escrypt GmbH – Embedded Security
Systemhaus für eingebettete Sicherheit

Vehicular Security Hardware
The Security for Vehicular Security Mechanisms

Marko Wolf, escrypt GmbH – Embedded Security

Embedded Security in Cars Conference (*escar*), Hamburg, November 18th, 2009

SEVENTH FRAMEWORK PROGRAMME
The work is co-financed by the European Commission through the 7th framework program.

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211

The need for vehicular security
Possible attacks in a vehicular environment

Funded by the EU

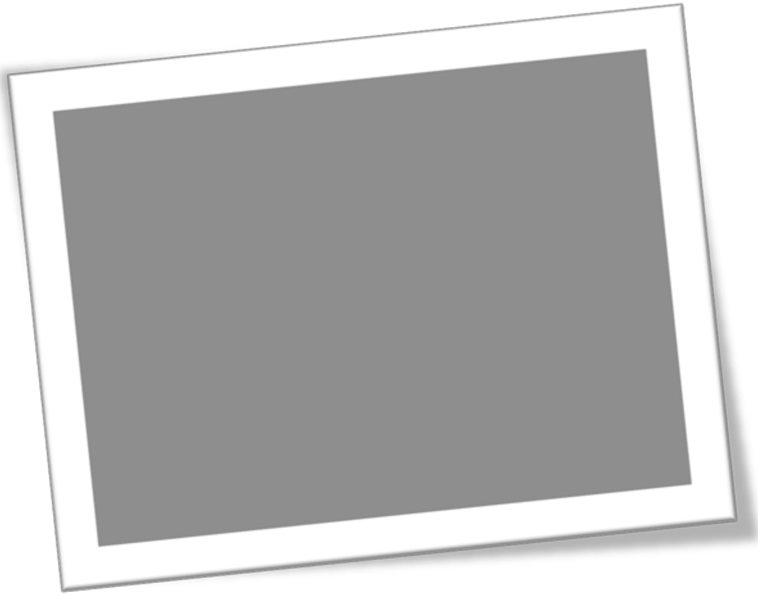
- **Steal** the vehicle or a valuable component
- **Circumvent** restrictions in hardware or software functionality (e.g., speed locks, feature activation, software updates)
- **Manipulate** financially, legally, or warranty relevant vehicular components (e.g., toll devices, digital tachograph, chip tuning)
- **Spy on** manufacturer's expertise and intellectual property (e.g., counterfeits, industrial espionage)
- **Violate** privacy issues (e.g., contacts, last trips)
- **Impersonate** (e.g., electronic license plate)
- **Misuse** external communication (e.g., disturb, misuse, harm)
- **Harm** passengers, destroy OEM’s reputation (e.g., safety attacks)

➲ **Strong need for reliable security mechanisms!**

The security of security mechanisms
Why applying standard solutions won't work

Funded by the EU

- **Beyond "standard attacks" ..**
  - **Insider attacks**
  - **Offline attacks**
  - **Physical attacks**
- **Many different attackers and attacking incentives**
- **Many different attack points**
- **Vehicular IT is client/server, embedded and mobile world**



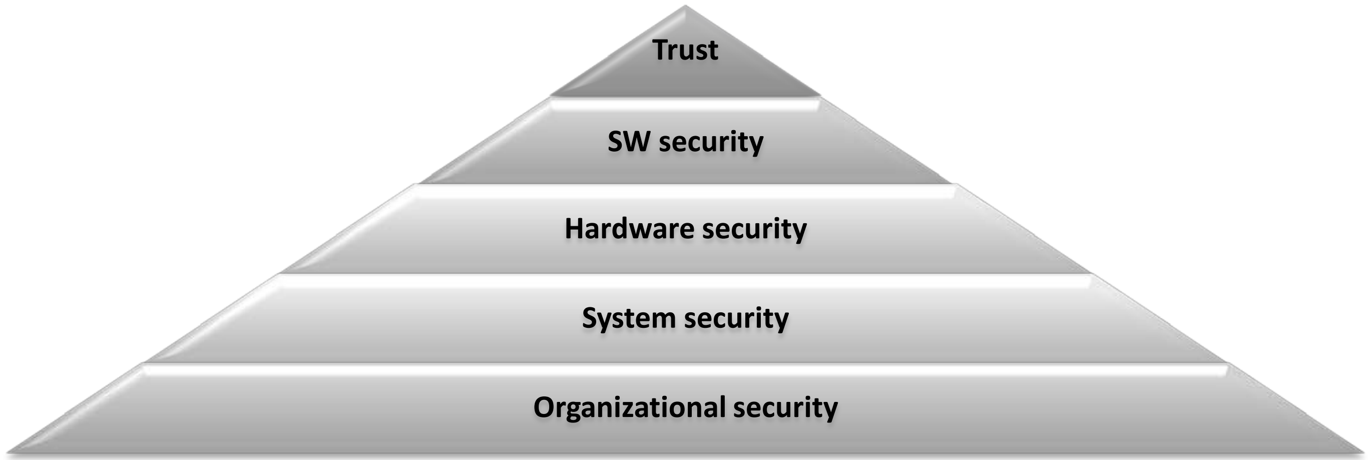
➲ Standard security solutions won't work!

info@escrypt.com

The security of security mechanisms

Trust in security mechanisms

Funded by the EU



- **Organizational attacks** (e.g., social engineering) can be prevented by well-thought *security processes, secure infrastructures and organizational security policies*
- **Logical attacks** (e.g., cryptographic weaknesses or weak APIs) can be prevented by a *secure well-thought security system design and adequate security protocols*
- **Software attacks** (e.g., weak OS mechanisms or malware) can be prevented by reliable *software security mechanisms* (e.g., secure init, secure RTEs) and the application of *hardware security mechanisms that protect & enforce security of software mechanisms*
- **Hardware attacks** (e.g., security artifacts manipulations/read-out, physical locks, side-channels etc.) can be prevented by *hardware tamper-protection measures*

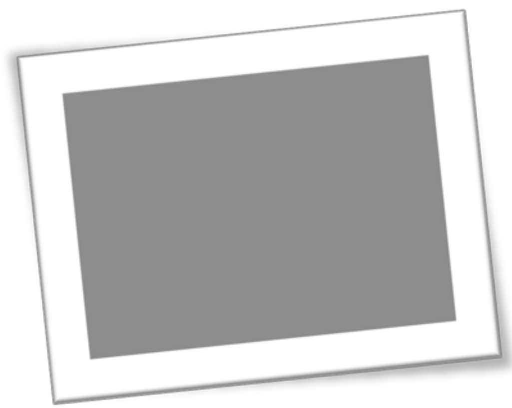
info@escrypt.com

escrypt Embedded Security

Vehicular Security Hardware
What security hardware can help

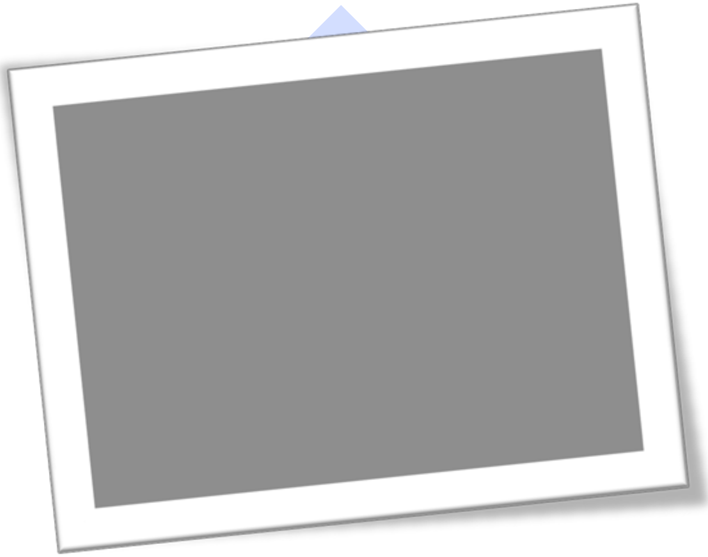
Funded by the EU

- **Protects** software security mechanisms by
  - ➲ Providing a trustworthy *security anchor* for upper SW layers
  - ➲ *Secure generation, secure storage, and secure processing* of security-critical material shielded from all pot. malicious SW
- **Prevents** hardware tampering attacks by
  - ➲ Applying *tamper-protection* measures
- **Accelerates** security mechanisms by
  - ➲ Applying *cryptographic accelerators*
- **Reduces** security costs on high volumes by
  - ➲ Applying highly optimized special circuitry instead of general purpose hardware



Engineering a **Vehicular Security Hardware**
Quick Requirements analysis

- **Security Requirements**
  - High level: creation, storage, management & processing of security artifacts (e.g., keys, certificates, random numbers), authentications schemes, secure “timer” (e.g., clock, counter)…
  - Low level: symmetric engine, asymmetric engine, hash function, TRNG, secure storage…
  - Physical level: Physical coupling, tamper-evidence, tamper-resistance, tamper-response, and side-channel resistance
- **Functional Requirements**
  - Latency and band width
  - Memory, space, and performance
  - Interface compatibility, security updates
  - Physical stress…



- **Other requirements**
  - Costs
  - Patents and export restrictions
  - Certification reg. safety (IEC 61508, SIL etc.) and security (e.g., FIPS 140, Common Criteria)

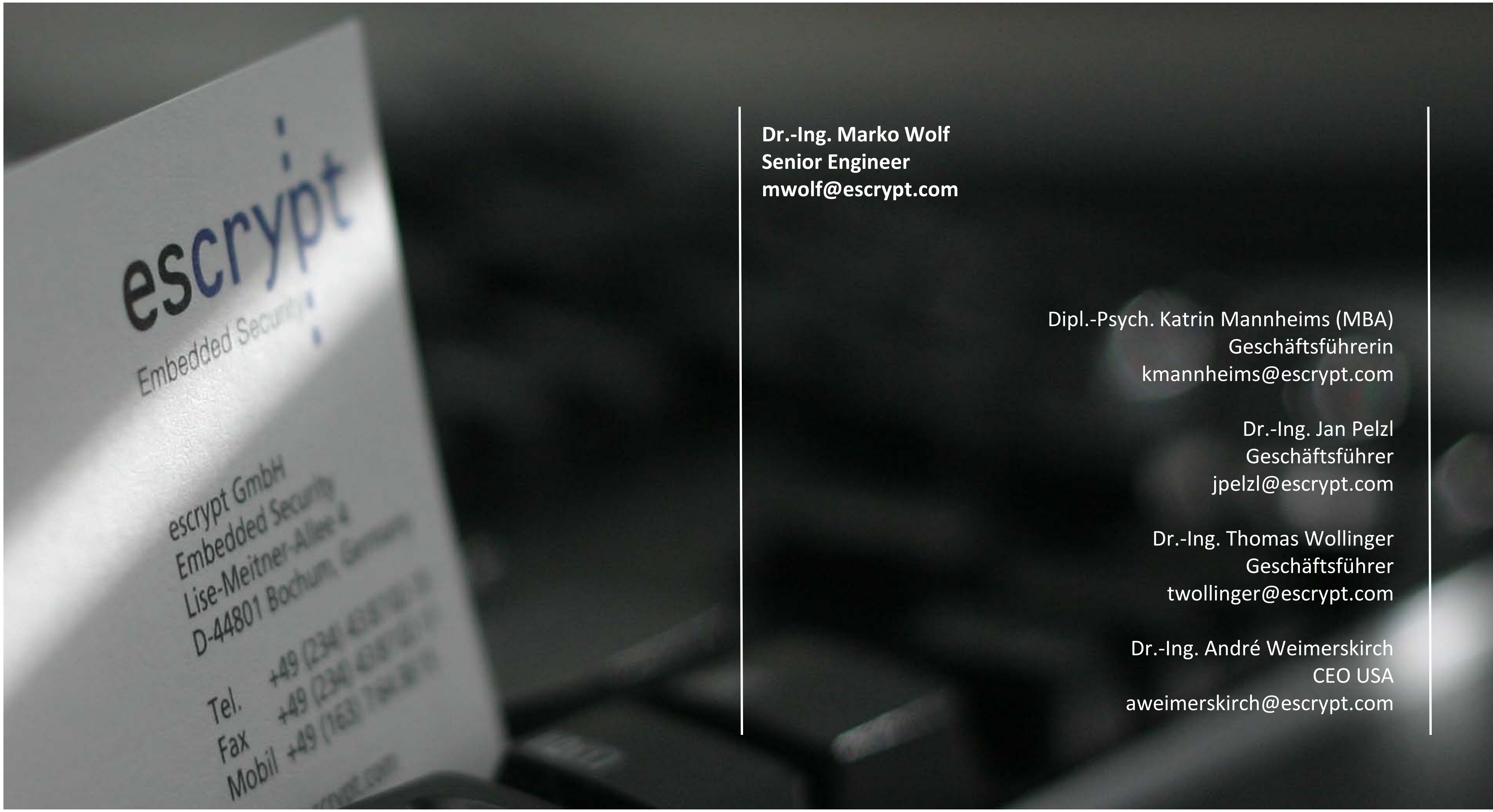
Vehicular Security Hardware
What is the current situation?

Funded by the EU

- **Proprietary** and **single-purpose** hardware security solutions in vehicular environments, for example:
  - Immobilizer
  - Digital tachograph
  - Toll Collect OBU
- General-purpose hardware security modules for **non-automotive** environments , for example:
  - IBM cryptographic coprocessor
  - Cryptographic smartcards
  - Trusted Platform Module
  - Mobile Trusted Module

➲ **Are where any solutions for vehicular security HW?**

info@escrypt.com



Dr.-Ing. Marko Wolf
Senior Engineer
mwolf@escrypt.com

Dipl.-Psych. Katrin Mannheims (MBA)
Geschäftsführerin
kmannheims@escrypt.com

Dr.-Ing. Jan Pelzl
Geschäftsführer
jpelzl@escrypt.com

Dr.-Ing. Thomas Wollinger
Geschäftsführer
twollinger@escrypt.com

Dr.-Ing. André Weimerskirch
CEO USA
aweimerskirch@escrypt.com

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211