
  - Trusted Service Management
- **Certification**
- **Summary**

Attacks are increasing

TYPES OF MALWARE TARGETING MOBILE DEVICES



CUMULATIVE ANDROID MALWARE INCREASE



Source: Juniper

Threats for mobile devices

- **Mobile devices hold significant amounts of personal information and sensitive credentials, which if stolen can be used for a variety of malicious purposes**

- **The mobile eco-system presents some characteristics on which attackers can take benefit**
  - Always-on – improving accessibility
  - Internet access through Browsers
  - Application markets
  - Wireless interfaces (WiFi, 3G, BT, NFC) vulnerable to „Man in the Middle“ or „Relay“ attacks

Agenda

- **Mobile Devices and Security**
- **Government, Payment and other Services are going mobile**
- **Technologies for secure mobile devices**
  - The Trusted Execution Environment
  - The SIMAlliance Open Mobile API
  - Secure Elements
  - Trusted Service Management
- **Certification**
- **Summary**

Accessing eGovernment Cloud Services

- **Provide strong authentication and access for eGovernment services**
- **Allow generation of qualified electronic signatures using a mobile device**

Wallets are migrating into Smartphones

Mobile as Wallet
(Convergence of applications)

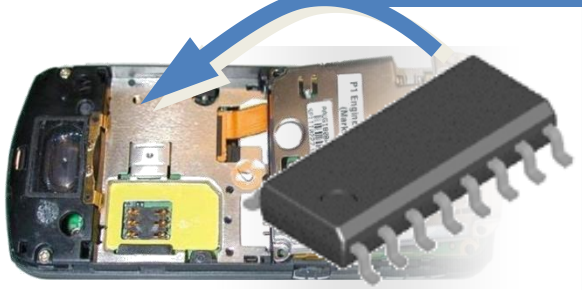
- **Local payment via NFC**
- **Mobile banking transactions**
- **Ticketing**
- **Identification**

Agenda

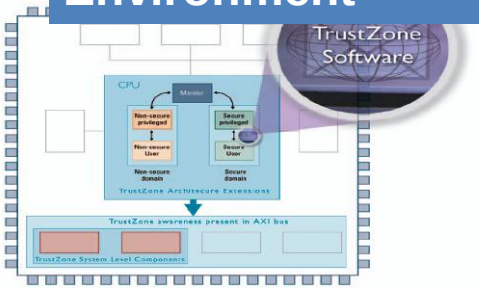
- **Mobile Devices and Security**
- **Government, Payment and other Services are going mobile**
- **Technologies for secure mobile devices**
  - The Trusted Execution Environment
  - The SIMAlliance Open Mobile API
  - Secure Elements
  - Trusted Service Management
- **Certification**
- **Summary**

Security Solutions for Trusted Services around the Mobile

Embedded SE



Trusted Execution Environment



Contactless card

Removable SE

SIM-based SE

SE = Secure Element

Trusted Execution Environment (TEE)

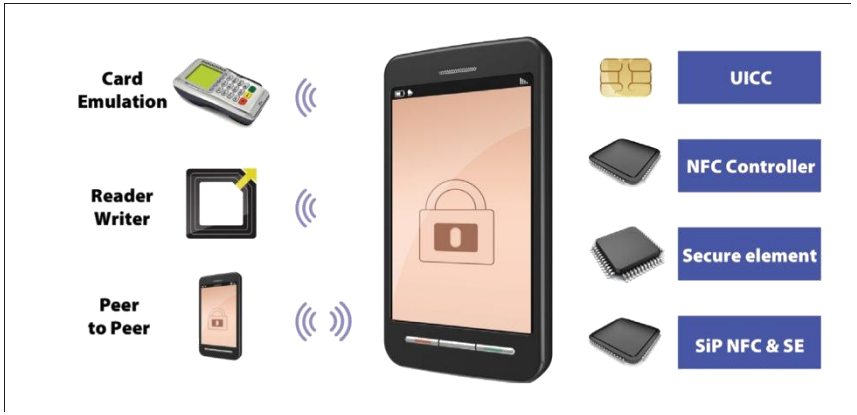
- **Is an isolated environment running aside the Smart Device operating system**
- **Hosts Trusted Applications deployed by Service Providers**
  - Insuring integrity and confidentiality of services
  - Providing isolation between Trusted and Normal Appliations
- **Provides some easy mean to build services based on**
  - Cryptography
  - Secure Storage
  - Secure Time
  - Secure screen display
- **Designed to allow efficient security certification**

SIMAlliance Open Mobile API

- **Enables Smart Phone Applications to access any Secure Elements in the device**
  - SIM card, µSD, embedded Secure Element, NFC
- **Can be implemented on any Smart Phone, whatever is their operating system**
  - Android version is available
- **Provides high level service to allow Smart Phone Application to**
  - Choose a Secure Element
  - Store data in Secure Element
  - Send service specific commands

Secure Elements – The Security Anchor

- Designed to strongly protect data (keys, personal information)
- Provides strong cryptography
- **Only certifiable device which resists side channel attacks** (Laser, power analysis, ...)
- Available in various form factors, with manifold interfaces
- Remotly manageable
- Interoperable through Standards

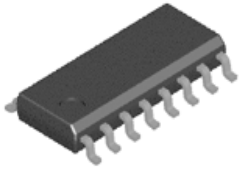


Secure Elements in Mobile Devices

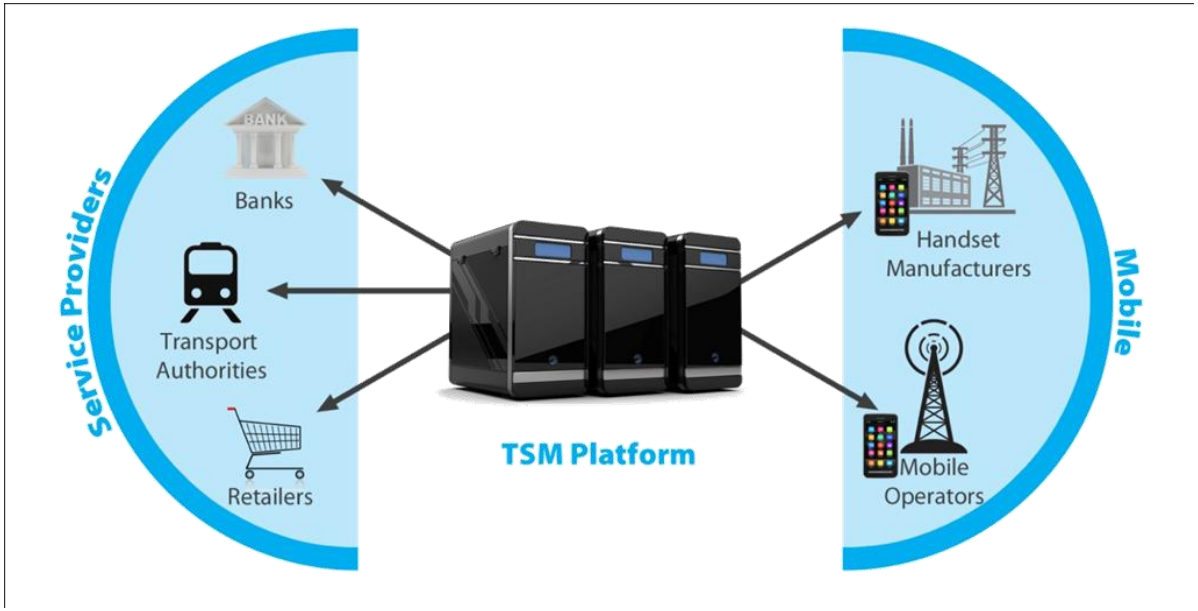
- **SIM**
  - owned by the mobile network operators
  - independent of the handset
  - over-the-air activation and management

- **Secure micro SD card**
  - Owned by a 3rd party (e.g. Bank)
  - Removeable

- **Embedded secure element**
  - Owned by the handset manufacturer
  - Remotely manageable

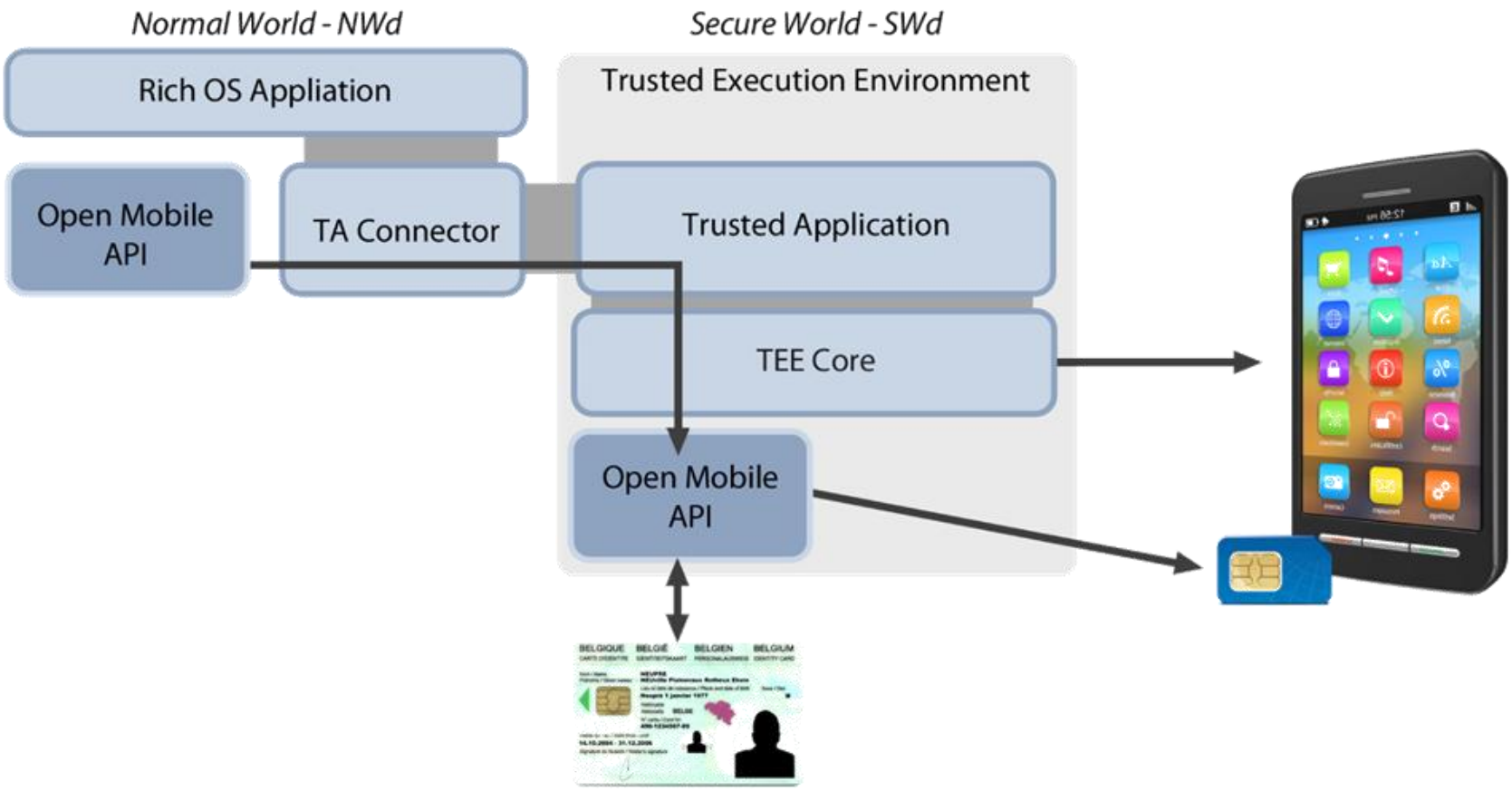


Trusted Service Management (TSM)



- **Over-the-air management of secure elements and trusted services**
  - Provisioning
  - Subscription
  - Deployment
  - Life cycle management

Security infrastructure



Agenda

- **Mobile Devices and Security**
- **Government, Payment and other Services are going mobile**
- **Technologies for secure mobile devices**
  - The Trusted Execution Environment
  - The SIMAlliance Open Mobile API
  - Secure Elements
  - Trusted Service Management
- **Certification**
- **Summary**

Security Certification

- **Measuring security is fundamental to offering to all stakeholders a high level and easy-to-read security classification.**

- **Major certification schemes are Common Criteria, EMVCo and FIPS**

- **Different technologies are requiring different levels of security certification.**
  - Being tamper resistant, smart secure devices offer guarantees of the highest level of security
  - TEE is targeting a balanced security certification insurance, compatible with Smart Phone lifecycle

Agenda

- **Mobile Devices and Security**
- **Government, Payment and other Services are going mobile**
- **Technologies for secure mobile devices**
  - The Trusted Execution Environment
  - The SIMAlliance Open Mobile API
  - Secure Elements
  - Trusted Service Management
- **Certification**
- **Summary**

Summary

- The need for better security for mobile devices, applications and transactions is growing in importance.
- Combining technologies like secure elements, Open Mobile API and Trusted Execution Environment will facilitate system-wide security for mobile applications and transactions.
- Security certifications are providing reliable and proven security solutions

THANK YOU FOR YOUR ATTENTION

ANY QUESTION ?

www.eurosmart.com