An overview of some security and privacy design challenges in Embedded applications

gemalto
security to be free

Jean-Pierre Tual

Agenda

- Introduction to Security Technologiess
- Examples from the Mobile Industry
- Examples from the automotive Industry
- Examples from the Energy Industry
- Security and privacy preserving design principles

Trends

- High Bandwidth Wireless Connected World
- Smart objects: phones, tablets, wearables
- Internet of Things / M2M explosion
- Cloud Computing & Everything as a Service
- Data explosion & Big data
- HW/SW Virtualization
- Convergence IP and Telecom networks
- Open Source SW
- Security and privacy management

DIGITAL REVOLUTION

Major issues with embedded systems

- Scalable architecture
- Remote management
- Long-life cycle
- Security
- Privacy
- Overall cost

Basic security technology building block in embedded security

- Smart cards / security elements (SE)
- Trusted Execution Environment
- OTA servers
- Trusted service manager
- Device remote personalization

Removable versus Non Removable SE

- Removable Secure Element
  - As soon as the SE is used with **multiple** “readers” then the SE is still standalone.
  - Banking Cards,
  - GP cards (ID, Licences, CPS, Passports)
- Non removable Secure Element
  - As soon as the SE is used into a **single** device then :
    - Step 1: The SE is soldered in becoming an embedded SE.
    - Step 2: The SE is embedded in a TEE or a SOC (System On Chip)
  - Full remote personalization is required

Classical security model (Server, PC,..)

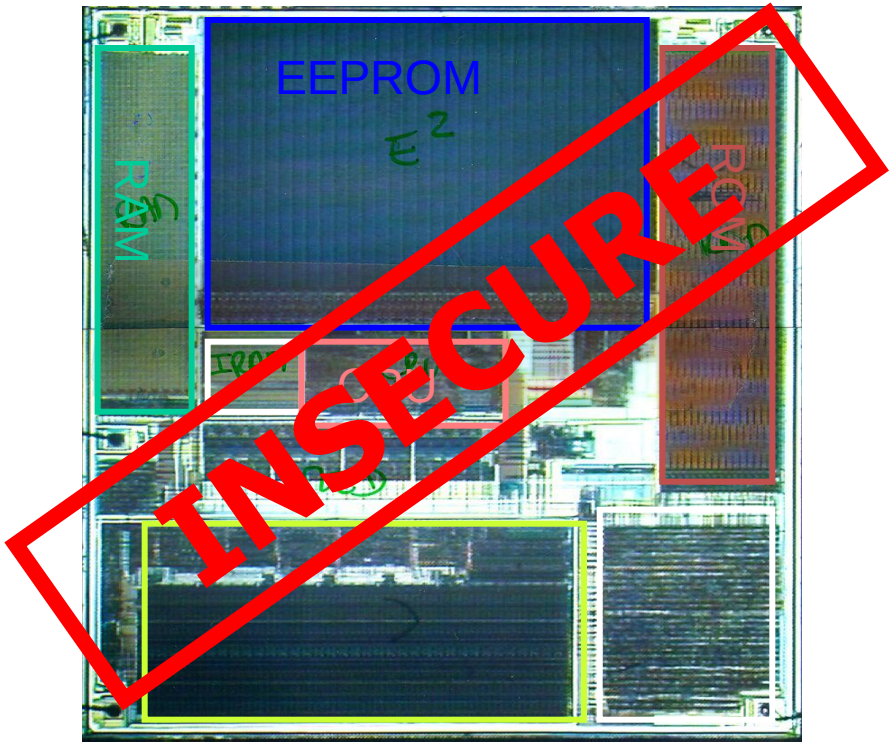
- Protected environment
- Trusted users
- Direct access to data

Embeded security model (M2M, IoT,….)

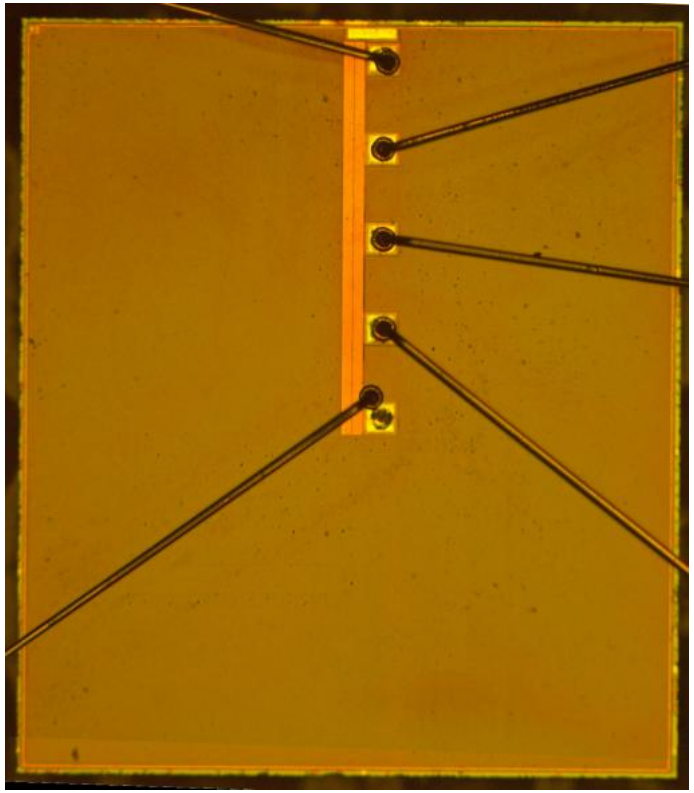
- Unprotected environment
- Non trusted users
- No direct access to data
- **Tamper resistant devices**

What does it means for SE ?

Tamper resistance at chip level



- Blocks can be easily identified
- No shield
- No glue logic
- Buses clearly visible

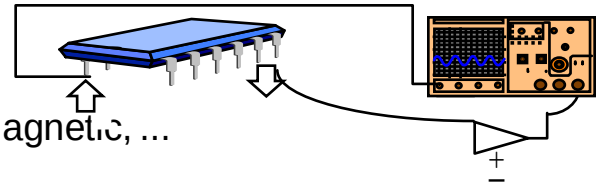


- Shield
- Glue logic
- No Buses visible
- Memories and buses encryption
- Sensors

Secure Elements: expected resitance to Physical and Logical attacks

Physical Attacks

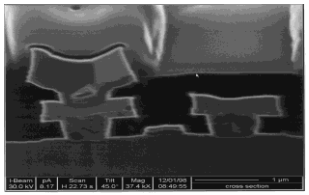
- **Side-Channel analysis***: Monitor analog signals on all interfaces and analyze:*



- **Fault injection***: use of Laser, Glitchers, Flash light…*

to bypass protections and infer secrets.

- **Invasive manipulation***:*
  - Chip observation
  - Deposit probe pads on bus lines
  - Reverse ROM mapping
  - Disconnect RNG
  - Cut tracks

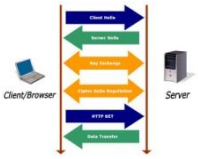


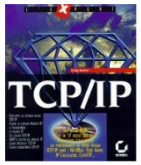
Logical Attacks

- **Aggressive software:** Buffer overflow, Aggressive applets, Trojan Horses, Viruses, Cryptography,..

- **Environment: Servers, PCs, readers and handsets configurations:**

- **Protocols and stack implementations:**



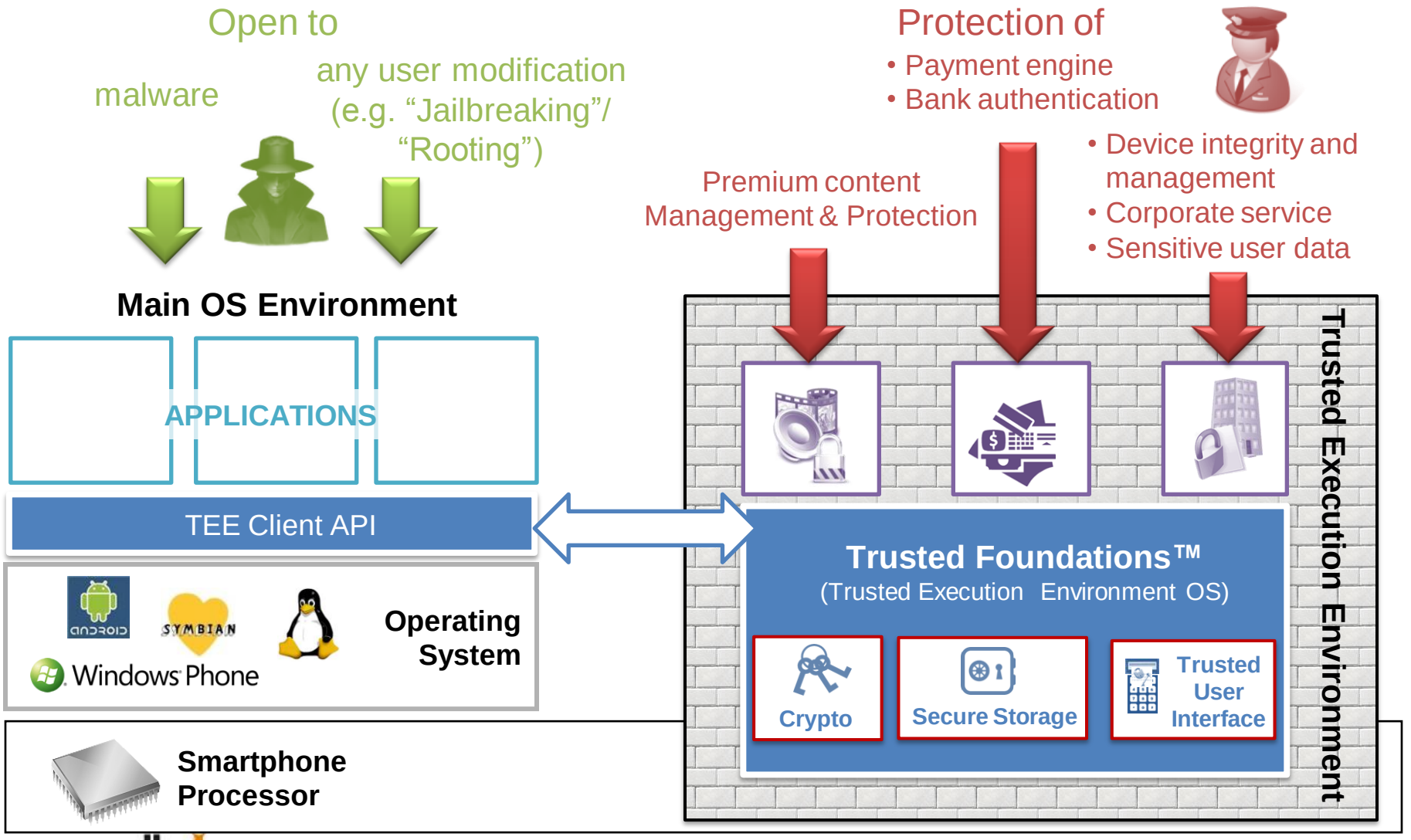


Bluetooth® 3G

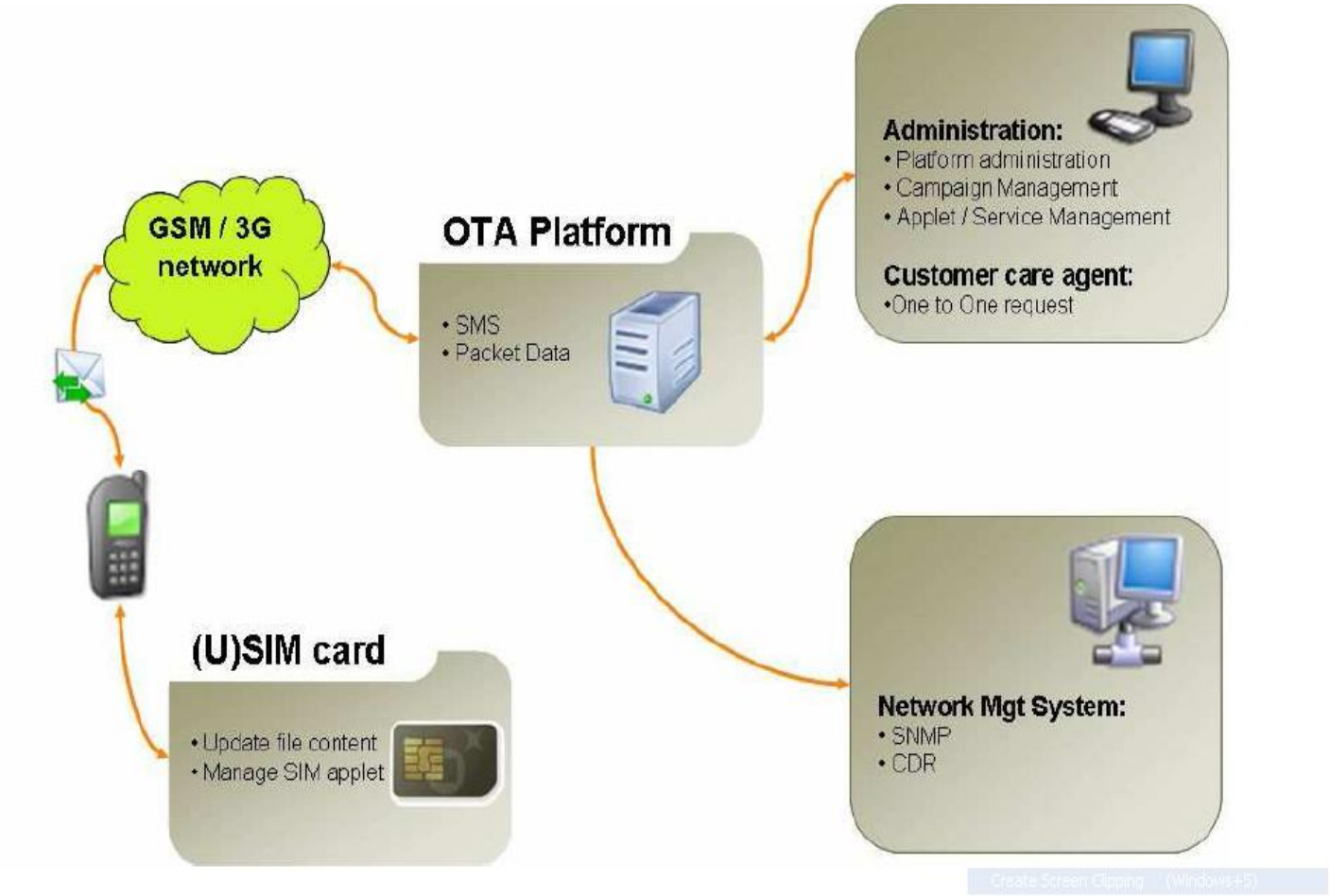
Impact on SW components

- The software provisioning must to the following rules
  - Late personalization even after customer issuance
  - Full Remote update because the components are soldered/embedded and cannot be changed
  - Scalability of deployment schemes
  - Embedded local security
  - Long life cycle management (bugs and security patchs)
  - Flexibility according to the country and the field actors (late customization after issuance to the final customer
- Emerging concepts from the Mobile world can be customized on purpose
  - TEE
  - OTA
  - TSM

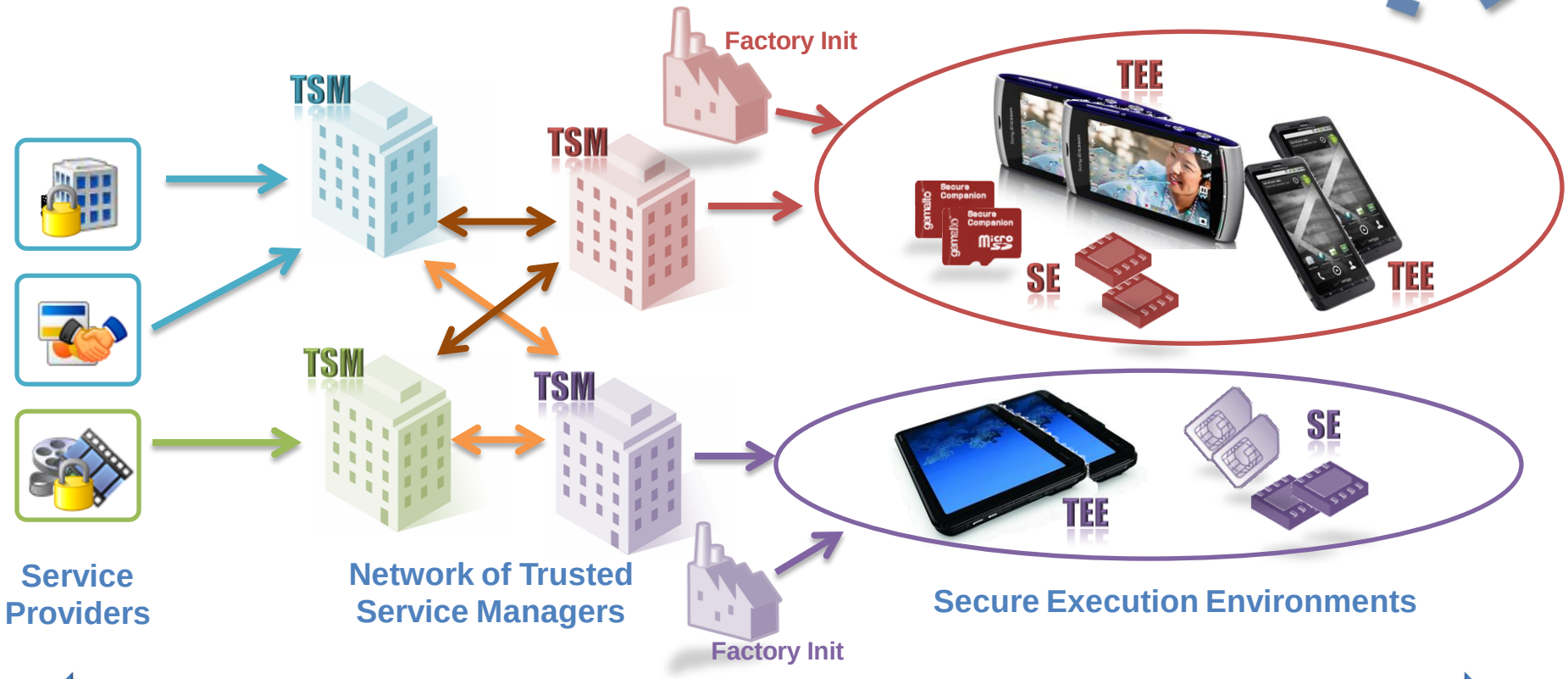
Enforcing Security: Trusted Execution Environment (TEE)



Remote management of devices by millions



TEE and SE remote Administration

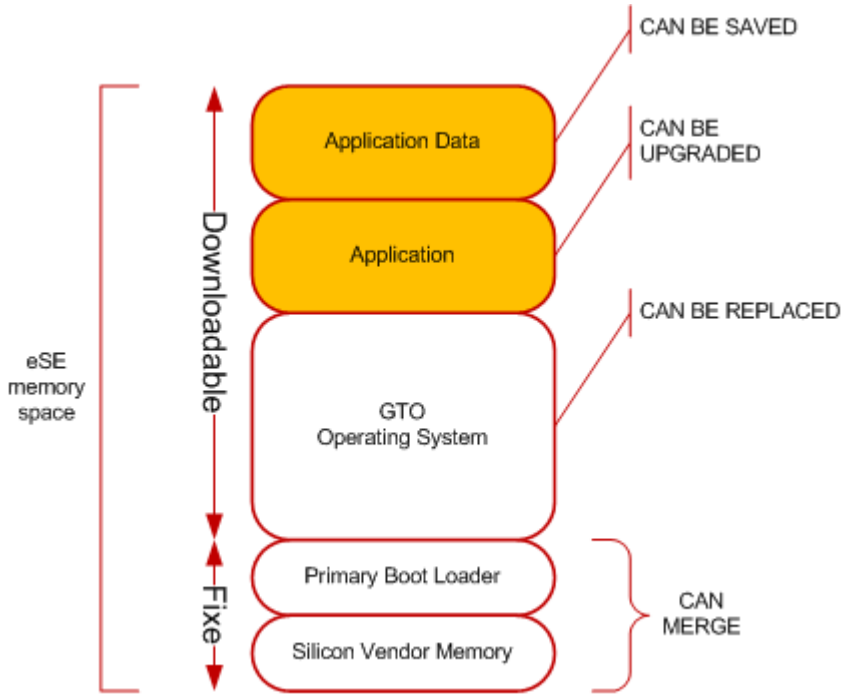


End-to-End Secure Infrastructure

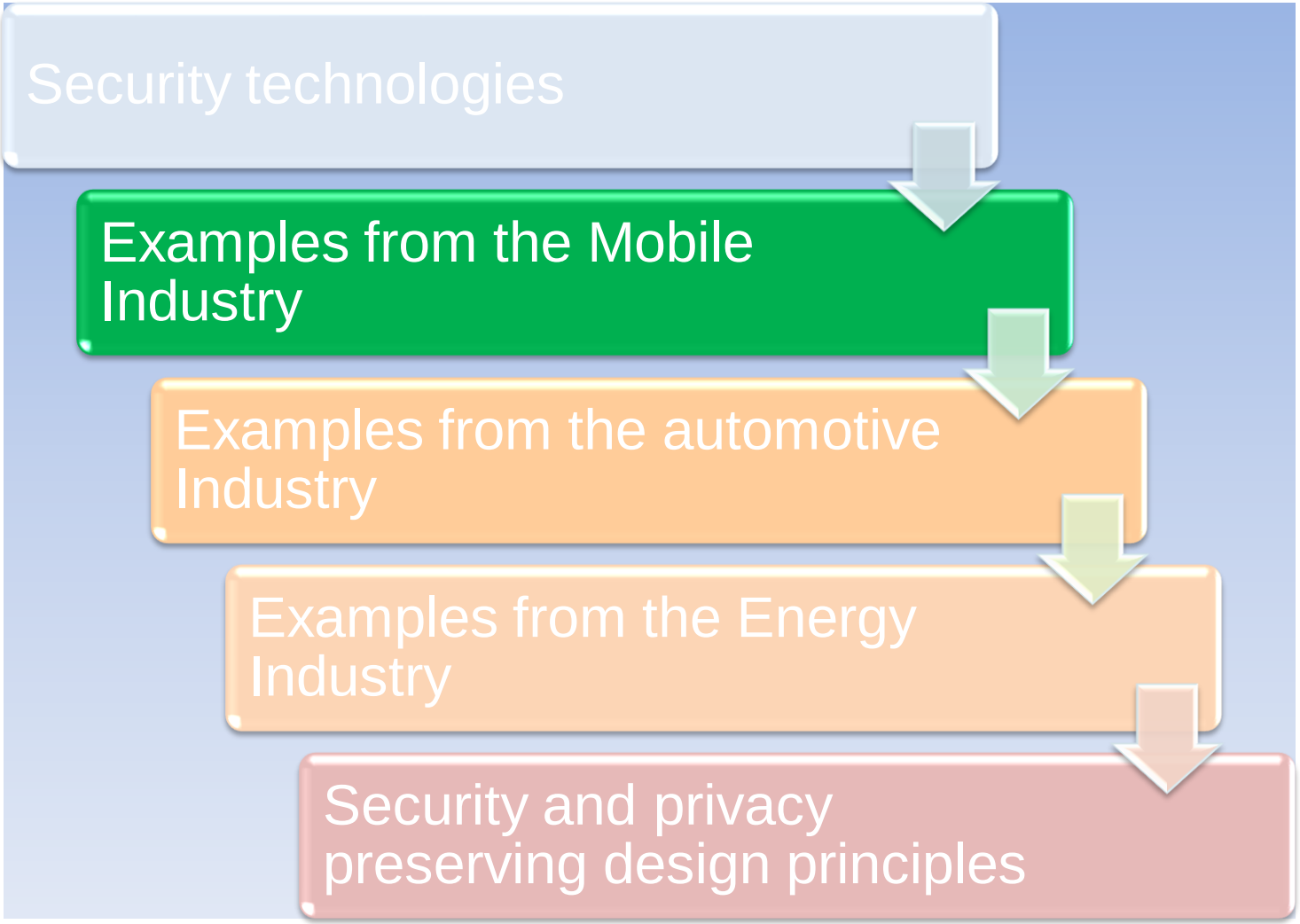
- Same remote administration architecture for TEE and Secure Elements
- Complementary of TEE and SE

Full Remote Personalization

- Primary Boot Loader
  - Allow the downloading of the OS
  - Can be embedded into the silicon vendor dependent software
  - Can be generic (consolidated market)
  - Can be vendor dependent (fragmented market)
  - Independent of the OS
- Operating system
  - Market dependent
  - Bundled with the applications
  - Allow the application data saving (before OS upgrade)

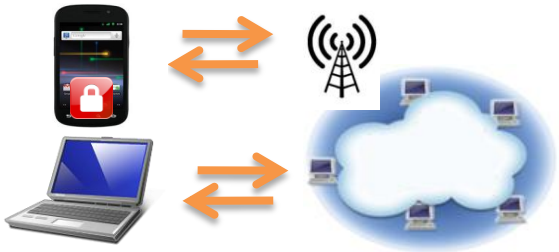


Agenda


Security technologies
Examples from the Mobile Industry
Examples from the automotive Industry
Examples from the Energy Industry
Security and privacy preserving design principles

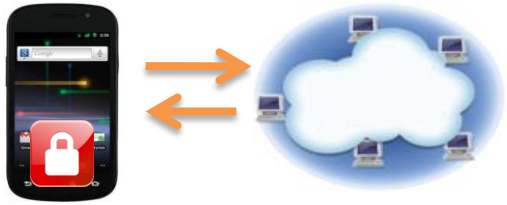
Some Mobile Security use cases….

Mobile as a token



I use my mobile to secure on-line transactions:
Out of band authentication (e-banking, e-gov servises…)

Mobile as a laptop

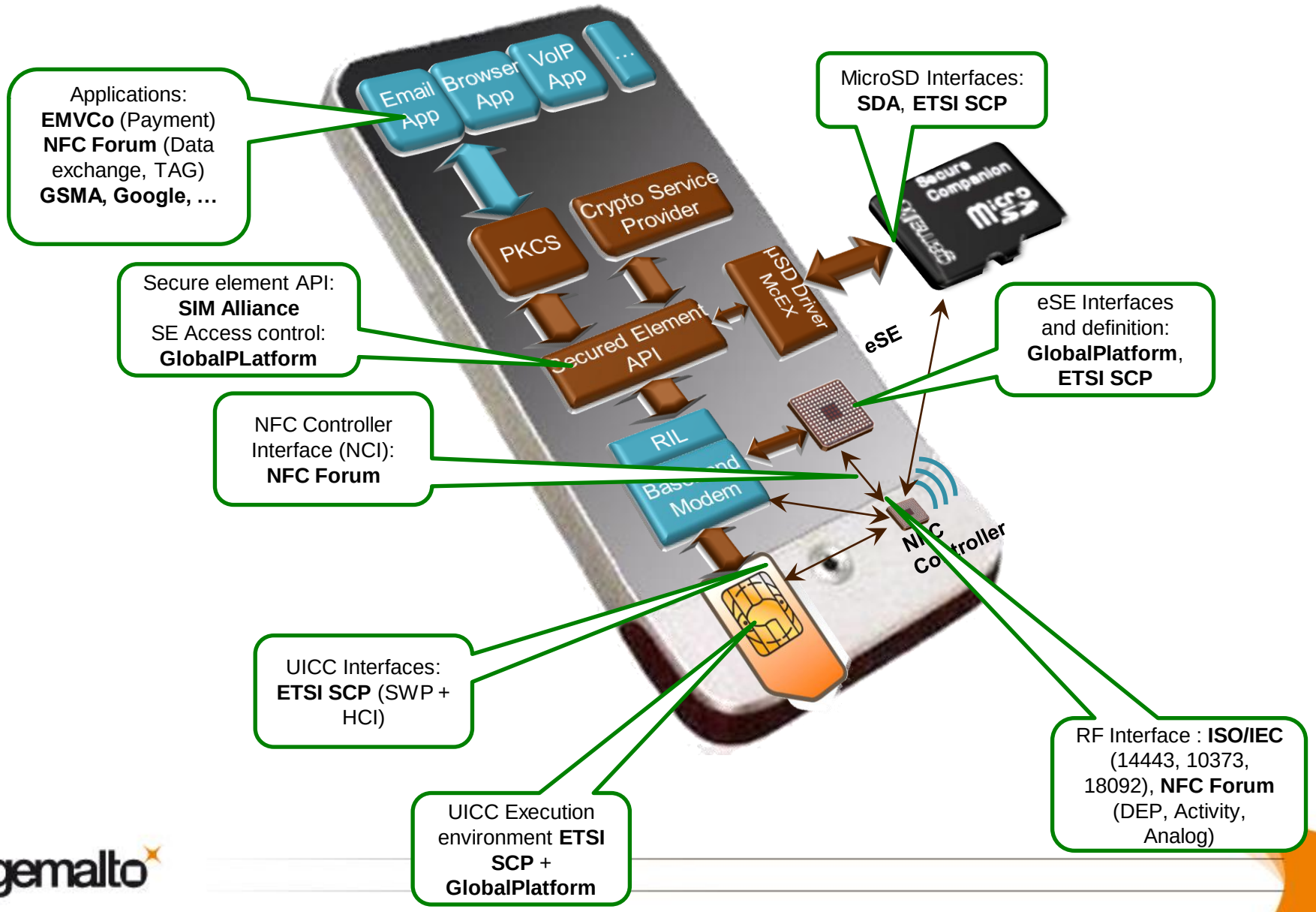


I use my mobile for:
Mobile banking, email encryption, VoIP encryption, VPN access, secured application login, secure storage…

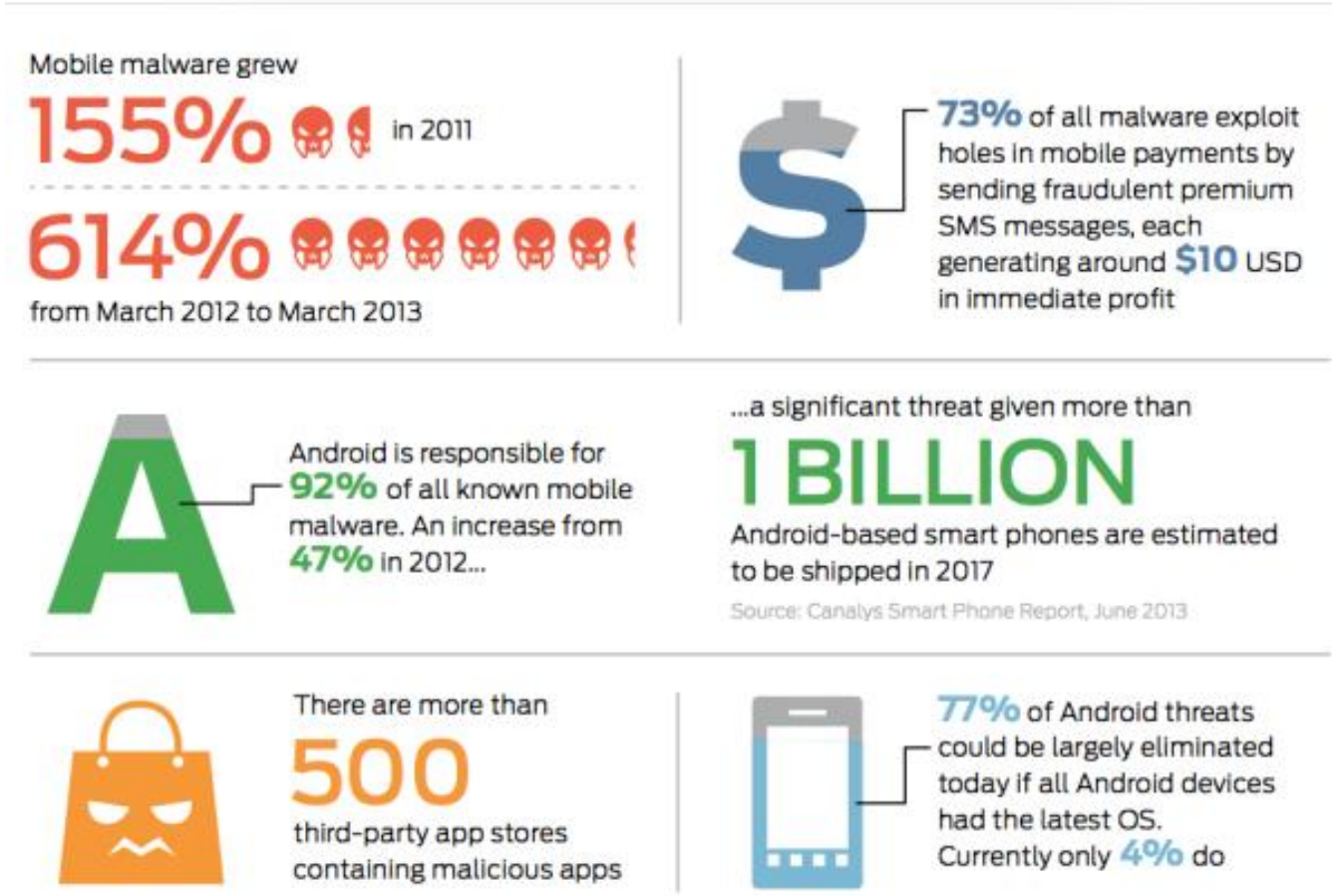
Mobile as a smartcard

I use my mobile to run transactions:
Mobile payments, transports…

Mobile devices: potential points of security enforcement… and attacks!



The actual landscape



A snapshot from the third annual Mobile Threats Report from Juniper Networks.
(Credit: Juniper Networks)

Some exploits (cont)

Google play

Banking

- March 2013: “Android SMS malware package targets customers of the Commonwealth Bank, Westpac, Citibank, BankWest and ING Direct in Australia, as well as 64 other financial institutions in the US, France, India, Italy, Germany, New Zealand, Singapore, Spain, Switzerland and Turke

  - When the victim logs into their online acc
    ‘injects’ a page into a victim’s br
    but is actually from the a
    phone number
    introdu
    ank
    ter their mobile
    e bank has recently

  - The ma designed to capture SMS one-time passcodes.

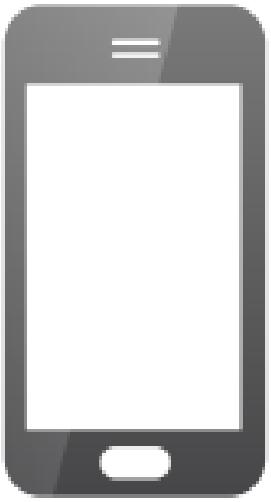
  - NB: Malware developer can buy verified developer accounts at Google Play for $US100 apiece”

Cybercrooks swiped £30 million (€36m) from the banks accounts of 30,000 customers in Italy, Germany, Spain and Holland over the summer

The threats

Supply chain

Enrolment



Device

User

Networks

Threats in product life cycle

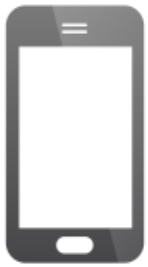
- The supply chain.

  - Weak root keys generation
  - Insider knowledge (keys, debug protocols,…)
  - HW and SW Trojan
  - Bugs (e.g. in OEM code)

- Enrolment and provisioning.

  - Weak user authentication
  - Weak device authentication
  - Alternative app stores
  - Fake apps
  - Trojans

- Usage…



Device

HW

Peripherals: Biometric sensors, USB, Camera…
Local storage: dump of Flash memory
JTAG
Physical attacks (Side-channel, Fault injections…)

Boot

Bypass Secure boot sequence

Baseband

OS

Kernel:
Libs/APIs/Drivers/System Apps:
Privilege escalation, KeyLogging, MiTM

App

Local Storage
Run Time injection
DoS
Fake App

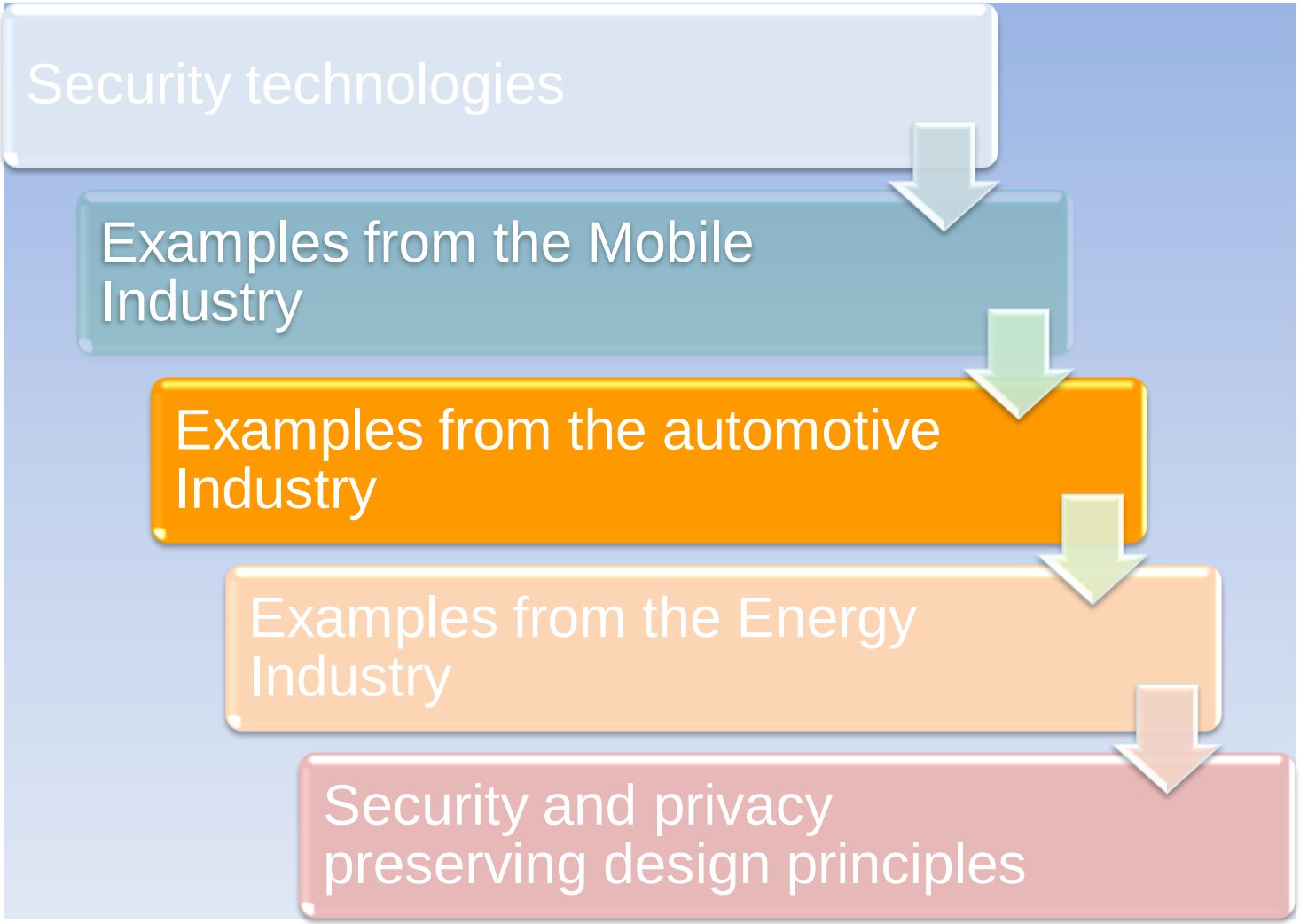
Browser

Local Storage (Keys, Cookies)
Framing
Click Jacking

Fake Access Points: Fake BTS, WiFI,…
MiTM
Relay Attacks
DNS Poisoning

Phishing
Social engineering
Jailbreaking
ID theft

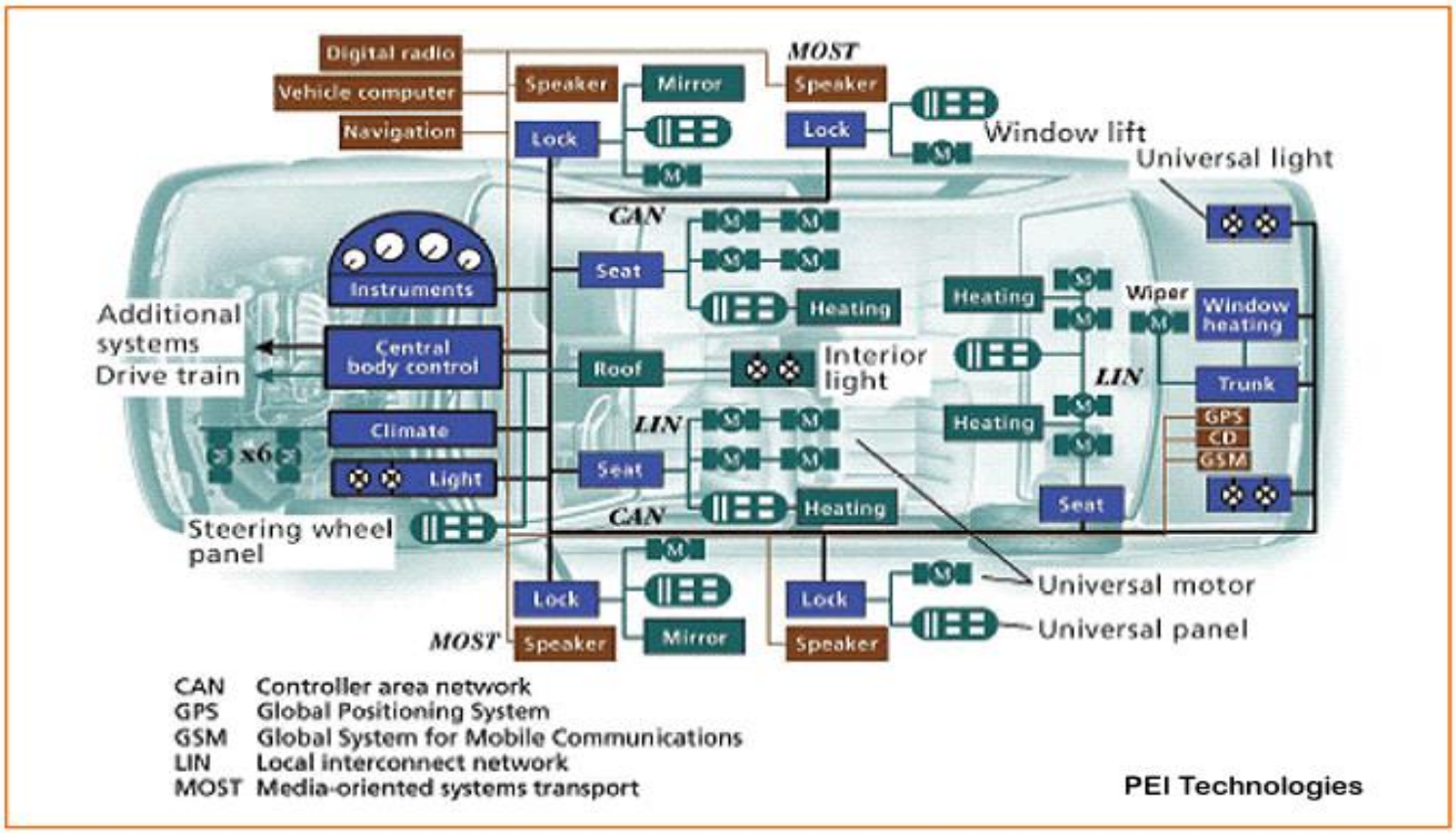
Agenda


Security technologies
Examples from the Mobile Industry
Examples from the automotive Industry
Examples from the Energy Industry
Security and privacy preserving design principles

Everything that can be hacked *will* be hacked !

Security issues in a modern car

- Modern cars have over 80 ECUs connected to the CAN bus



Security issues

- CAN is an insecure low-level protocol
- CANs main contain wireless components implicating potential massive security issues
- Message are unencrypted plain-text broadcasted to every device on the CAN
- Documentation open and made available freely
- No component authentication
- Any device can send a command to any other devices

Consequences

- Demonstration by researchers (*) of a sniffer/injection tool, introduced into the CAM by simply plugging a device in to the car's federally mandated universal *OBD*-II diagnostics
- Example of attacks made possible including at 45 mph speed
  - Disable brakes
  - Engage brakes
  - Disable wipers and continuously spray fluid
  - Permanently activate horn
  - Kill engine
  - Unlock all doors
- Most attacks made also possible wireless

(*) University of Califormia and Washington

http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5504804&tag=1

http://dl.acm.org/citation.cfm?id=2018396

Next threat: car as a programming platform

- Services are provided as apps
- The car needs to provide a rich API in order to be an attractive platform for developers
  - Case study: RelayRides app on OnStar

Hardware factorization in cars

Navigation

Speed radar locator

Open android platform

A smart phone with 4 wheels ?

Ecodriving

Multimedia

Point of Sale terminal

CPU

Memory

Code, data and secrets

Com. Modules

GPRS, RTC, Ethernet, Bluetooth, WiFi

GUI

LCD, Printer

Business logic

Smart card transaction, risk management
Data signature and up-load

Security

Tampering detection, key erase

Telematic Control Unit

CPU

Memory

Code, data and secrets

Com. Modules

GPRS, PLC, USB, WiFi

Trusted UI

Business logic

E-call, nav, diag, info, …

Security

Tampering detection, key erase

Example of hobbyist at work

Example of professionals at work

PCB Reverse, PCB Clone,MCU Reverse,Chip Crack,PCB Manufacturing, PCB Designing, PCB Cloning, PCB fabrication, PCB Rework,PCB Assembly

HeTe l l Technolgy In China

Great Service ◆ Highest Quality ◆ Competitive Pricing

086-0755-61327568 && 086-0755-61327569

pcbhetell@gmail.com hetelltech@gmail.com skype:hetell0755

Home | About | PCB Cloning | PCB Designing | MCU Crack | PCB Assembly | Contact US | PCB layout |

Products & Services

- PCB Reverse Engineering
- Altera Chip decryption
- Atmel MCU Crack
- CYPRESS MCU Attack
- Dallas MCU Code Extraction
- EMC IC Code Extraction
- Freescale IC Crack

AT89C51RB2 MCU Attack, Atmel AT89 IC Code Extraction

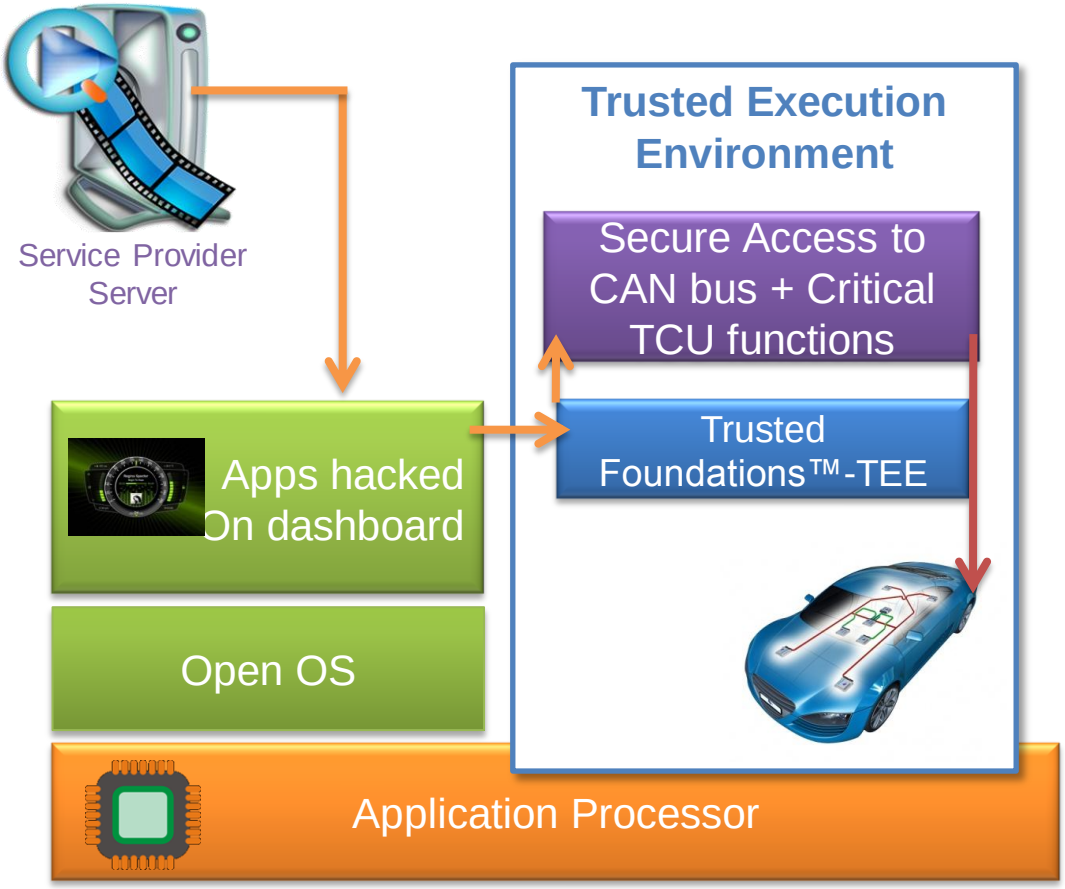
For AT89C51RB2 MCU Code Extraction, AT89C51RB2 IC Crack, AT89C51RB2 MCU Break, and other Atmel IC Attack. we use high-end technologies and the latest laboratory equipment to perfect the technique of microcontroller code recovering (extracting the code from locked microcontrollers). We had analyzed a wide variety of chip types which are commonly used in different industries, which enable us to open the chips and extract the program inside with quick speed and accuracy, and thus help lauching your project quicker and cheaper.

Description

The AT89C51RB2 is a high-performance Flash version of the 80C51 8-bit microcontrollers.It contains a 16K Bytes Flash memory block for program and data.The Flash memory can be programmed either in parallel mode or in serial mode with the ISP capability or with software. The programming voltage is internally generated from the standard VCC pin.

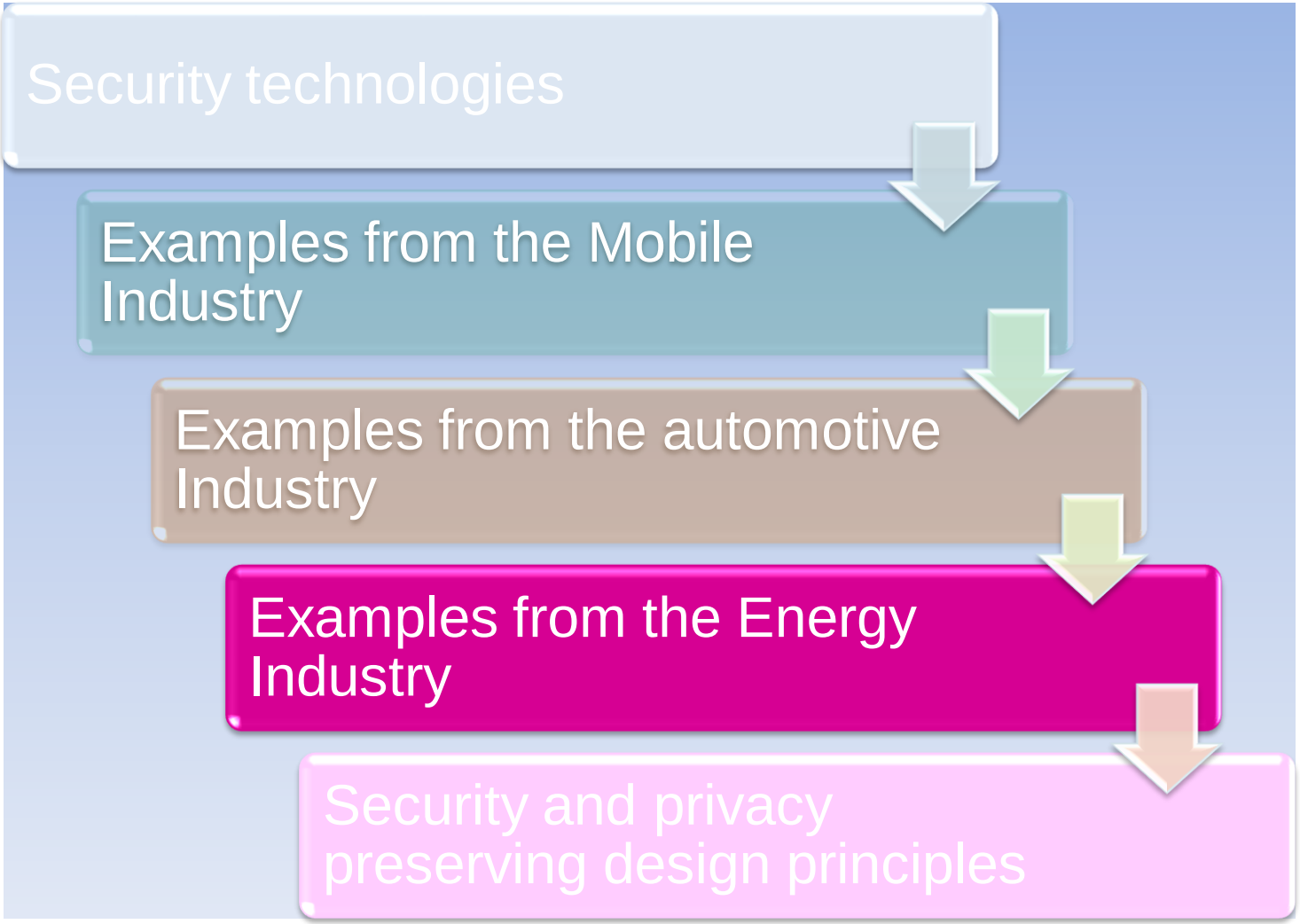
Features

Guidelines for security improvement in cars

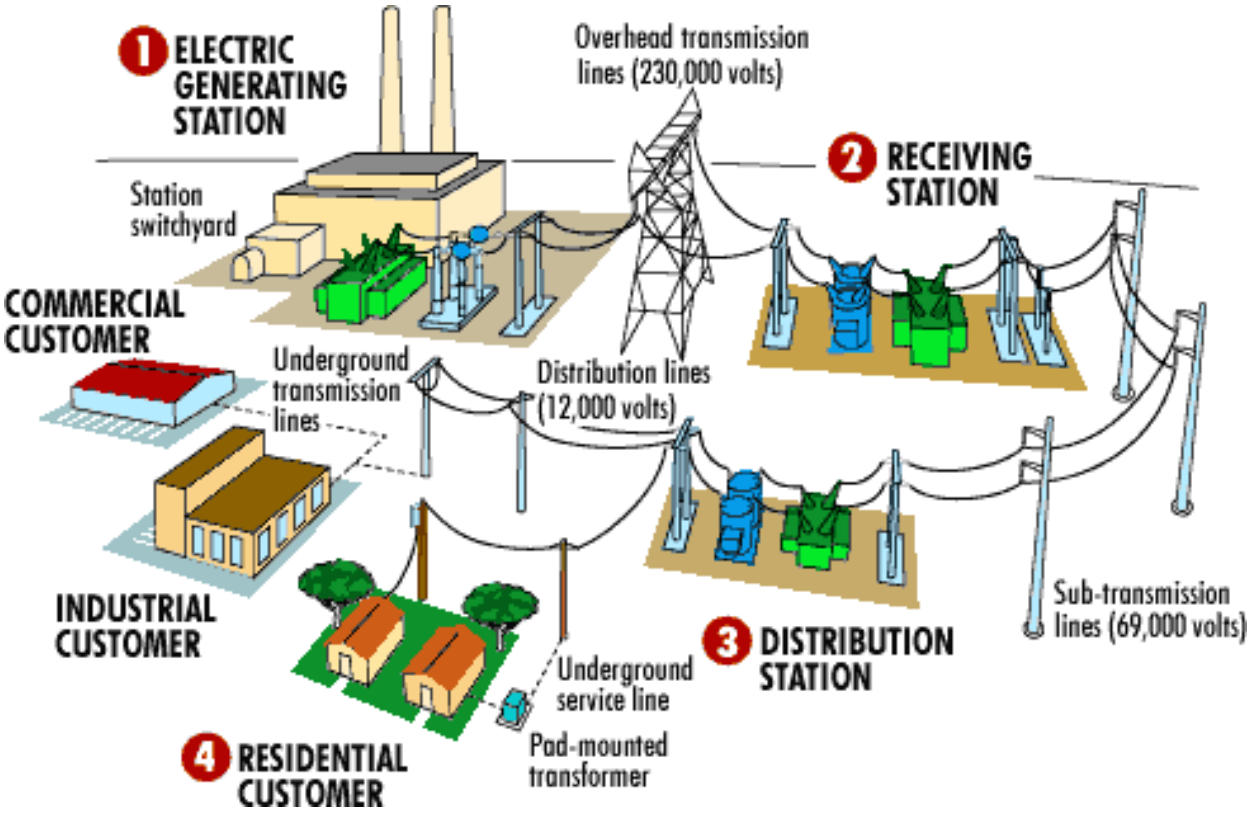


- Controller authentication
  - Only valid controllers can communicate on the CAN
- Encrypted communication
  - Must be high performance, so use symmetric key
  - Distribute symmetric key using asymmetric encryption during authentication
- TEE for ECU Protection (firewall)
- Solution to protect Automotive asset against the attacks like:
  - Malicious Application
  - Deny of Services
  - ECU malicious update

Agenda

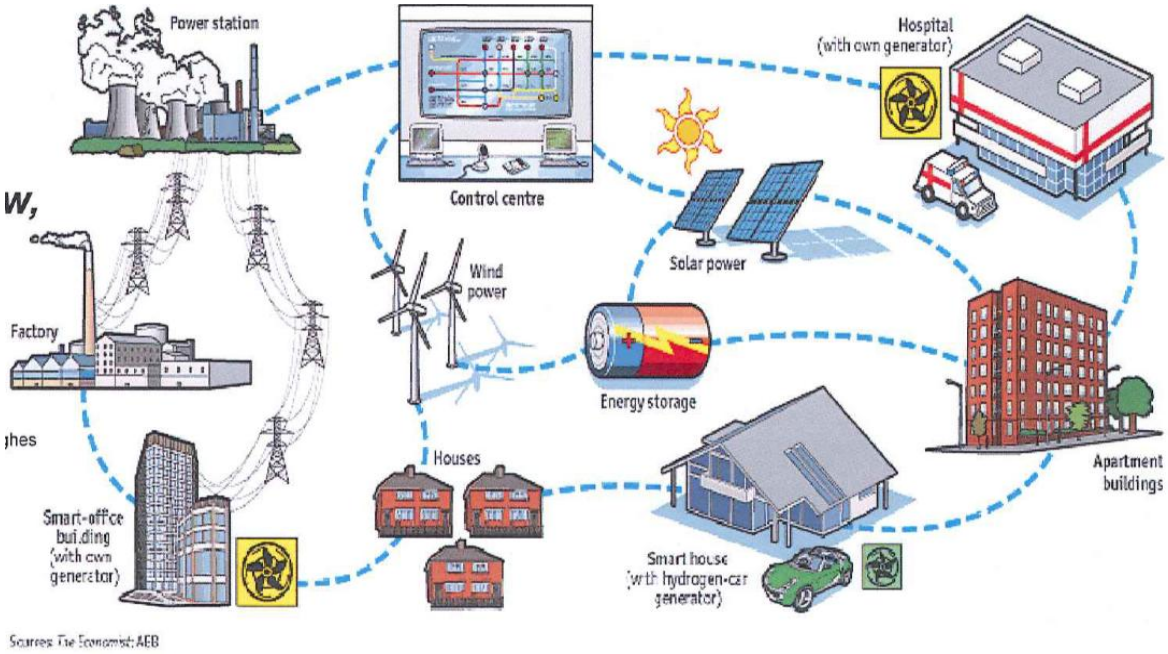

Security technologies
Examples from the Mobile Industry
Examples from the automotive Industry
Examples from the Energy Industry
Security and privacy preserving design principles

From grid ….

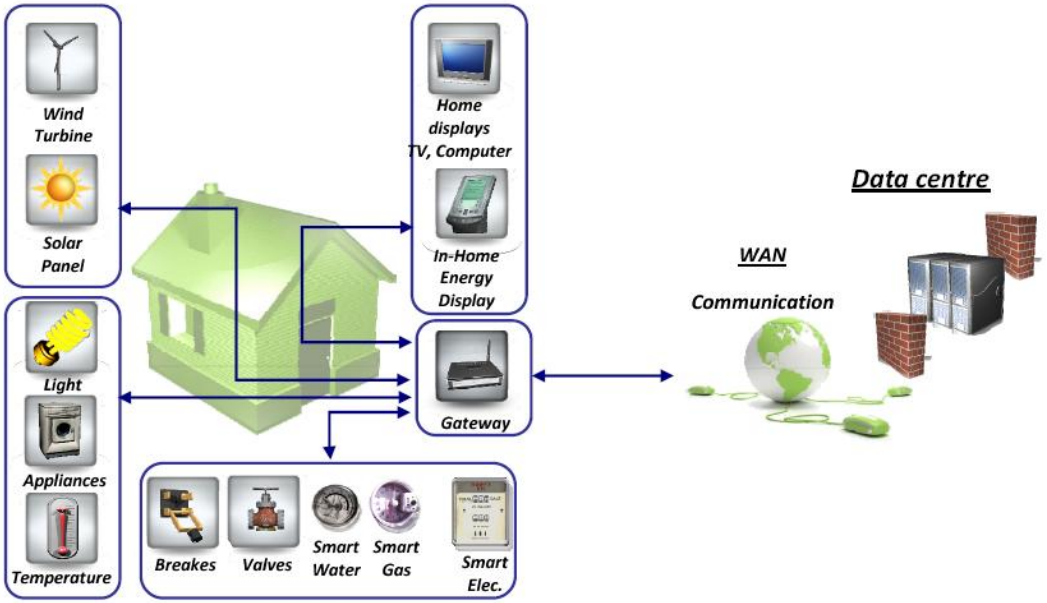


- One way energy flow
- Centralized, bulk generation
- Few actors, central information system

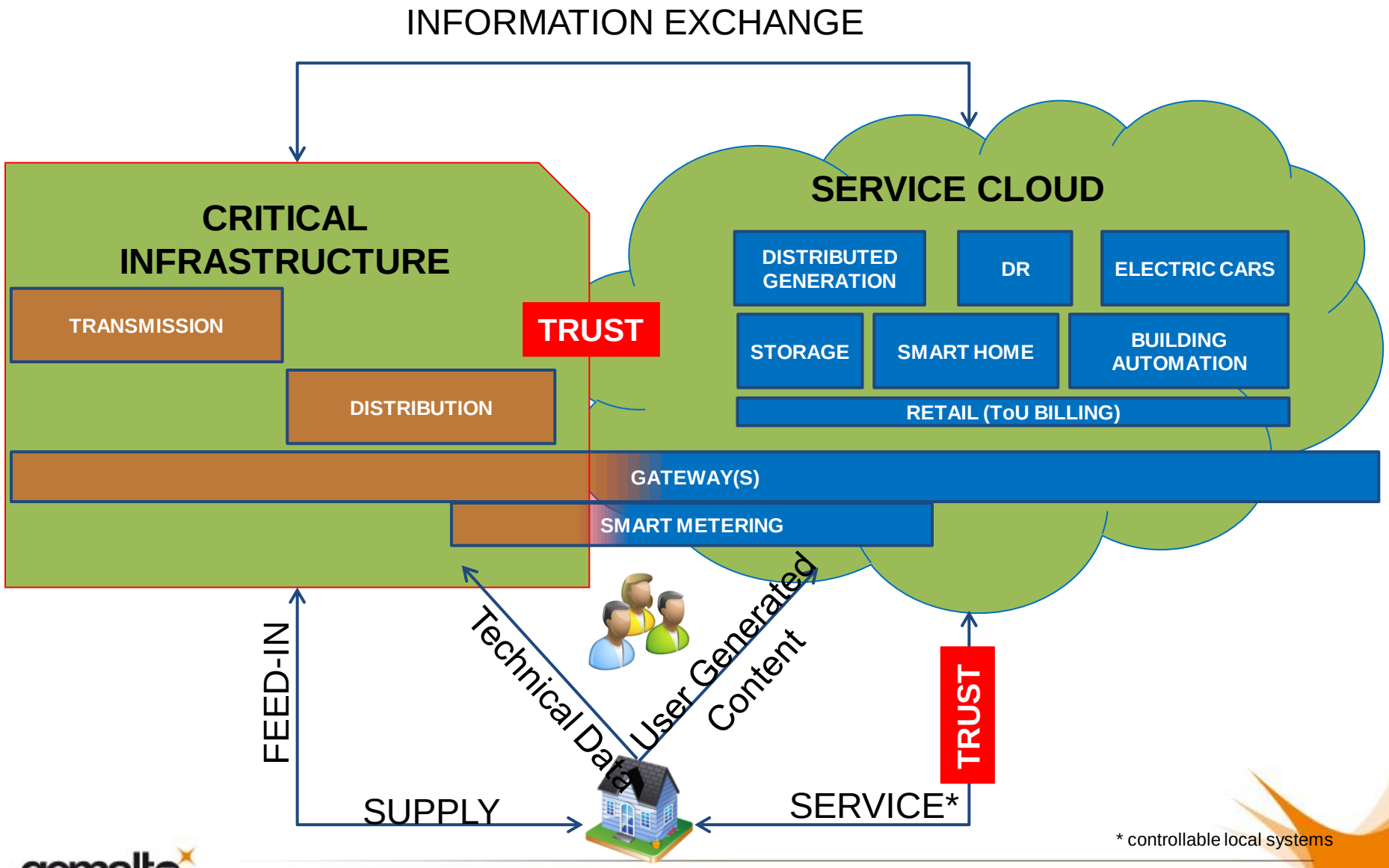
… to smart grid



- Bi-directional energy flow, distributed production
- Numerous actors
- Open information system which is critical for grid management

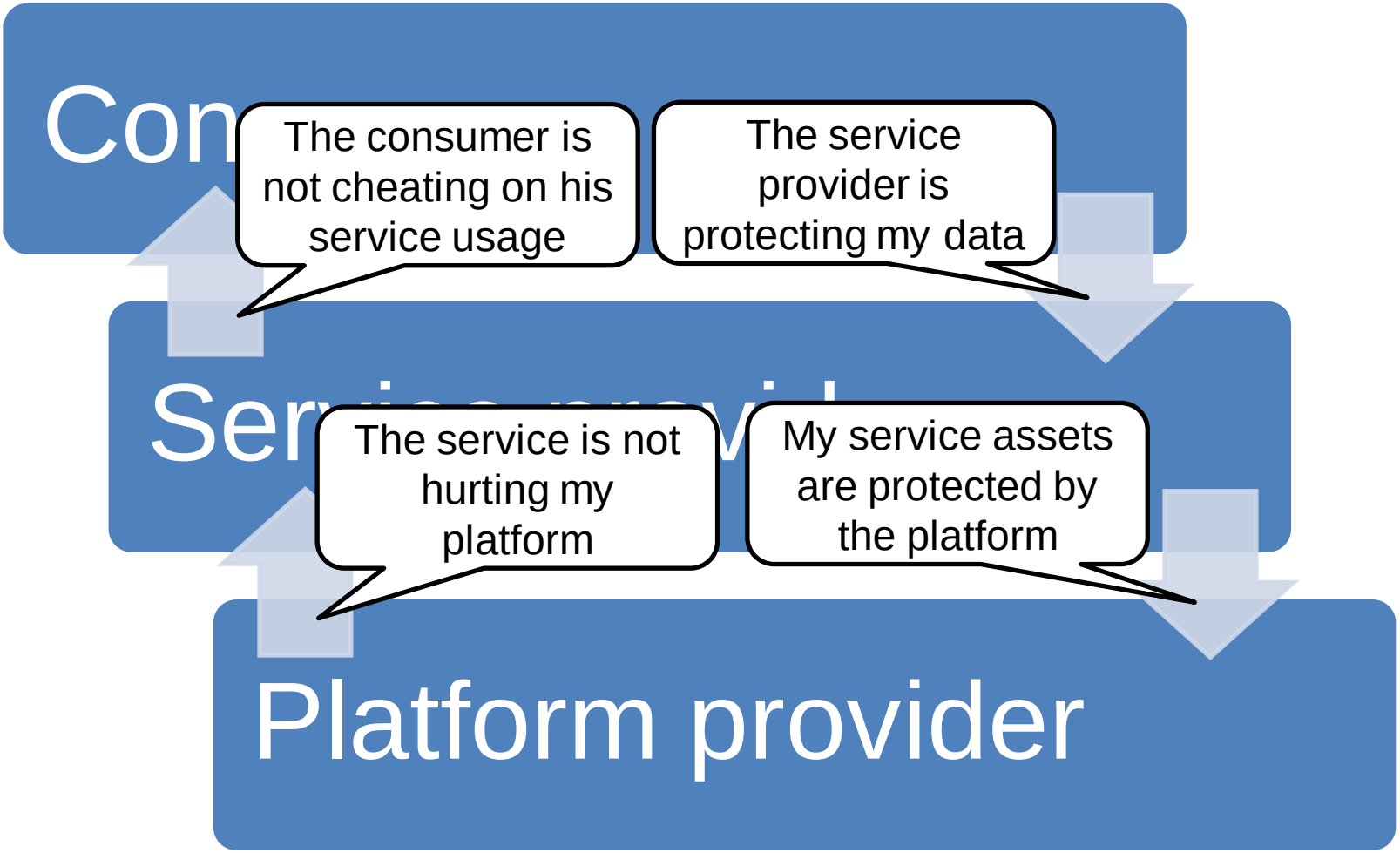


Trust will be the key enabler for a smart energy ecosystem



* controllable local systems

Trust relationships



Software security

- Protected environment
- Trusted users
- Direct access to data

Hardware security

- Unprotected environment
- Non trusted users
- No direct access to data
- **Tamper resistant devices**

Where are smart meters and concentrators ?

Point of Sale terminal

CPU

Memory

Code, data and secrets

Com. Modules

GPRS, RTC, Ethernet, Bluetooth

GUI

LCD, Printer

Business logic

Smart card transaction, risk management
Data signature and up-load

Security

Tampering detection, key erase

Smart Meter

CPU

Memory

Code, data and secrets

Com. Modules

GPRS, PLC

GUI

LCD

Business logic

Metrology, tariff and plans management
Data signature and up-load

Security

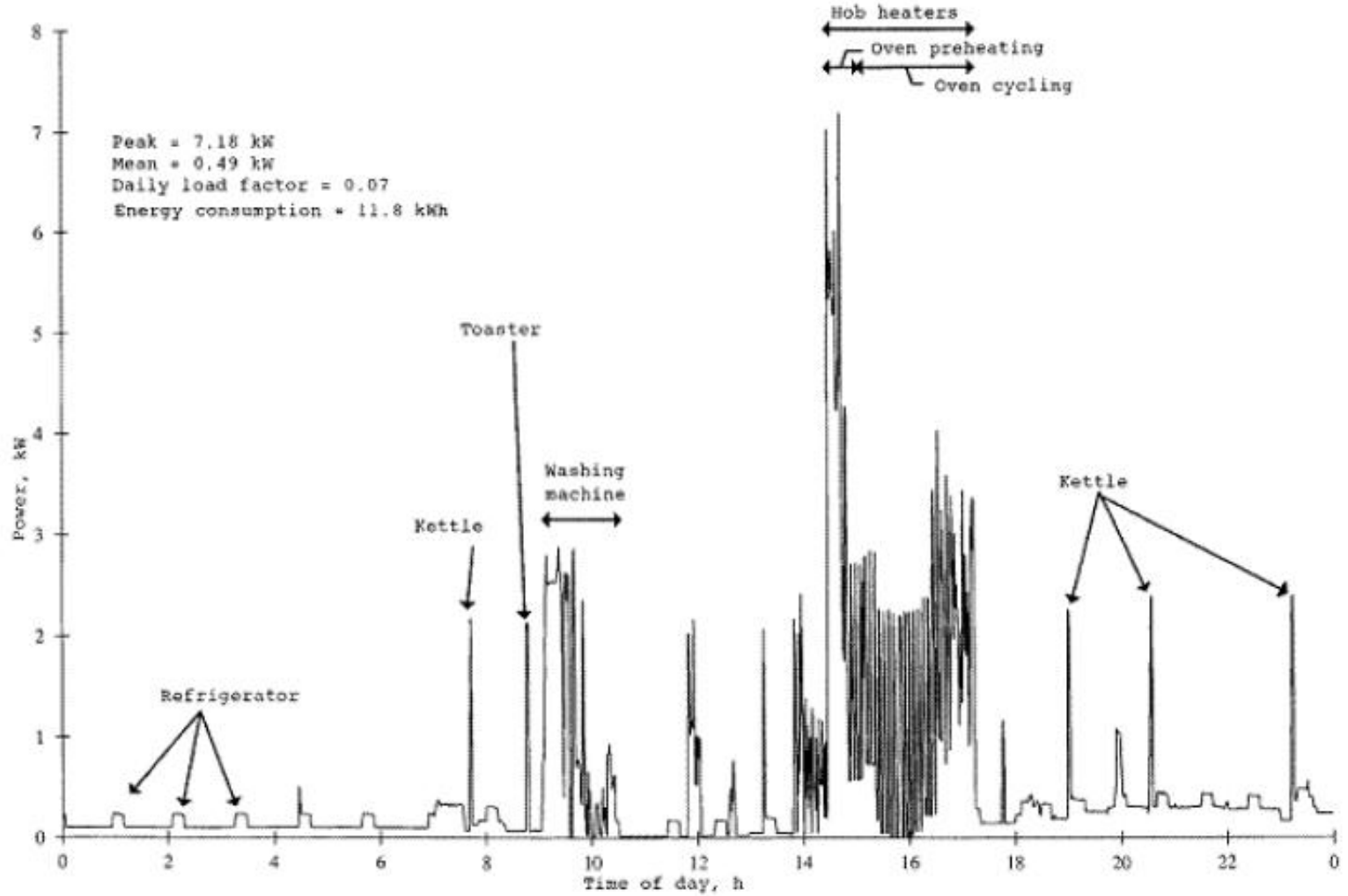
Tampering detection, key erase

Is privacy a problem ?

- We are talking about what is ongoing inside your house !
- Who wants to monitor your load profiles
  - police ? robbers ? tax administration ? tabloids ? immigration service ? and **most probably advertising people !**
- There are some existing regulations but:
  - Need to know principle should apply
  - Explicit consent should apply
  - Privacy enabling technologies can help

Local secure processing will lower data leakage risks

House load curve over 24 hours



Attacks always get better !

Fachhochschule Münster University of Applied Sciences

DaPriM
Data Privacy Management

Hintergrund und experimentelle Ergebnisse zum Thema „Smart Meter und Datenschutz“

Arbeitspapier[1] – Technischer Report, Status: ENTWURF, Version 0.6, Greveler, 20. Sep. 2011

Labor für IT-Sicherheit der FH Münster: Prof. Dr.-Ing U. Greveler, Dr. B. Justus, D. Löhr MSc.
Forschungsprojekt DaPriM (www.daprim.de)

English Abstract: Advanced metering devices (smart meters) are being installed throughout electric networks in Germany (as well as in other parts of Europe and in the United States). Unfortunately, smart meters are able to become surveillance devices that monitor the behavior of the customers leading to unprecedented invasions of consumer privacy. High-resolution energy consumption data is transmitted to the utility company allowing intrusive identification and monitoring of equipment within consumers' homes (e. g., TV set, refrigerator, toaster, and oven). Our research shows that the analysis of the household's electricity usage profile does reveal what channel the TV set in the household was displaying. Moreover, the data being transmitted via the Internet is unsigned and unencrypted. All tests were performed with a sealed, operational smart meter used for electricity metering in a private home in North Rhine-Westphalia, Germany.

Smart Meter und erhobene Daten

im europäischen Rahmen ist die Einführung von intelligenten Strommessgerä-

How about hardware sharing ?

Demand response: gateway

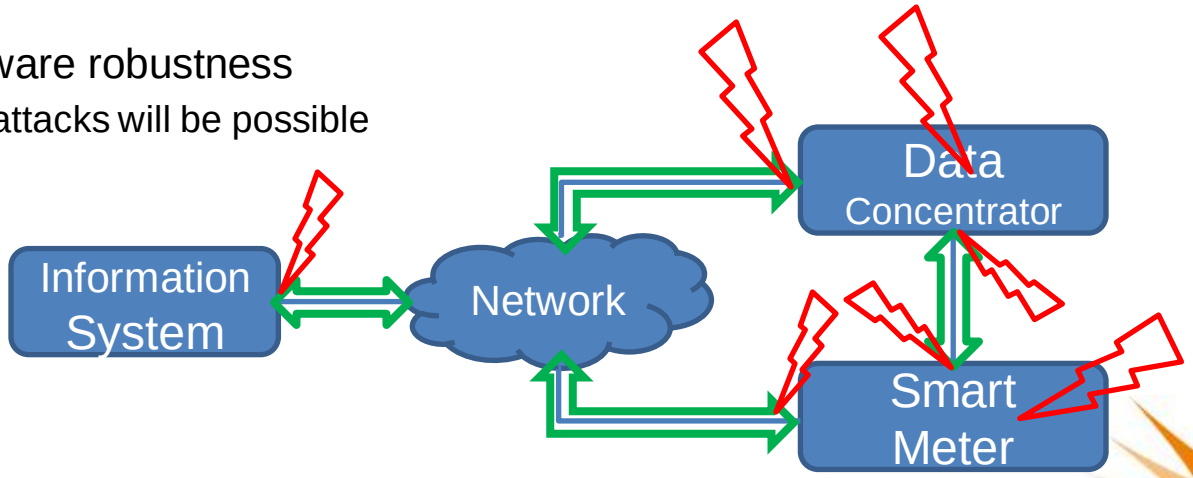
Home energy management

PV array management

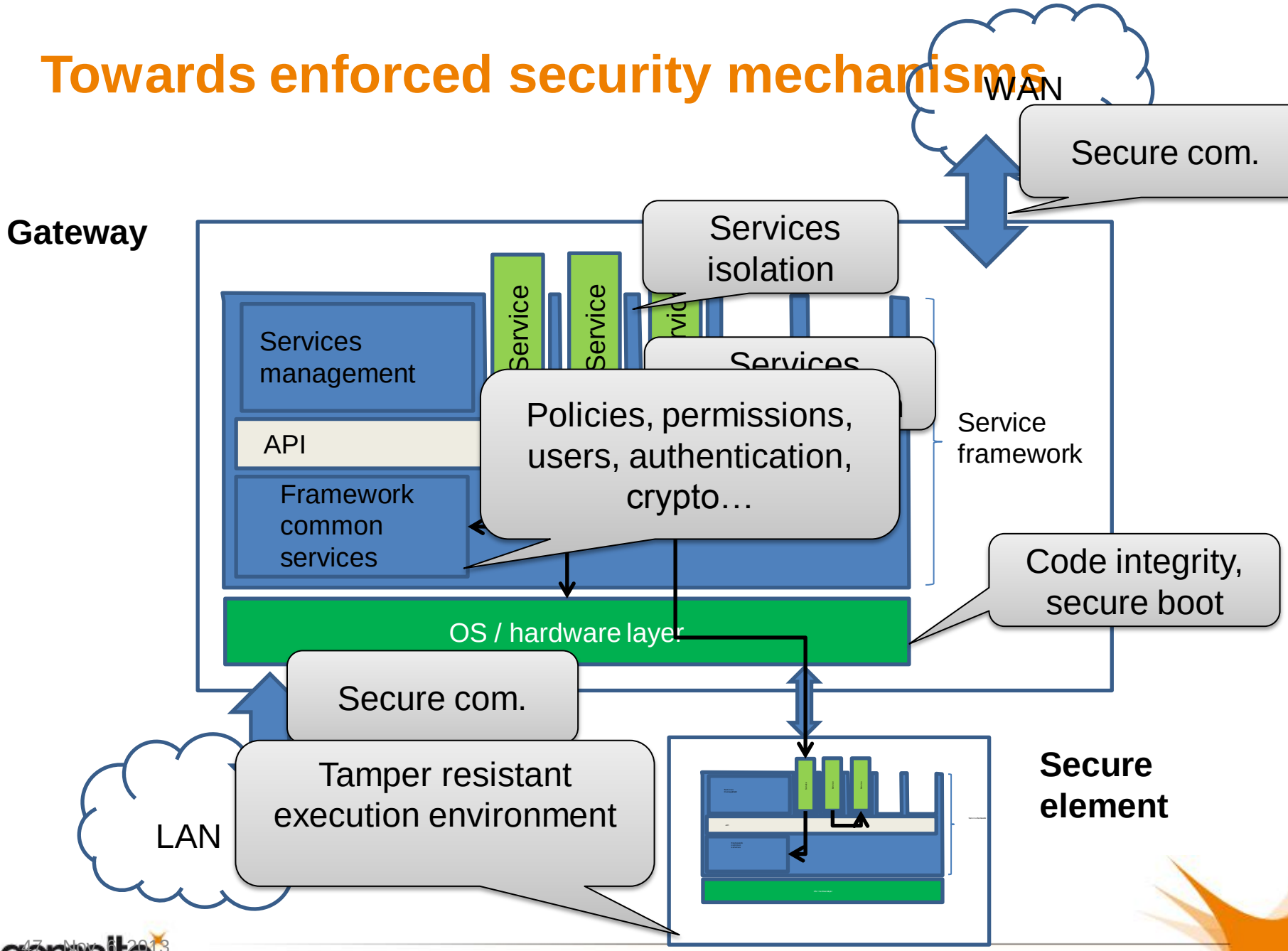
Security mechanisms & weaknesses

- Cryptographic mechanisms start to be introduced
  - Communication encryption
  - Data integrity (e.g. consumption measurements, firmware upgrade)

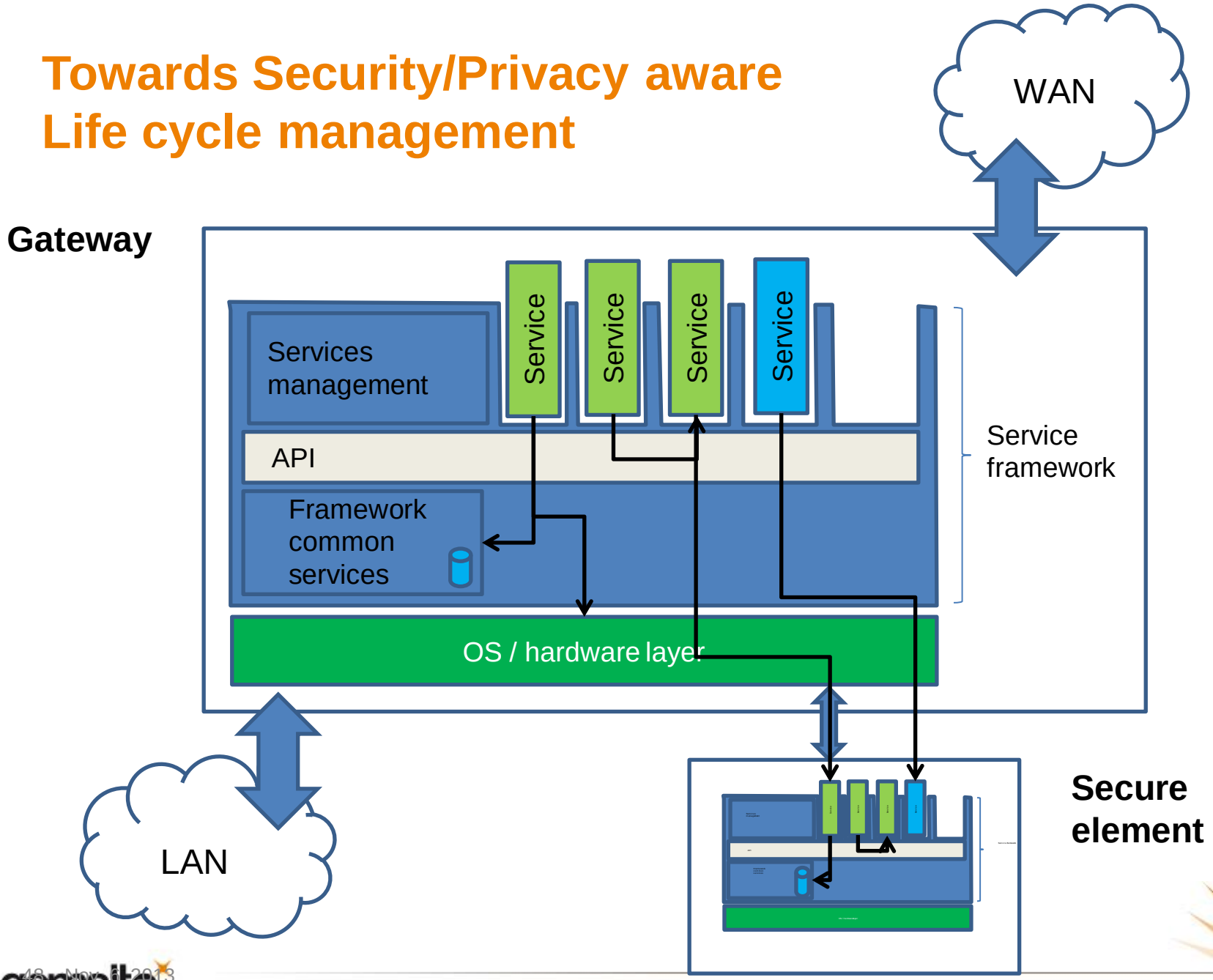
- But end-points remain vulnerable
  - Very limited physical protection
    - No tamper resistance
    - Limited tamper evidence
  - Limited software robustness
    - Remote attacks will be possible



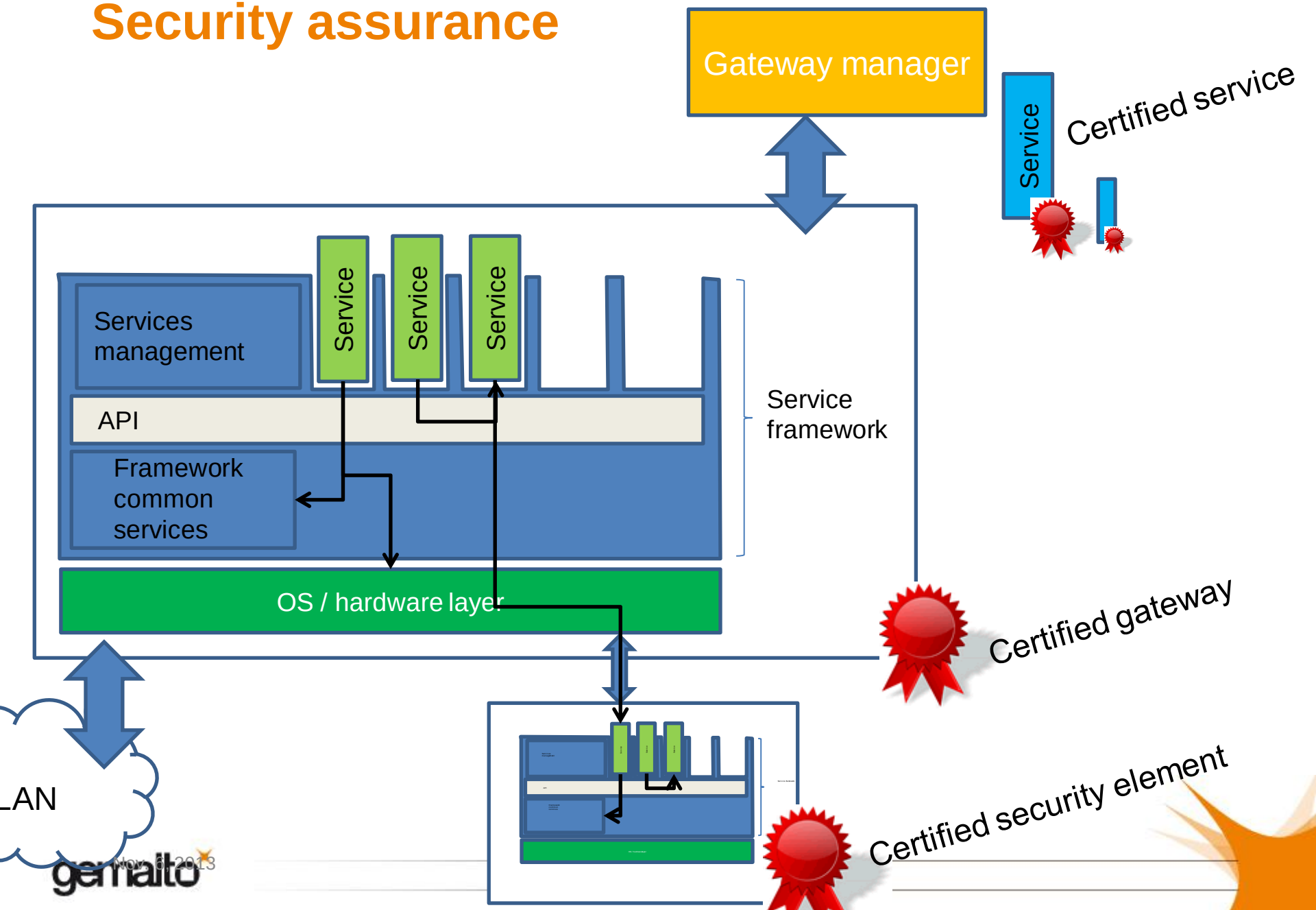
Towards enforced security mechanisms



Towards Security/Privacy aware Life cycle management

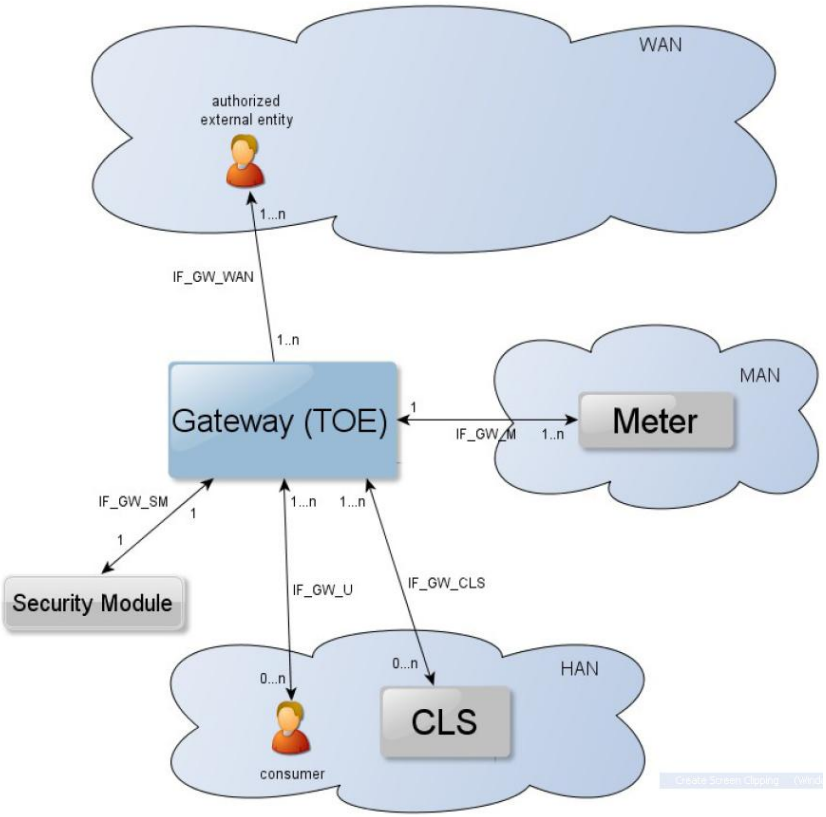


Security assurance



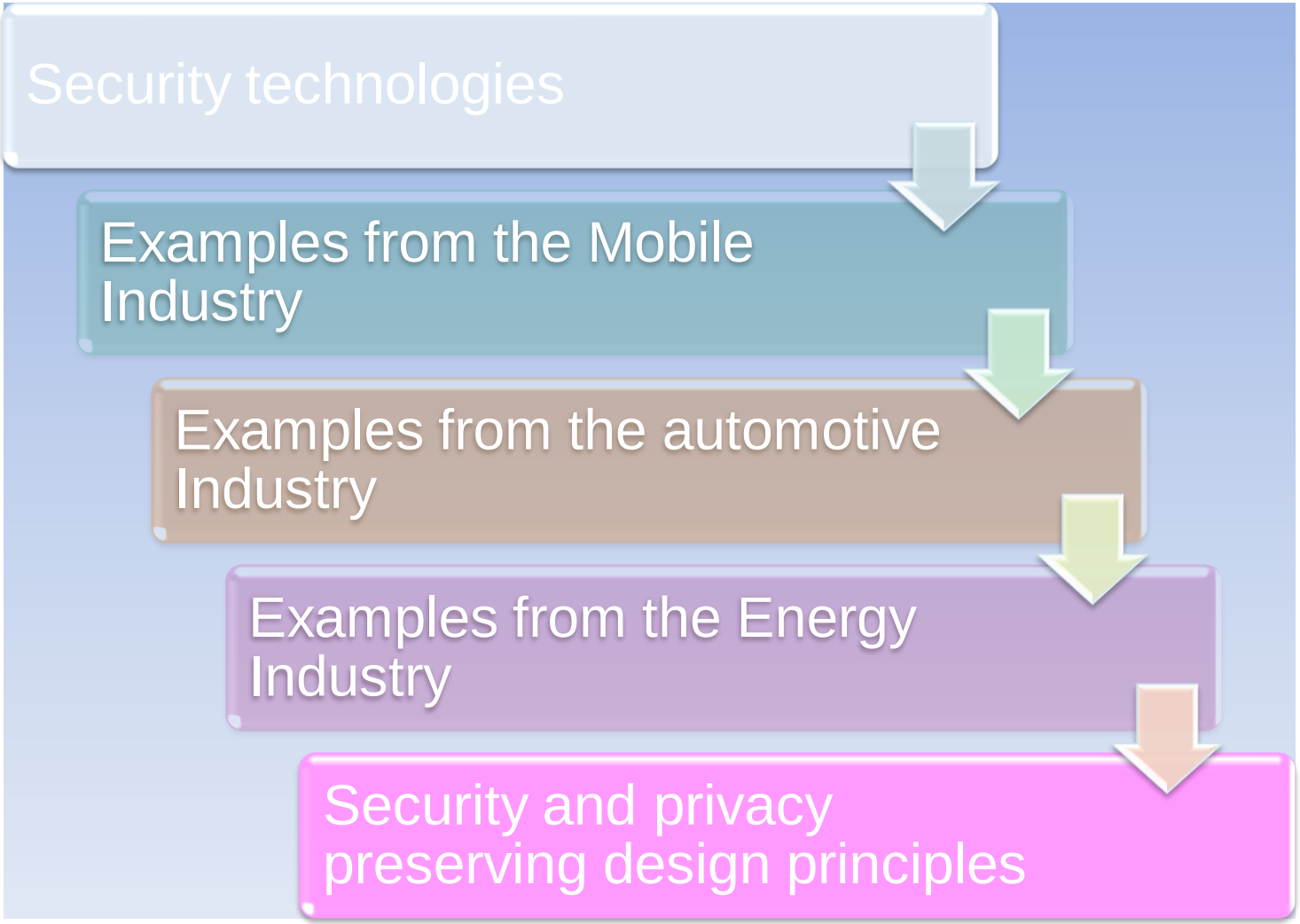
Certification vision in Germany (BSI)

- Protection Profile for the Gateway of a Smart Metering System (EAL4+)



- There will be another PP for the security module (EAL4+)
- No security constraint on the smart meter !

Agenda


Security technologies
Examples from the Mobile Industry
Examples from the automotive Industry
Examples from the Energy Industry
Security and privacy preserving design principles

A security/privacy keeping framework is needed

- Permissions need to be managed based on
  - Service provider / developer identity
  - Certification status
  - User authentication
  - Device (e.g. Car) life cycle state (e.g. in maintenance)
  - Real time context (e.g. speed)
- Of course we need permissions on API
  - But it's not so simple
  - Avoid the "Click I accept" syndrome
- Apps and services will also need
  - Users and device (car!) authentication
  - Billing framework

Security Process

- Detailed risk analysis
  - Identification of attackers and assets
  - Threats and attack scenarios
  - Risk quantification for each scenario
- Validation plan to check equipment against the risks
  - Test list to cover each threat
  - Detailed procedure for each test
- Use/adapt equipment testing in hardware and software attack lab

Identification and authentication

- Management of identities and roles
  - Ex of Roles in Automotive = owner, driver, passenger, shift manager, fleet manager, maintainer, …
- Flexible authentication methods
  - Biometrics
  - Cryptography
  - Hardware based
- Flexible security levels
  - Not the same level needed for kids screen skinning and door opening
- Various form factors
  - USB tokens, SD cards, mobile phone, key fob, driving license, ….

Risk analysis is the most sensitive step

- Who will be the attacker ?
  - Do you protect the consumer or from him ?
  - In cars: owner, driver, passenger, shift manager, fleet manager, maintainer
  - Should we take into account cyber attacks ?
  - Built your own threat model and be prepared to adapt it !
- Quantitative evaluation is difficult
  - How to evaluate the equipment cost ?
    - How about rental, how about new techno (e.g. OpenBTS)
  - How to evaluate the man power ?
    - Hackers teams have an almost infinite man power pool
  - How to evaluate the attack knowledge ?
    - More and more public papers and open source
- Take into account complex/new use cases
  - P2P rental, fleet management, BYOD, open or secure environment
- Take into account the full product life cycle
  - Provisioning, maintenance, reconditioning, ownership change, upgrade, patch, dispose

Attacker Model

- Hacker
  - No physical access to the vehicle
- Malicious Driver
  - Some access to the vehicle
- Malicious Car Repairer
  - Complete access to the vehicle
- Terrorist Organization
  - Attack on the infrastructure

Some points worth thinking

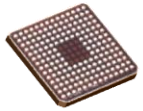
- Avoid security by obscurity
  - Anything can be reverse engineered
  - Examples: Comp128-1 vs Milenage, Mifare vs DesFire
- Design for the unknown
  - Creativity of attackers (e.g. DPA)
- Consider end-to-end security
  - Build your own security (e.g. relying on network security only is risky)

Threats (example)

- Threat 1: Attacker can control some physical elements (ECUs) of a car (locally/remotely)
  - [TH 1.1] Attacker can control some physical elements of a non running car
  - [TH 1.1.1] Attacker can open/close the door of the car (BCM)
    - Locally can mean through a wireless mean
  - [TH 1.1.2] Attacker can start the car engine (ECM)
  - [TH 1.1.3] Attacker can switch off/on the headlights
  - [TH 1.2] Attacker can control some physical security elements of a running car and have an impact on the car safety
  - [TH 1.2.1] Attacker can speed up / slow down the car (SCU)
  - [TH 1.2.2] Attacker can stop the engine (ECM)
  - [TH 1.2.3] Attacker can force the car to brake or can prevent the car to brake (BrCM)
  - [TH 1.2.4] Attacker can launch the AirBag
  - [TH 1.2.5] Attacker can switch off the ABS
  - [TH 1.2.6] Attacker can switch off/on the headlights
  - [TH 1.2.7] Attacker can modify some driving parameters (hardness of brake, softness of direction)
  - [TH 1.2.8] Attacker can modify some comfort elements (massage automactic chair)

Privacy by design Principles

- 1. Proactive not Reactive; Preventative not Remedial
- 2. Privacy as the Default Setting
- 3. Privacy Embedded into Design- Not an add-on
- 4. Full Functionality — Positive-Sum, not Zero-Sum
- 5. End-to-End — Full Lifecycle Protection
- 6. Visibility and Transparency — Keep it Open
- 7. Respect for User Privacy — Keep it User-Centric


Tamper Resistance

EMVCo

MasterCard

VISA

Common Criteria

National Institute of Standards and Technology

FIPS 140-2 FIPS CRYPTOGRAPHY

Bundesamt für Sicherheit in der Informationstechnik

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

gemalto

Conclusion

- Embedded security problems start to be understood
- Several initiatives in the mobile
  - » Samsung Knox
  - » Secure Enclave
  - » SE Linux

- Other domains still embryonic
- Innovative solutions are emerging on the market: TEE, whitebox cryptography, homomorphic VM,…
- Secure Elements are part of the pictures
- Research collaboration between academics and industry is the next MUST

gemalto
security to be free

Thanks for your attention !