mobile business

Lecture 12

Mobile Trusted Devices

Mobile Business I (WS 2016/17)

Prof. Dr. Kai Rannenberg

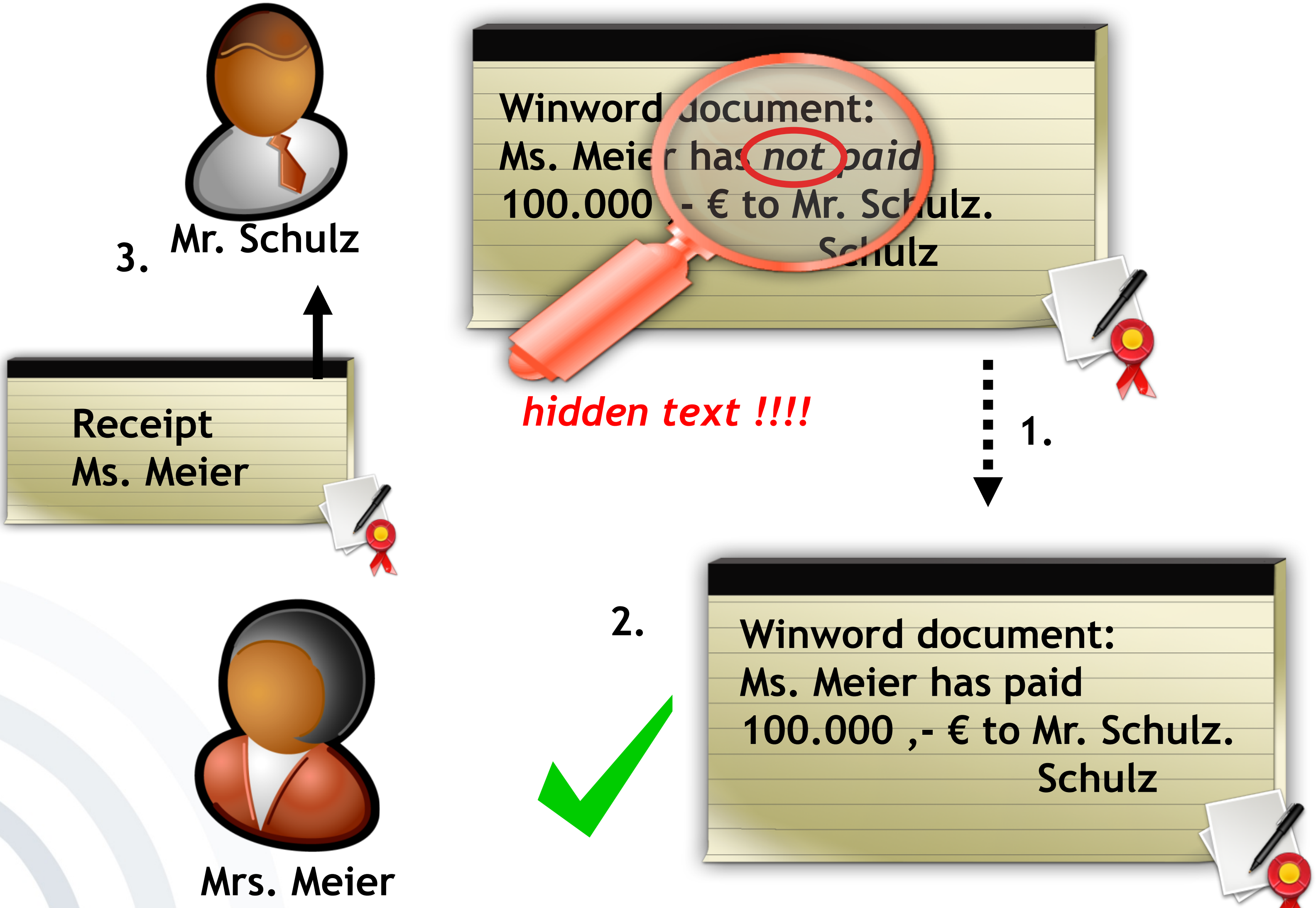
Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Presentation Problems



3. Mr. Schulz

Receipt
Ms. Meier

Mrs. Meier

Winword document:
Ms. Meier has *not* paid
100.000 ,- € to Mr. Schulz.
Schulz

hidden text !!!!

1.

2.

Winword document:
Ms. Meier has paid
100.000 ,- € to Mr. Schulz.
Schulz

Based on [Isselhorst and Rohde]

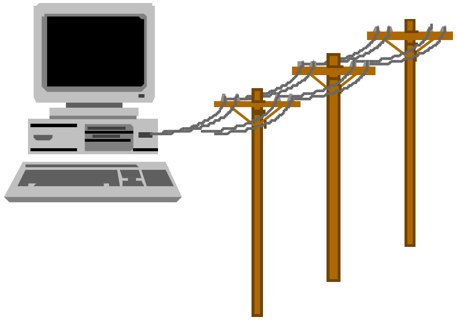
SigG-Requirements to Technical Components

Example: display of data (§ 17(2))

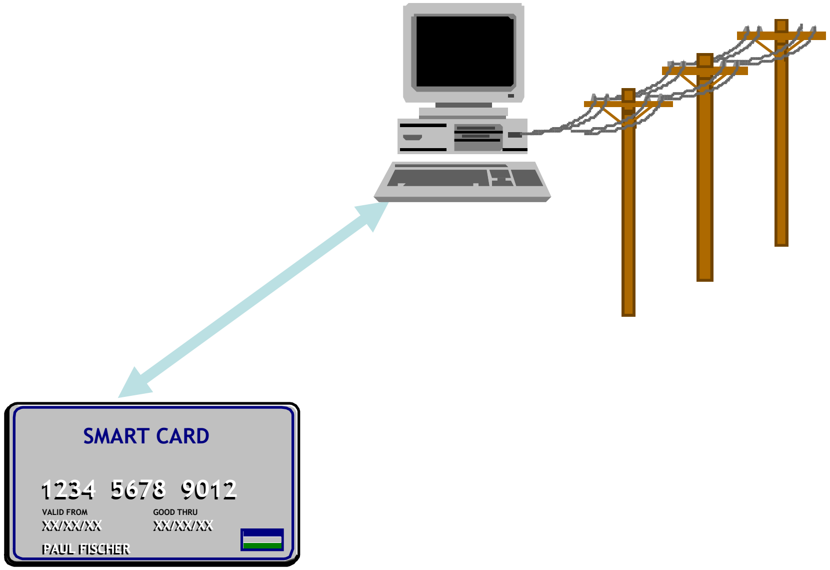
- Explicit indication before a signature is being created
- Perceptibility which data the signature refers to
- Accordance of displayed data and signed data (“What you see is what you sign.”)

Secure Equipment

Threats from Trojan Horses



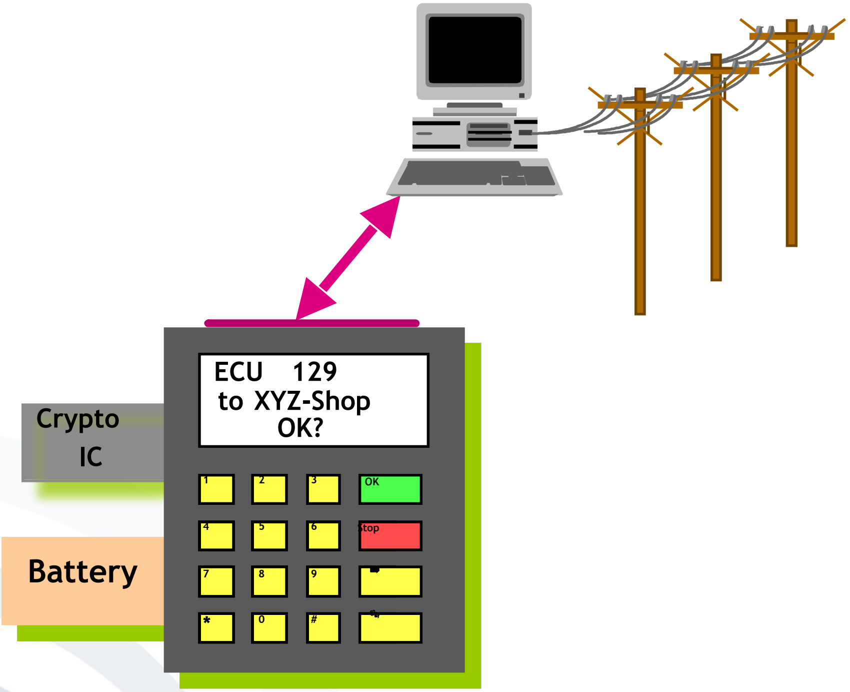
Private key on HD, in memory



Private key and signature function in chip card

Secure Equipment

Avoiding Threats from Trojan Horses



Wallet with private key and signature function

Secure Equipment

How to view a document

Order

Buyer's organization, address, country
Tel./fax/email/URL
Company registration no.
VAT-No.
Buyer’s name
Certificate
Seller's organization, address, country
Seller’s name
Date
Buyer's reference number
Content description
Seller's article number
Buyer's article number
Number of items
Unit of item
Item price
Tax
Freight and delivery
Total
Currency
Shipping address
Comments
Appended files
Applicable Law
Agreed means of payment
Payment agreed by
Buyer’s signature

Split User Interface

← **All fields on normal screen**

Essential fields on secure hardware

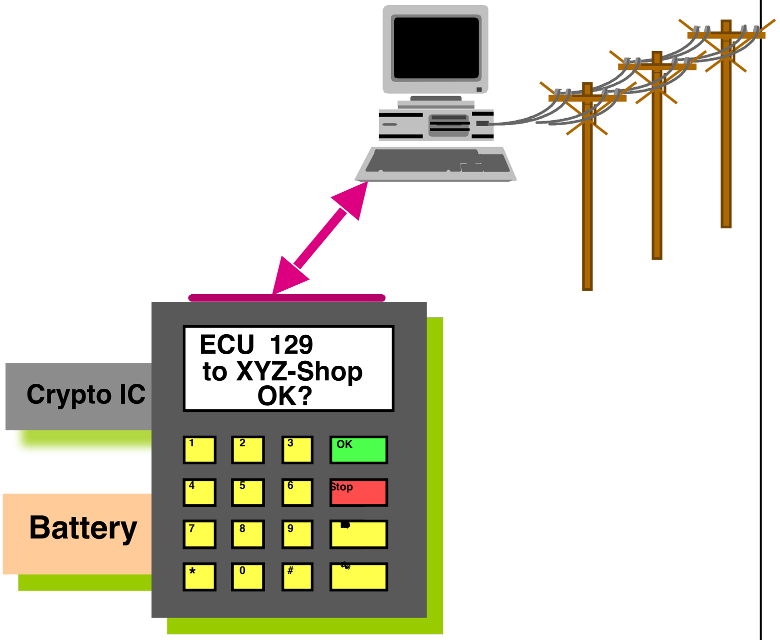
↓

Order

Buyer
Certificate
Date
Description
Total
Currency
Signature

A popular vision: Security Assistants

- Storing personal data
  - Addresses, calendars
  - Money, keys
  - Preferences …
- Performs sensitive processes
  - Decoding of confidential messages
  - Signature creation
- Assists negotiations
  - Documents which are accepted by other parties
  - Methods of payment
  - Reachability



Challenges of Personal Terminals

- Usability
  - Portability
  - Good visibility of important information („new network“)
  - Adequate representation of the functionality
- Protection from
  - Unauthorized access to stored data
  - Manipulation of the functionality (e.g. “Trojan Horses”)
  - Denial-of-Service attacks
- Trust (of non-experts)
  - Does the equipment do what it shall do?
  - How (much) can I trust it?

Personal Security Assistants Platforms?

- Personal digital assistants
- Mobile phones
- Watches
- Pens
- Chip cards
- …

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Once upon a time …

- Closed platforms
- No additional software could be installed.
- Limited functionality

[Source: Nokia]

Mobile Devices Today

- Open platforms
- Lots of software can be installed:
  - For different purposes
  - From different vendors
- Communication with different protocols possible:
  - GSM/GPRS, UMTS, LTE
  - Bluetooth, Infrared, WLAN, NFC
- Private and confidential data can and will be stored on the mobile device.
- Camera is (in many cases) included.

[Source: Sony]

Mobile Devices Today

Risks

- Risks of Malware
  - Viruses, Worms, Dialler, Trojan Horses, etc.
- Passwords can (and will most likely) be deactivated.
- External storage media enables potential attackers to steal private information.
- Different communication protocols can be used to attack device or steal data.
- Camera also introduces new risks:
  - Stealing paper-based confidential information
  - Invasion of personal privacy
- Powerful attackers with a clear business and operational case

System Error

Windows Phone has encountered a fatal disk corruption error. Your device will now shut down and attempt a factory restore to recover the corrupt operating system sector. If your device is unable to restore successfully, please contact customer support.

Error Code: 0x8d53001d

Hardware-Störung:
Kamera neu start.

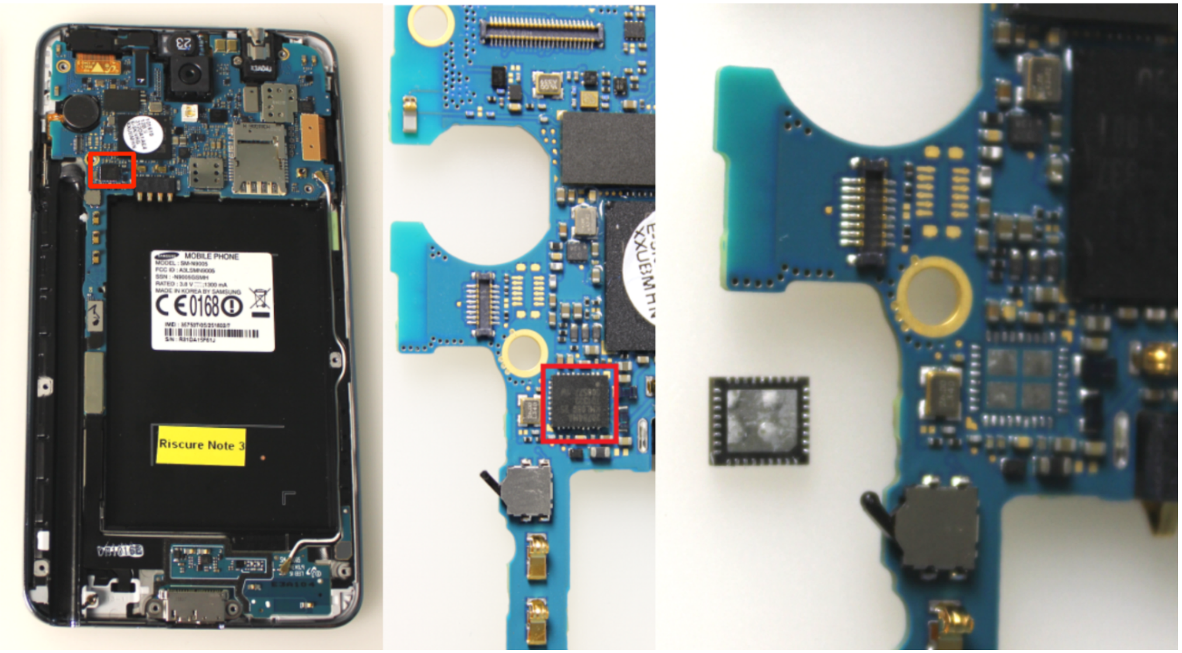
Secure Element (SE)

- Secure Elements (SE) are hardware tokens that offer secure services, e.g. tamper-proof storage and cryptographic operations.

  - Smart card (contact or contactless)
  - SIM/UICC cards
  - Smart/Secure microSD cards
  - Embedded Secure Elements (eSE)

Embedded Secure Element (eSE)

- Secure microcontroller
- Unremovable part of the mainboard of the device (usually a smartphone)
- Interchanging or extraction of the secure element is not possible (unlike other SE form factors).
- eSE use various types of interfaces (SWP, DWP, I2C, USB, proprietary interface).



[Riscure 2014]

Interest in Trusted Computing

- Trend from open platforms to open and trusted platforms
- Risks coming with the openness
- Trusted Computing for mobile platforms promises open and secure systems.
- Considered important in industry
- Many initiatives, approaches and players in the mobile communication industry

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Standardisation Activities

Organization/ Project	Participants	Goals	Results
Mobile Phone Work Group of the TCG (since 2005)	Nokia and a "large number of wireless vendors, component manufacturers and mobile service or content providers"	Adaptation of TCG specifications to mobile device requirements	Reference Architecture and trusted Module Specification
Trusted Mobile Platform project (2003/2004)	Intel, IBM, NTT DoCoMo	Architecture definition of a trusted execution environment at different trust levels	Hardware and Software Architecture Description, Protocol Specification
GSM Association / Mobile Application Security	Mobile Operators (Vodafone, Orange, T-Mobile, France Telecom)	Definition and promotion of a Mobile Application Security Framework for open operation system platforms	Application Security Terminal Requirements based on domain model and terminal security policies, Application Certification Program
OMTP Group (till 2010) Application Security Project Trusted Environment Project	Mobile Operators, Equipment Manufacturers, Service Providers	Recommendation for open mobile platforms establishing an open framework for mobile device manufacturers and associated software and hardware suppliers Development of the Mobile Application Security Framework Requirement definition for hardware-based security functions	Application Security Framework
Security Working Group of the Open Mobile Alliance (OMA)	Mobile Operators, Equipment Manufacturers, Service Providers	Specification of the operation of security mechanisms, features and services for mobile clients, servers and related entities	Specifications of Wireless Transport Layer Security, Wireless Identity Module, Wireless Public Key Infrastructure, Smartcard Web Server, and other requirements for application layer and transport layer security

Based on [PiskRannRoss2005]

Trusted Computing Group (TCG)

- Consortium of (more than 100) companies
- Initiative founded in 2003 as successor to the Trusted Computing Platform Alliance (TCPA)
- Led by AMD, Cisco, Fujitsu, HP, IBM, Infineon, Intel, Juniper, Lenovo, Microsoft and Wave
- Goal: implement trusted computing
- www.trustedcomputinggroup.org

Trusted Computing Group (TCG)

- About:

  “The Trusted Computing Group (TCG) is a not-for-profit organization formed to develop, define and promote open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.”

  [TCG2014]

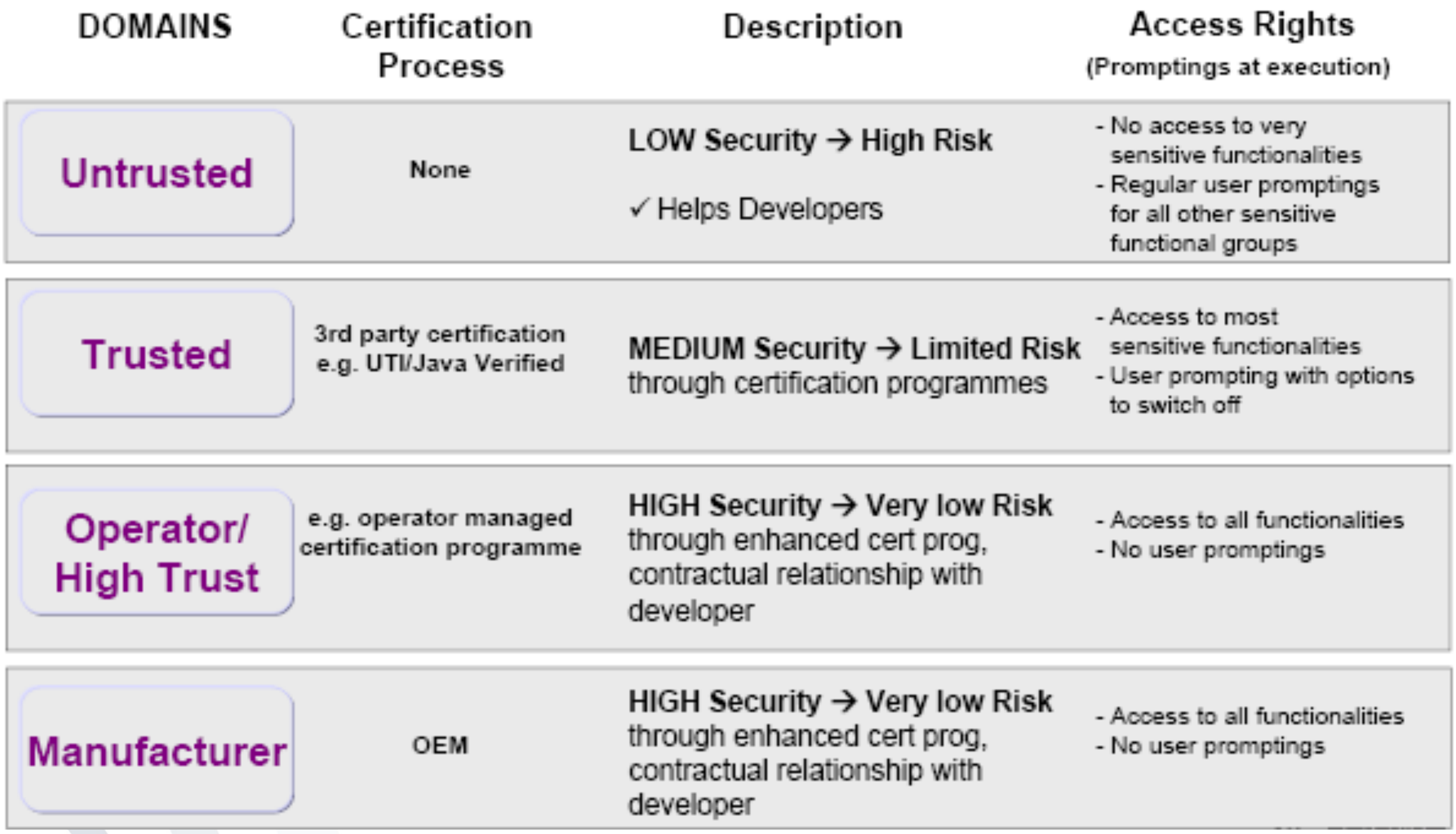
Trusted Platform Module (TPM)

- The TPM is a chip to make computers more secure as a part of the TCG specification.
- It is like a hard coded smartcard with the big difference that it is not bound to a concrete user, but to a system (e.g. a PC).
- ***Other usages***: PDAs, mobile devices, and consumer electronics.
- Passive chip, can neither influence the booting process nor the operation directly
- Has a unique identifier and so serves for the identification of the system.

Identities and Attestation

- Feature: User shall be able to make provable statements.
- Problem: to secure the provability, the statement has to come from the TPM. Furthermore the TPM has to prove that it is a real TPM:
  1. It has to be possible that corrupt TPMs may be barred from the process.
  2. For privacy reasons a TPM should not have a recognisable identity.
- Solution via:
  - Trusted third parties
  - Zero-knowledge proof

Mobile Application Domains according to GSMA



DOMAINS	Certification Process	Description	Access Rights (Promptings at execution)
Untrusted	None	LOW Security → High Risk ✓ Helps Developers	- No access to very sensitive functionalities - Regular user promptings for all other sensitive functional groups
Trusted	3rd party certification e.g. UTI/Java Verified	MEDIUM Security → Limited Risk through certification programmes	- Access to most sensitive functionalities - User prompting with options to switch off
Operator/ High Trust	e.g. operator managed certification programme	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	- Access to all functionalities - No user promptings
Manufacturer	OEM	HIGH Security → Very low Risk through enhanced cert prog, contractual relationship with developer	- Access to all functionalities - No user promptings

[GSM2005]

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

(Mobile) Equiment Identifier

- IMEI (“international mobile equipment identity“)
- IMSI („international mobile subscriber identity“)
- Apple Unique Device Identifier (UDID)
  - Combination of 40 numbers and letters
- Google Android ID
  - Can be changed by user with factory reset
- Trusted Platform Module (TPM)
  - (Public part of the) Endorsement Key (EKpub)

(Mobile) Equiment Identifier

- IMEI, IMSI, UDID, Android ID, TPM: Who knows the user‘s identity and interprets the user‘s behaviour?

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Mobile Market Players

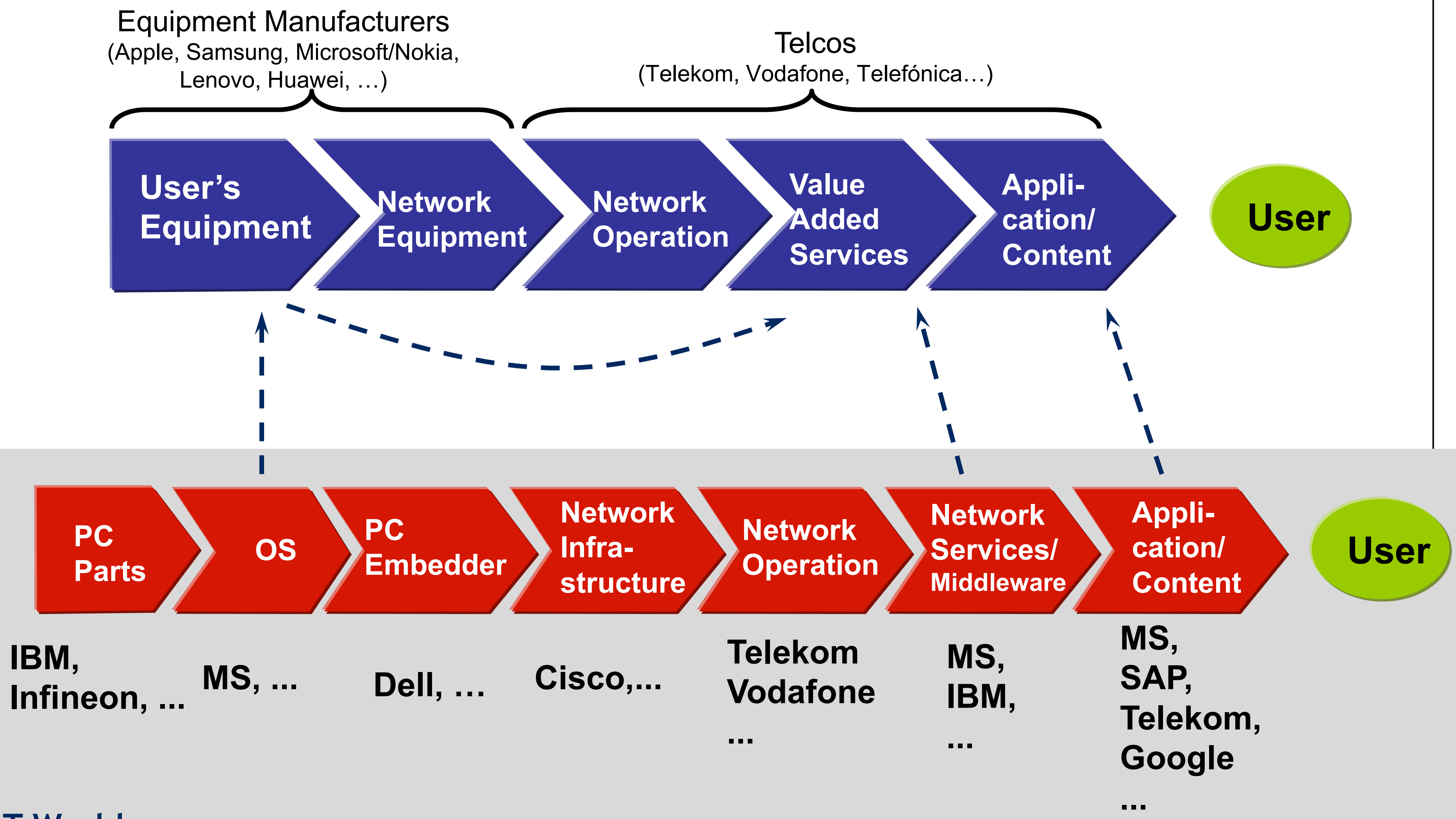
- Mobile equipment manufacturers
- (Mobile) Telecom Operators
- MVNOs
- Content providers
- Application service providers
- Private customers
- Corporate buyers
- Corporate users
- Intelligence agencies

Mobile Equipment Manufacturers

- In the past, main manufacturers of mobile devices were mobile phone manufacturers (e.g. Nokia, Motorola), producing both hardware and the software.
- Meanwhile the value chain for mobile devices has become more complex: Significant parts may come from third parties, e.g.
  - hardware from ARM, Infineon, Texas Instruments,
  - software from Google, Microsoft.
- The more a manufacturer is perceived as the provider of the respective platform, the more risks of the mobile platform are affecting them.
- Today, mobile devices are sold particularly as part of a powerful ecosystem (Google, Apple, Microsoft).

Mobile equipment & IT value chain

GSM World



Equipment Manufacturers
(Apple, Samsung, Microsoft/Nokia, Lenovo, Huawei, …)

Telcos
(Telekom, Vodafone, Telefónica…)

User's Equipment

Network Equipment

Network Operation

Value Added Services

Appli-cation/ Content

User

PC Parts

OS

PC Embedder

Network Infra-structure

Network Operation

Network Services/ Middleware

Appli-cation/ Content

User

IBM, Infineon, ...

MS, ...

Dell, …

Cisco,...

Telekom Vodafone ...

MS, IBM, ...

MS, SAP, Telekom, Google ...

IT World (based on [SAP])

(Mobile) Telecom Operators

- Functions of mobile operators that relate to trusted computing:
  - operate networks,
  - provide communication services,
  - maintain direct customer relationships,
  - provide mobile devices to customers (often by subsidising their costs).
- Powerful players in the mobile market:

T Deutsche Telekom

Telefonica

vodafone

中国移动通信
CHINA MOBILE

Mobile Virtual Network Operators

Definition:

A **mobile virtual network operator** (MVNO) is a company that does not own a licensed frequency spectrum and wireless infrastructure, but resells wireless services under their own brand name, using the network of another mobile network operator.

Explanation:

- An MVNO's roles and relationship to the mobile phone operator vary by market.
- In general, an MVNO is an entity or company that works independently of the operator and can set its own tariff structures.

congstar
blau MOBILFUNK
TURKCELL EUROPE
ortel MOBILE
ALDI TALK MEDION mobile
mobilcom debitel
simyo
FONIC
Das ist die Wahrheit.
1&1

Content Providers

- Are producing and/or distributing digital content (e.g. music, movies, games, ring tones, TV)
- Interest in:
  Securing their property rights on the provided content
  ➲ Digital Rights Management (DRM)

BMG
BERTELSMANN
JESTA digital
SONY PICTURES
20th Century Fox
Paramount
warner | music | group
EMI
viacom
NBCUniversal
Walt Disney PICTURES
THE WALL STREET JOURNAL.
Spotify

Application Service Providers

- Providing mobile application services (e.g. LBS, mobile banking, mobile payment services)
- Interest in:
  Ensuring that the devices used by customers for authenticating transactions are not compromised.

iZettle PayPal finanz informatik WHERIFY Wireless Location Services

Private Customers

- Usually not concerned about security of their mobile device.
- Interest in:
  Functionality, usability and design properties of their mobile device

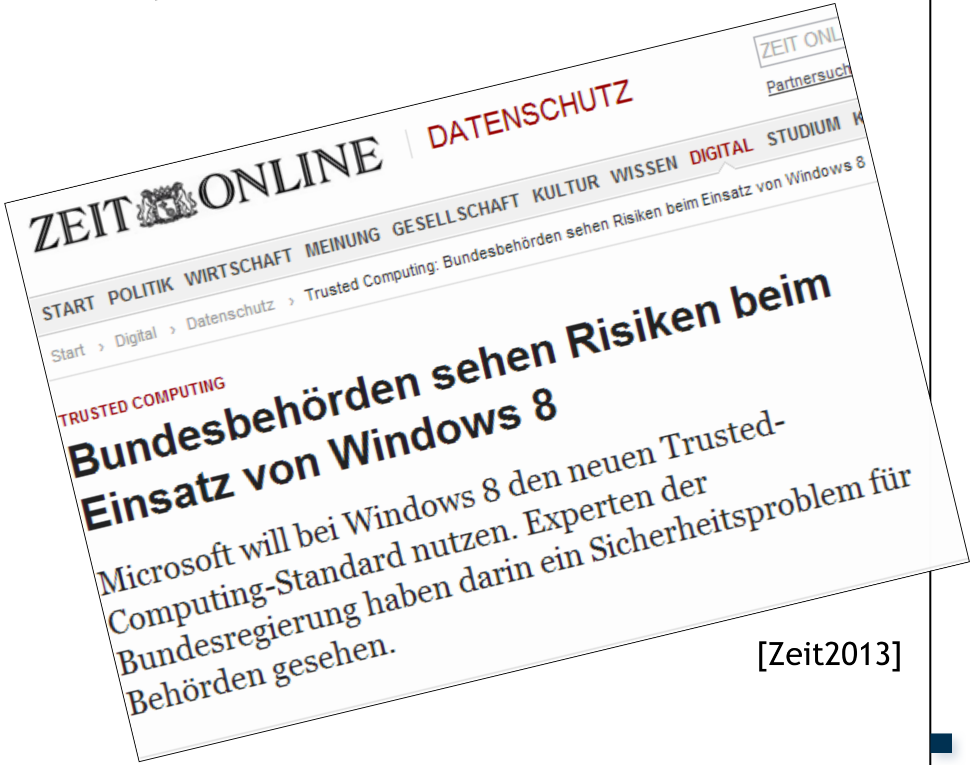
➲ Security failures are perceived as a mistake made by the device manufacturer/mobile OS provider/ mobile network operator.

Corporate Buyers

- IT managers, technical staff and system administrators
- Concerned about mobile devices and mobile access causing security holes in their enterprise system.

➲ Most security-conscious customers

➲ Benefit from Mobile Device Management solutions (cf. Section “Usage Scenarios for Trusted Mobile Platforms”)


ZEIT ONLINE | DATENSCHUTZ

ZEIT ONL

Partnersuch

START POLITIK WIRTSCHAFT MEINUNG GESELLSCHAFT KULTUR WISSEN DIGITAL STUDIUM K

Start › Digital › Datenschutz › Trusted Computing: Bundesbehörden sehen Risiken beim Einsatz von Windows 8

TRUSTED COMPUTING

Bundesbehörden sehen Risiken beim Einsatz von Windows 8

Microsoft will bei Windows 8 den neuen Trusted-Computing-Standard nutzen. Experten der Bundesregierung haben darin ein Sicherheitsproblem für Behörden gesehen.

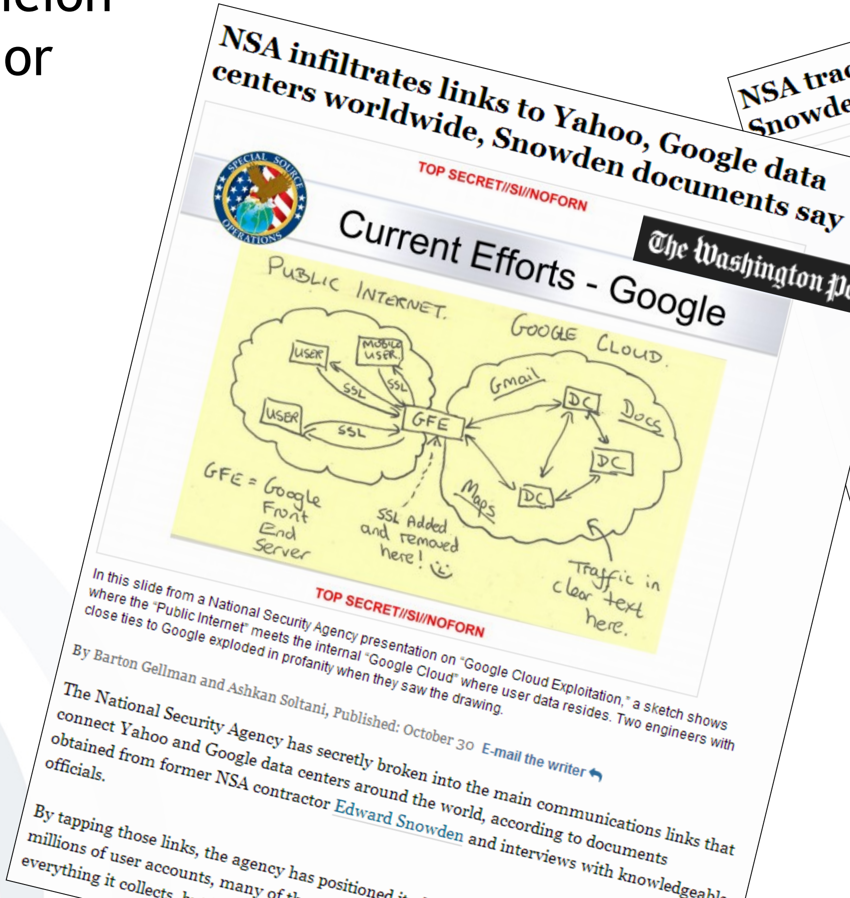
[Zeit2013]

Corporate Users

- Are using mobile infrastructures predominantly for business needs.
- Like private users, but with usage restrictions imposed by employers or (Mobile)OS for security purposes
    - This includes corporate users who are allowed to bring and use personally owned mobile devices (*Bring your own device - BYOD*)

Intelligence Agencies

- Eavesdrop (and manipulate?) globally exchanged information to gather intelligence, regardless of whether a suspicion exists or not.



NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say

The Washington Post

TOP SECRET//SI//NOFORN

Current Efforts - Google

SPECIAL SOURCE OPERATIONS
PUBLIC INTERNET
GOOGLE CLOUD
USER
MOBILE USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! ☺
Traffic in clear text here.

TOP SECRET//SI//NOFORN

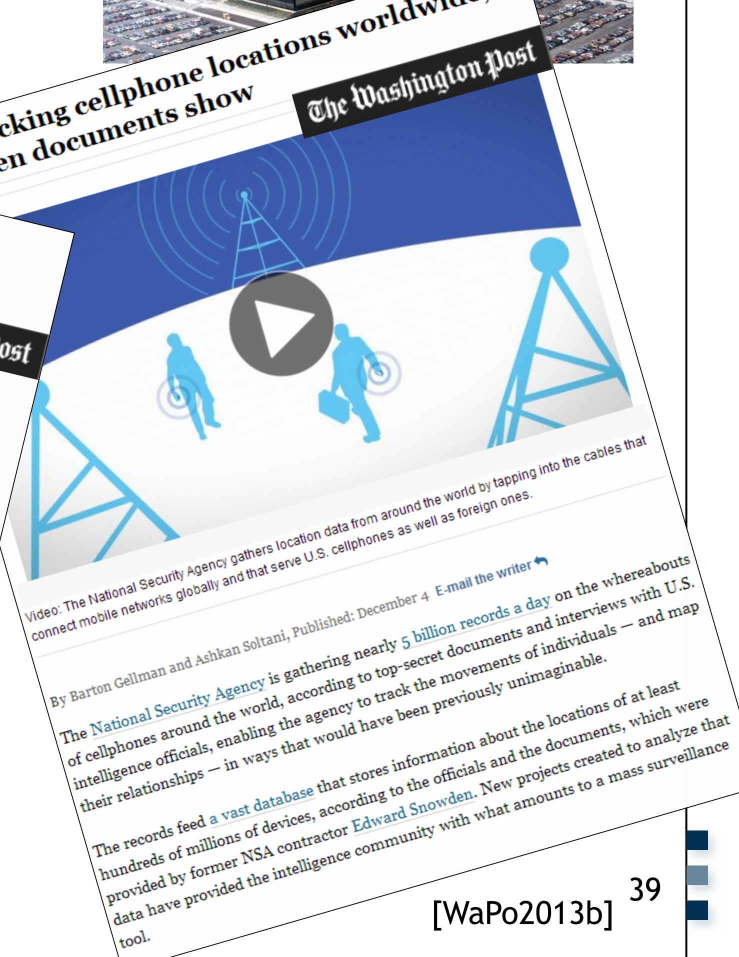
In this slide from a National Security Agency presentation on "Google Cloud Exploitation," a sketch shows where the "Public Internet" meets the internal "Google Cloud" where user data resides. Two engineers with close ties to Google exploded in profanity when they saw the drawing.

By Barton Gellman and Ashkan Soltani, Published: October 30 E-mail the writer

The National Security Agency has secretly broken into the main communications links that connect Yahoo and Google data centers around the world, according to documents obtained from former NSA contractor Edward Snowden and interviews with knowledgeable officials.

By tapping those links, the agency has positioned it
millions of user accounts, many of th
everything it collects

[WaPo2013a]



NSA tracking cellphone locations worldwide, Snowden documents show

The Washington Post

Video: The National Security Agency gathers location data from around the world by tapping into the cables that connect mobile networks globally and that serve U.S. cellphones as well as foreign ones.

By Barton Gellman and Ashkan Soltani, Published: December 4 E-mail the writer

The National Security Agency is gathering nearly 5 billion records a day on the whereabouts of cellphones around the world, according to top-secret documents and interviews with U.S. intelligence officials, enabling the agency to track the movements of individuals — and map their relationships — in ways that would have been previously unimaginable.

The records feed a vast database that stores information about the locations of at least hundreds of millions of devices, according to the officials and the documents, which were provided by former NSA contractor Edward Snowden. New projects created to analyze that data have provided the intelligence community with what amounts to a mass surveillance tool.

[WaPo2013b]

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

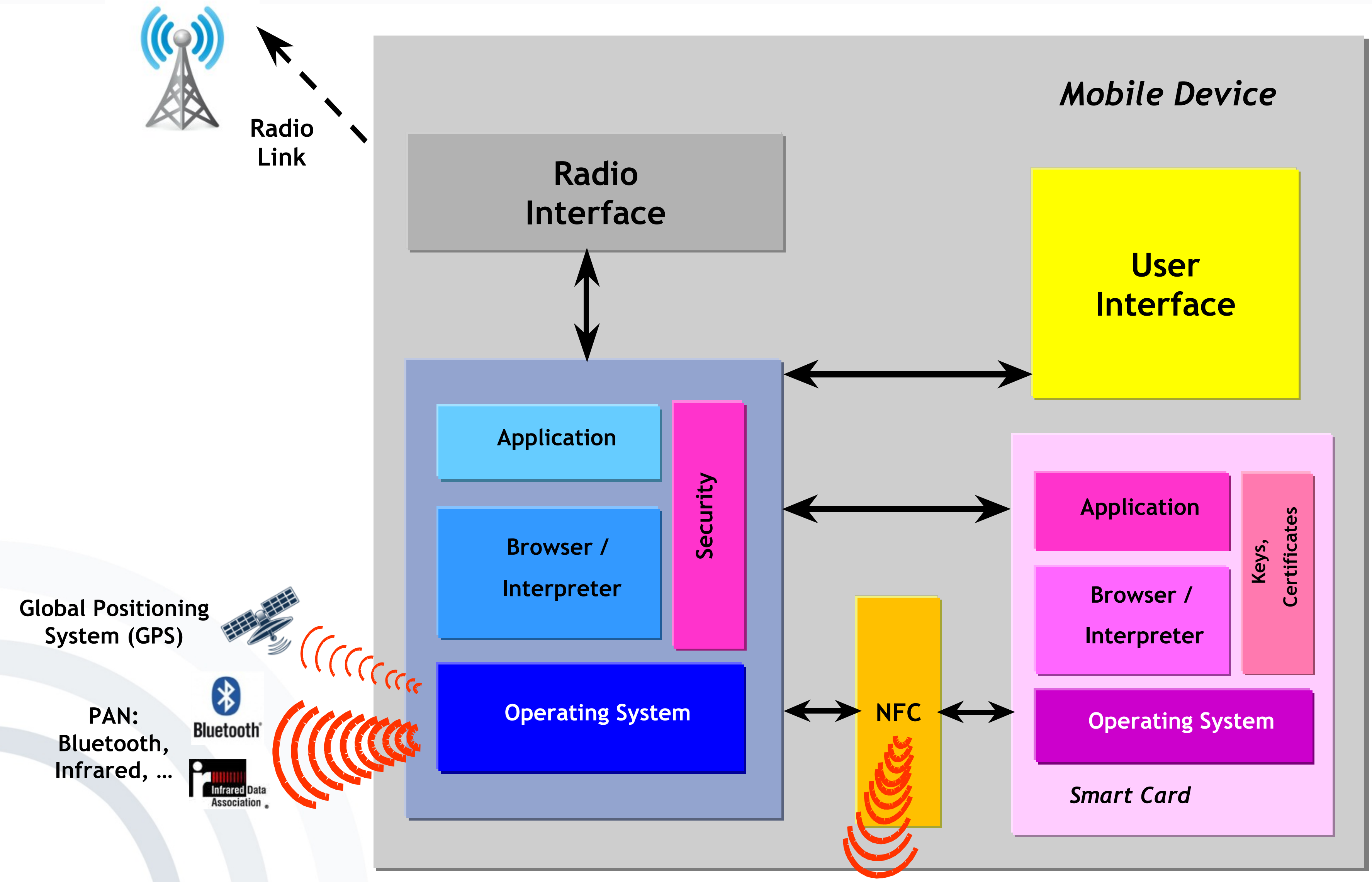
Usage Scenarios

- Secure OS
- Mobile Device Management (MDM)
- Secure corporate network interaction
- Digital Rights Management (DRM)
- Device misuse prevention
- Storage of additional credentials on the mobile device
- Mobile Wallets

Secure OS

- Trusted mobile platforms can help to protect the operating system (system software and applications) from manipulations.
- Integrity of the system can be observed by user or remote party (e.g. features like secure booting, Mobile Device Management)

OS – Functional Architecture



Based on [Posegga2001]

Near Field Communication (NFC)

Mobile Device Management (MDM)

- Software to secure, monitor, manage and support mobile devices
- Over-the-air distribution of
  - Applications
  - Data
  - Configuration settings

➲ Higher security level, lower cost and fewer downtimes

Secure Corporate Network Interaction

- Staff members can easily copy confidential information to the mobile device and carry it out of the secured perimeter.
- Trusted mobile device could facilitate secure device identification in the corporate network and provide reliable mechanisms for secure data exchange.

Digital Rights Management (DRM)

- Mobile device could provide a facility that can be integrated within a DRM infrastructure, e.g.
  - device authentication,
  - cryptographic functions,
  - certificate management support.

Device Misuse Prevention

- Most mobile devices provide device access protection via PIN or password input.
- Many mobile users don‘t use this functionality (inconvenience).
- Mobile device could provide protection mechanisms such as
    - strong user authentication,
    - strong user authorisation,
    - data access management,
    - data encryption.

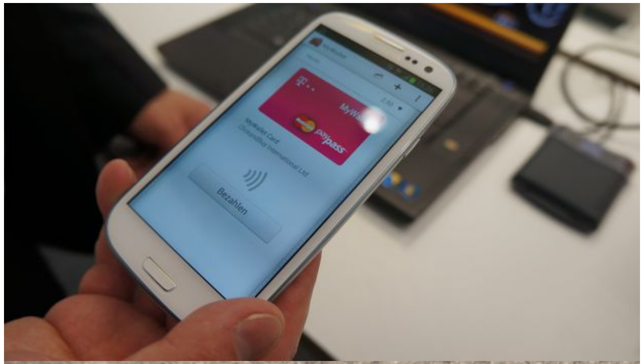
Storage of additional Credentials on the Mobile Device

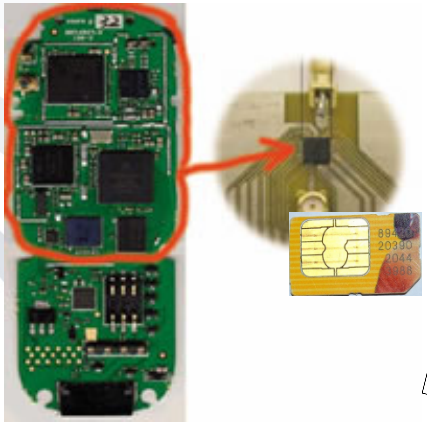
- SIM card is used as secure storage for mobile operator credentials.

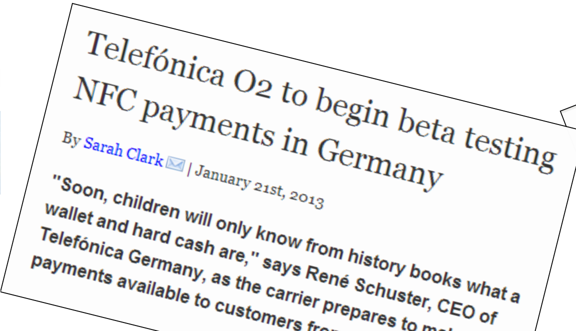
- Idea: Storing credentials on the device, if mobile devices can offer secure storage based on trusted computing.
- A trusted platform needs to provide
  - cryptographic functions,
  - key management support,
  - dependable user authorisation,
  - secure data access.

Mobile Wallets

- (NFC) Mobile Wallets
  - contain virtual payment cards and other cards, e.g. customer loyalty cards
  - use the UICC/SIM-based Secure Element (SE)
  - Deutsche Telekom, Vodafone, Telefónica and E-Plus independently launches in 2014.
- Mobile Wallet application runs in **non-secure memory** of the mobile device whereas UICC payment application runs within the SE.



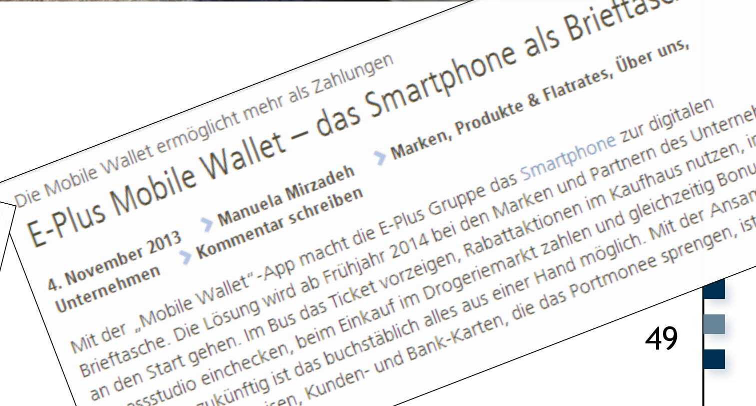




Telefónica O2 to begin beta testing NFC payments in Germany

By Sarah Clark | January 21st, 2013

"Soon, children will only know from history books what a wallet and hard cash are," says René Schuster, CEO of Telefónica Germany, as the carrier prepares to m
payments available to customers fro



Die Mobile Wallet ermöglicht mehr als Zahlungen

E-Plus Mobile Wallet – das Smartphone als Brieftasche

4. November 2013 › Manuela Mirzadeh › Marken, Produkte & Flatrates, Über uns, Unternehmen › Kommentar schreiben

Mit der „Mobile Wallet“-App macht die E-Plus Gruppe das Smartphone zur digitalen Brieftasche. Die Lösung wird ab Frühjahr 2014 bei den Marken und Partnern des Unterneh
an den Start gehen. Im Bus das Ticket vorzeigen, Rabattaktionen im Kaufhaus nutzen, im
ssstudio einchecken, beim Einkauf im Drogeriemarkt zahlen und gleichzeitig Bonu
zukünftig ist das buchstäblich alles aus einer Hand möglich. Mit der Ansam
isen, Kunden- und Bank-Karten, die das Portmonee sprengen, ist

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Matching

- Security options enabled by trusted platform features and the respective usage scenarios correspond to different interests of the different players within the mobile market:

  - The security of mobile platforms is valued as especially important by **equipment manufacturers**, **mobile operators, MVNO's** and **corporate buyers** (loss of money or reputation can pose significant problem for them). As most security conscious group, they have a high interest in the security of the operating system.

Matching

- For **corporate** and **private customers** high importance of reliable and trustworthy devices and malware protection.
- Mobile platform security also relevant for application providers (services dealing with sensitive or financial information)

Usage Scenarios and Players

Players and security features they are especially interested in

Usage Scenarios/ Players	Mobile Equipment manufacturers	Mobile operators	MVNOs	Content providers	Appl. Service providers	Private customers	Corp. buyers	Corp. users	Intelligence Agencies
Secure OS	++	++	++		+	+	++	+	
Digital Rights Management	+	+	+	++					
Device misuse prevention						+	++	+	
Storage of additional credentials	+				+	+	+		
Secure corporate network interaction		+			+		++	+	
Mobile Wallet	++	++				+			

Based on [PiskRannRoss2005]

Key Players’ Interests

Mobile Equipment Manufacturers

Secure operating systems

DRM

Mobile Wallet

Storage of additional credentials

Content Providers

DRM

Application Service Providers

Secure operating systems

Storage of additional credentials

Secure corporate network interaction

Device Owners

Malware and device misuse prevention (Corporate Buyers notably *Mobile Device Management*)

Free choice of applications and full device control

Mobile Operators

Secure operating systems

DRM

Mobile Wallet

Secure corporate network interaction

MVNO’s

Secure operating system

DRM

Device Users

Usability

Malware and device misuse prevention

Mobile Equipment Manufacturers

- In the past, main manufacturers of mobile devices were mobile phone manufacturers (e.g. Nokia, Motorola), producing both hardware and the software.
- Meanwhile the value chain for mobile devices has become more complex: Significant parts may come from third parties, e.g.
  - hardware from ARM, Infineon, Texas Instruments,
  - software from Google, Microsoft.
- The more a manufacturer is perceived as the provider of the respective platform, the more risks of the mobile platform are affecting them.
- Today, mobile devices are sold particularly as part of a powerful ecosystem (Google, Apple, Microsoft).

Overview

Mobile Trusted Devices

- Introduction and Motivation – Security Issues
- Security of Current Mobile Platforms
- Standardisation Activities for Trusted Mobile Platforms
- (Mobile) Equiment Identifier
- Mobile Market Players and their Interests
- Usage Scenarios for Trusted Mobile Platforms
- Matching Usage Scenarios and Players
- Conclusion and Outlook

Conclusion

- Mobile platforms had good chances to migrate into trusted platforms.
- All mobile market players are interested in device security enhancements.
- Major players are actively engaged in the standardisation and development process.
- Based on trustworthy platforms mobile devices could facilitate the development of security-critical mobile commerce and mobile business application and services (e.g. mobile payment, mobile signatures).

Outlook

- Missing at the moment:
  - An architecture combining the features the different parties are interested in
  - An entity to drive this architecture, e.g. the one consortium comprising all the players and interests
  - The availability of all standardisation results for public review

Literature (1)

- [GSM2005] GSM Association (2005), Mobile Application Security, www.gsmworld.com/using/security/gsma_mas_final_summary_v1.pdf, accessed 2006-11-03.
- [MurmanRossna2005] Murmann, Tobias; Rossnagel, Heiko (2005): Sicherheitsanalyse von Betriebssystemen für Mobile Endgeräte; In: Federrath, Hannes (ed): SICHERHEIT 2005, Sicherheit - Schutz und Zuverlässigkeit: Beiträge der 2.Jahrestagung des Fachbereichs Sicherheit der Gesellschaft für Informatik e.V. (GI), Lecture Notes on Informatics (LNI), S.129 – 139.
- [PiskRannRoss2005] Pisko, Evgenia; Rannenberg, Kai; Rossnagel, Heiko (2005): Trusted Computing in Mobile Platforms – Players, Usage Scenarios, and Interests; In: Datenschutz und Datensicherheit (DuD) (29:9), pp. 526-530.
- [Posegga2001] Posegga (2001), WiTness.
- [Riscure2014] Marc Witteman (Riscure): Are Embedded Secure Elements more secure than traditional smart cards?, www.cartes-america.com/files/are_embedded_secure_elements_more_secure_than_traditional_smart_cards___tilburg_witteman.pdf, accessed 2014-11-04.
- [TCG2014] Trusted Computing Group (2013), www.trustedcomputinggroup.org, accessed 2014-10-09.

Literature (2)

- [WaPo2013a] NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say, http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html, accessed 2013-12-09.
- [WaPo2013b] NSA tracking cellphone locations worldwide, Snowden documents show, http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html, accessed 2013-12-09.
- [Zeit2013] Bundesbehörden sehen Risiken beim Einsatz von Windows 8, www.zeit.de/digital/datenschutz/2013-08/trusted-computing-microsoft-windows-8-nsa, accessed 2013-12-05.