escrypt GmbH

Systemhaus
für eingebettete Sicherheit

Automotive Security
Existierende Lösungen und neue Ansätze

Jan Pelzl

Darmstädter „Automotive Software Engineering“-Kolloquim
19. Mai 2009, Darmstadt

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

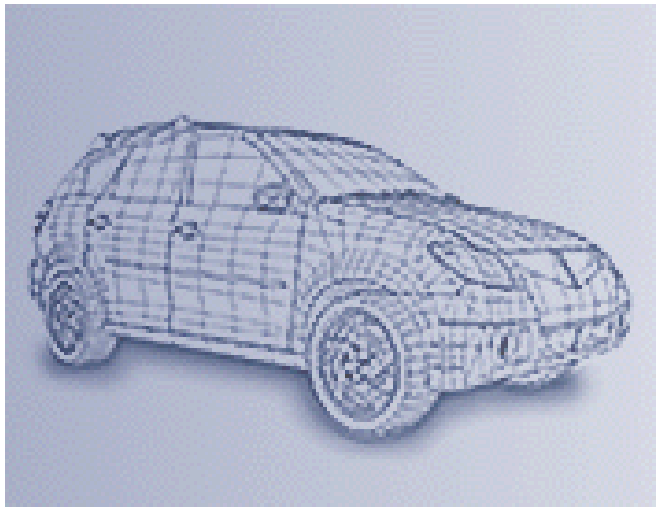
info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211

Übersicht

- Einleitung
  - Historie Sicherheitstechnologien
  - Warum IT-Sicherheit im Fahrzeug?
- Eingebettete Sicherheit im Fahrzeug
  - Dienste
  - Safety und Security
  - Anwendungsfälle im Automotive Bereich
  - Angreifer und Gefahren
- Automotive Security
  - Herausforderungen
  - Lösungsansätze
  - „Best-Practice“
- Case-Studies

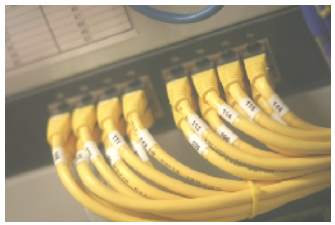
info@escrypt.com

Status Quo



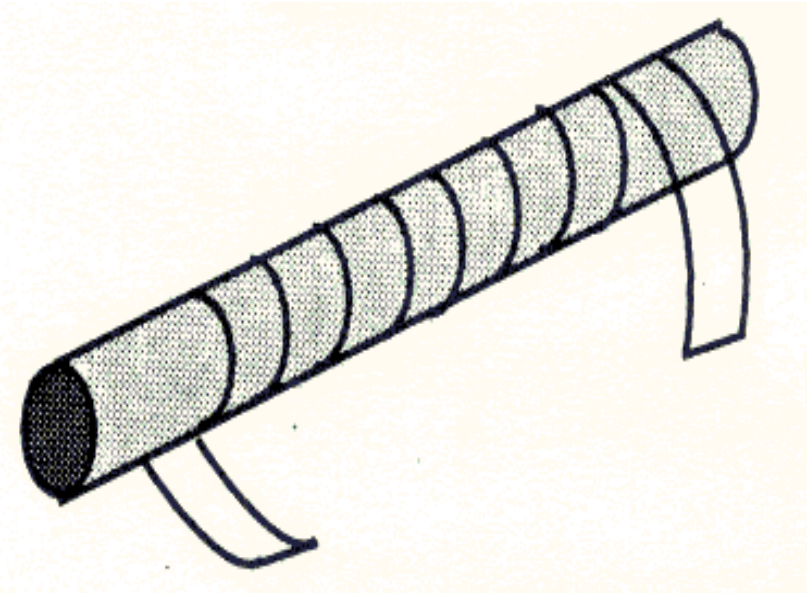
„Wenn das Auto die gleiche Entwicklung wie die Telekommunikation gemacht hätte, dann würde ein VW Käfer heute 10^9 km/h schnell sein, 400 Millionen PS haben, und würde routinemäßig vier mal pro Jahr ausgeraubt, ohne dass der Fahrer es merkt.“

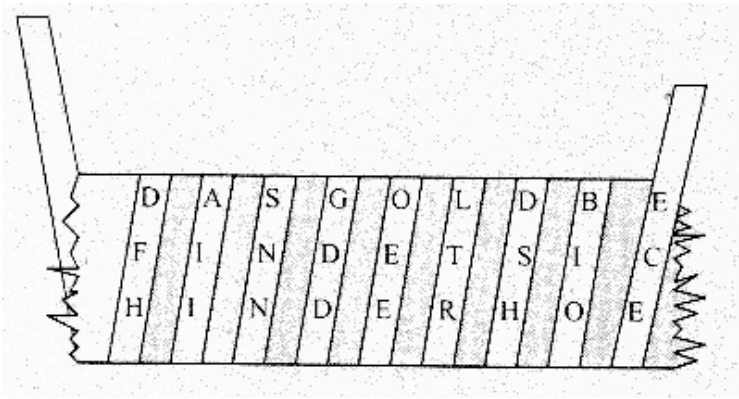
Willi Mannheims
Prof. Christof Paar
escrypt GmbH



info@escrypt.com

Sicherheitstechnologie 500 B.C.





Skytale of Sparta

Sicherheitstechnologie ca. 1940

German Enigma

(Polish, British & US break crucial for allied victory in WWII)

info@escrypt.com

Sicherheitstechnologie 1990

Smart card for banking applications

info@escrypt.com

Sicherheitstechnologie 2000

Electronic road toll

Cryptography:

prevents cheating **by** drivers

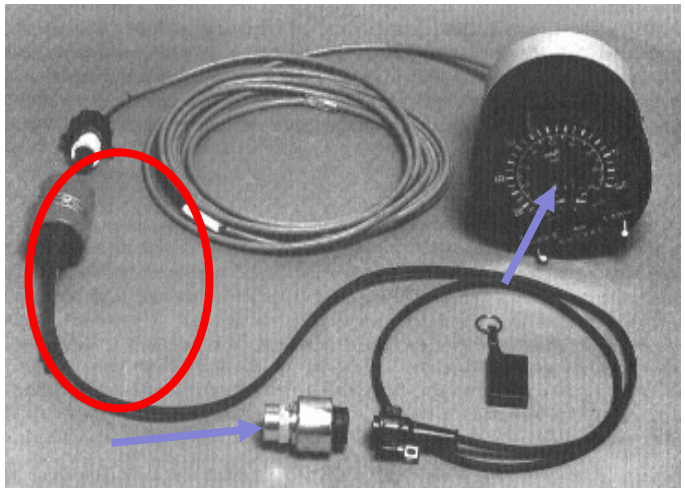
protects privacy **of** drivers

info@escrypt.com

Warum IT-Sicherheit im Fahrzeug?

Fallbeispiel Tachograph

- LKW-Fahrer-Kontrolle per Tachograph: Sensor & Anzeigeinstrument
- Ausgeklügelte Manipulations-Vorrichtung ermöglicht Betrug



Quelle: R. Anderson “Security Engineering”, Wiley, 2001

Aber: IT-Sicherheit kann solche Attacken verhindern
(siehe „digitaler Tachograph“)

info@escrypt.com

Fallbeispiel Wegfahrsperre

- Erste Systeme:
  einheitlicher Code (Passwort)

Code →

- Angreifer hört ab und clont Schlüssel

Verbesserte Wegfahrsperre

- weiterentwickelter Diebstahlschutz: wechselnder Code (zeitvariantes Passwort)

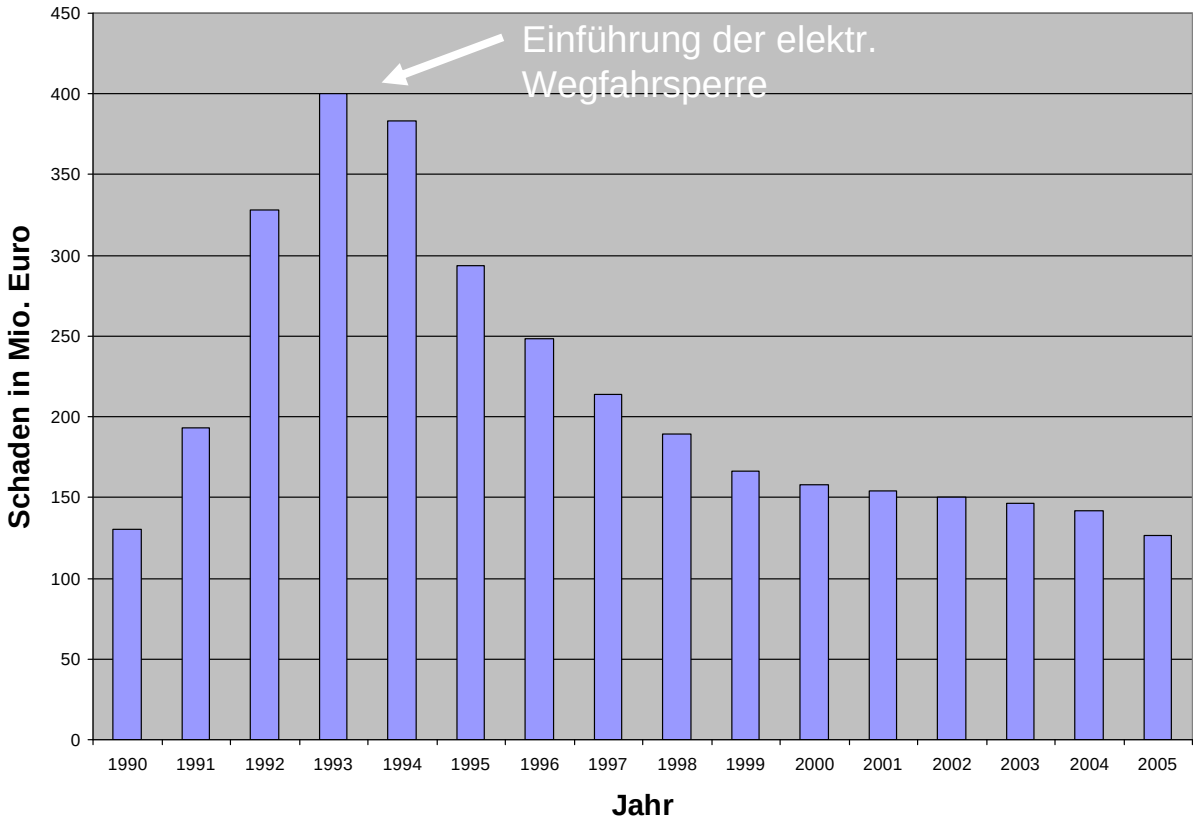
$$code = f_k(T_i)$$

- wobei $f_k()$ eine kryptographische Einwegfunktion ist

info@escrypt.com

Warum IT-Sicherheit im Fahrzeug?

Autodiebstahl: Entwicklung von 1990 bis 2005



Quelle: GDV

Fazit: Moderne IT-Sicherheit kann direkten praktischen Nutzen haben!

info@escrypt.com

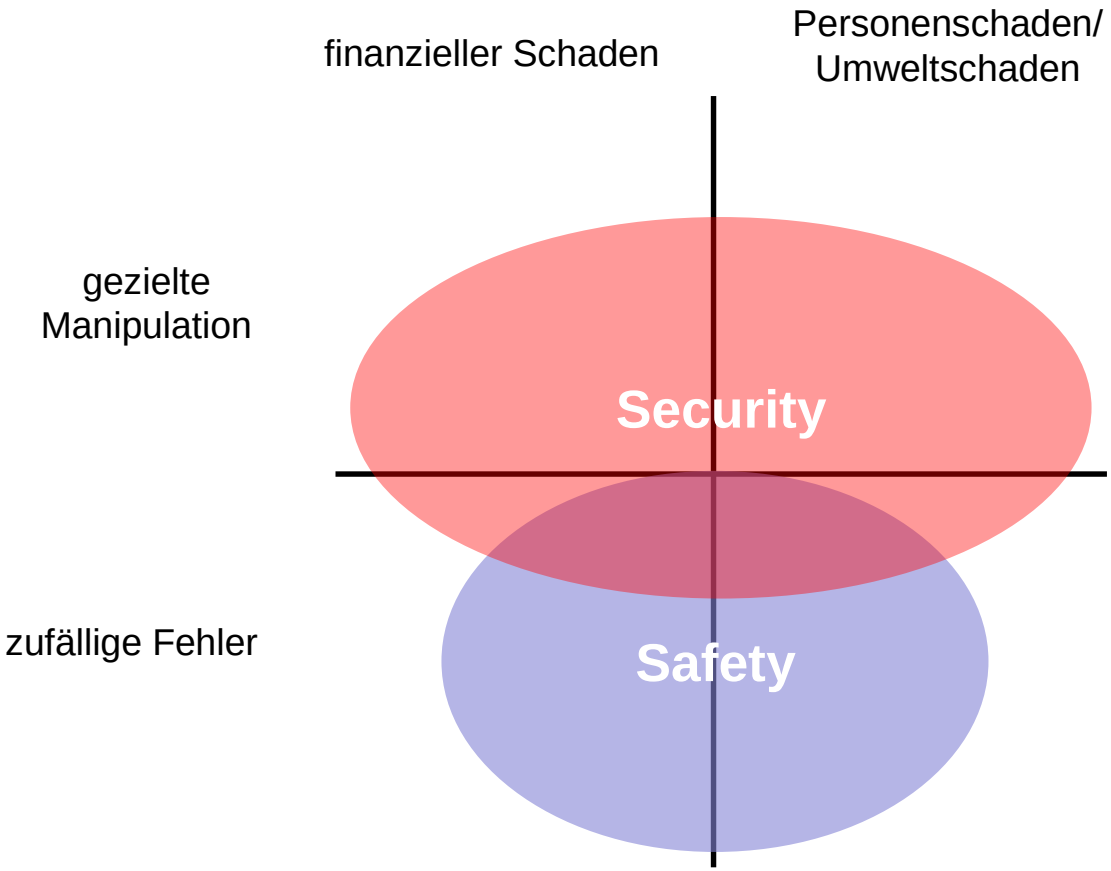
Welche Dienste bietet die IT-Sicherheit im Auto?

- Feststellung der Authentizität, z.B. von
  - Autoschlüsseln
  - Software-Komponenten
  - Hardware-Komponenten
  - Diagnose-Geräten
  - ...
- Integrität von Software und Hardware
- Vertraulichkeit, z.B. von
  - Fahrerinformationen (Navigationsziele, Personalisierung, Telefonbuch, ...)
  - Fahrzeugdaten (Diagnose-Daten, Software-Komponenten, ...)
- Nicht-Zurückweisbarkeit (bei elektr. Signatur von Daten)

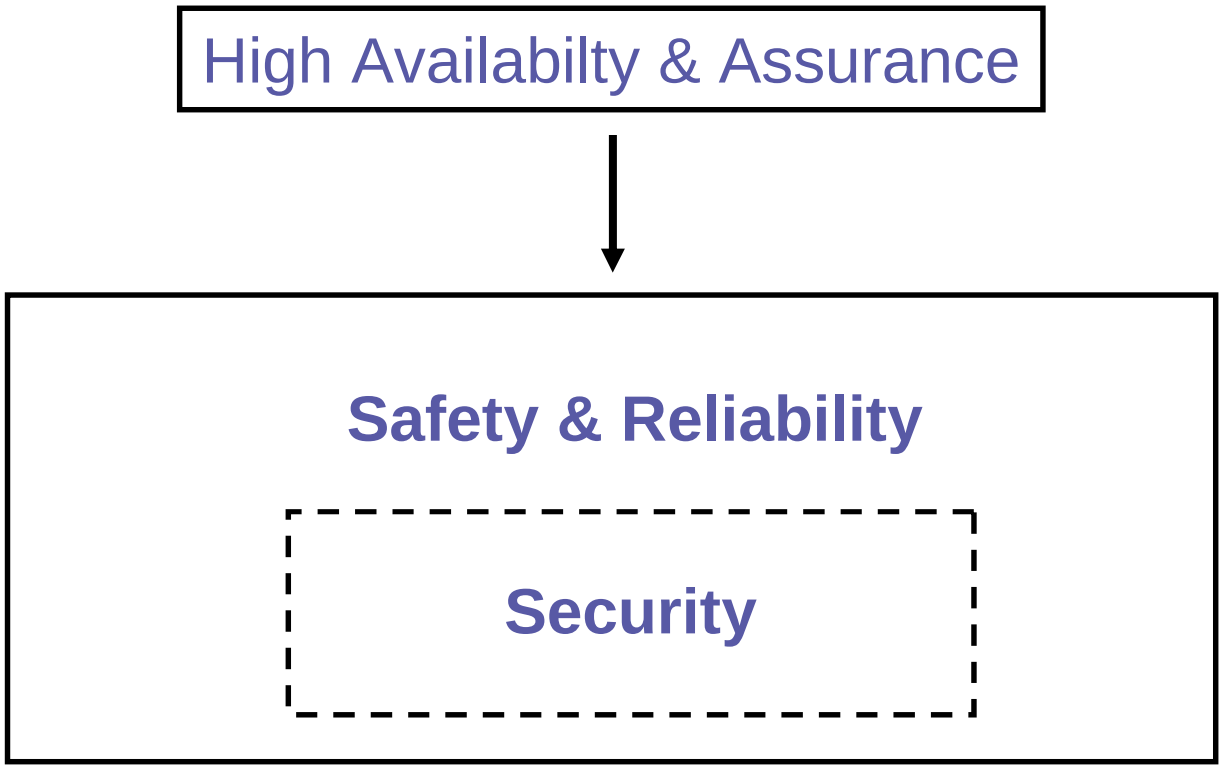
info@escrypt.com

Security vs. Safety (traditionelle Sicht)

§ Schutz durch Safety und Security



Security vs. Safety – Integration



⇒ **IT-Sicherheit als Grundlage für Zuverlässigkeit (Safety & Reliabilty)**

info@escrypt.com

Anwendungen im Fahrzeug mit Sicherheitsbedarf

Sichere Separierung

Software Update

Navigation

Pay-per-Use

Verbesserte Safety

Telematik

Internet

Keyless entry

Wegfahrsperre

Passive entry

Freischaltung

Infotainment

Tracking

C2I

Komponentenschutz

C2C

Tracing

Telefonie

X-by-Wire

Mauterfassung

Sichere Separierung

Location-based Services

Software Download

Komponentenidentifikation

Flottenmanagement

Notruf

Trusted Computing

Remote Immobilizer

info@escrypt.com

escrypt
Embedded Security

Klassifizierung der Angreifer

Besitzer

- geringe bis mittlere Erfahrung
- Physikalischer Zugang

Mechaniker/Mitarbeiter

- Technisch ausgebildet
- Insiderwissen
- Physikalischer Zugang

Wettbewerber/Gruppe

- evtl. sehr große Resourcen
- evtl. physikalischer Zugang

info@escrypt.com

Angriffspotential in derzeitigen Automobilen

Beispiele für attraktive Angriffe:

- Besitzer entzieht sich der Zahlung von Mautgebühren
- Besitzer zahlt nicht für digitale Angebote
- Besitzer erhöht PS-Zahl oder verändert den Kilometerstand
- Dritte spielen böswillig Software Updates auf
- Die Konkurrenz verursacht regelmäßig Störungsmeldungen im Bordrechner
- Die Konkurrenz beschafft sich technische Daten aus Telematiksystemen
- Dritte lesen Fahrerdaten (z.B. Telefonbuch, Navigationsziele) aus
- ...

info@escrypt.com

Herausforderung der eingebetteten IT-Sicherheit

- Moderne IT-Sicherheit bietet:
  - Kommunikationssicherheit
  - Manipulationsschutz
  - Rechtemanagement, Freischaltung, uvm.

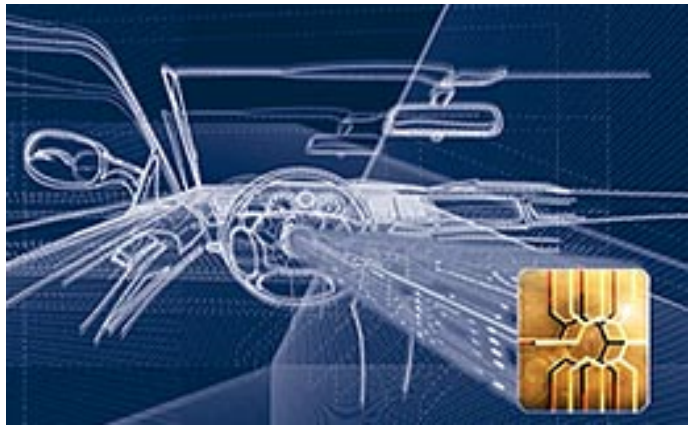
⇒ basierend auf kryptographischen Algorithmen und Protokollen …

⇒ **Alle Sicherheitsprobleme können (theoretisch) gelöst werden**

info@escrypt.com

Herausforderung der eingebetteten IT-Sicherheit

Wo liegt das Problem?



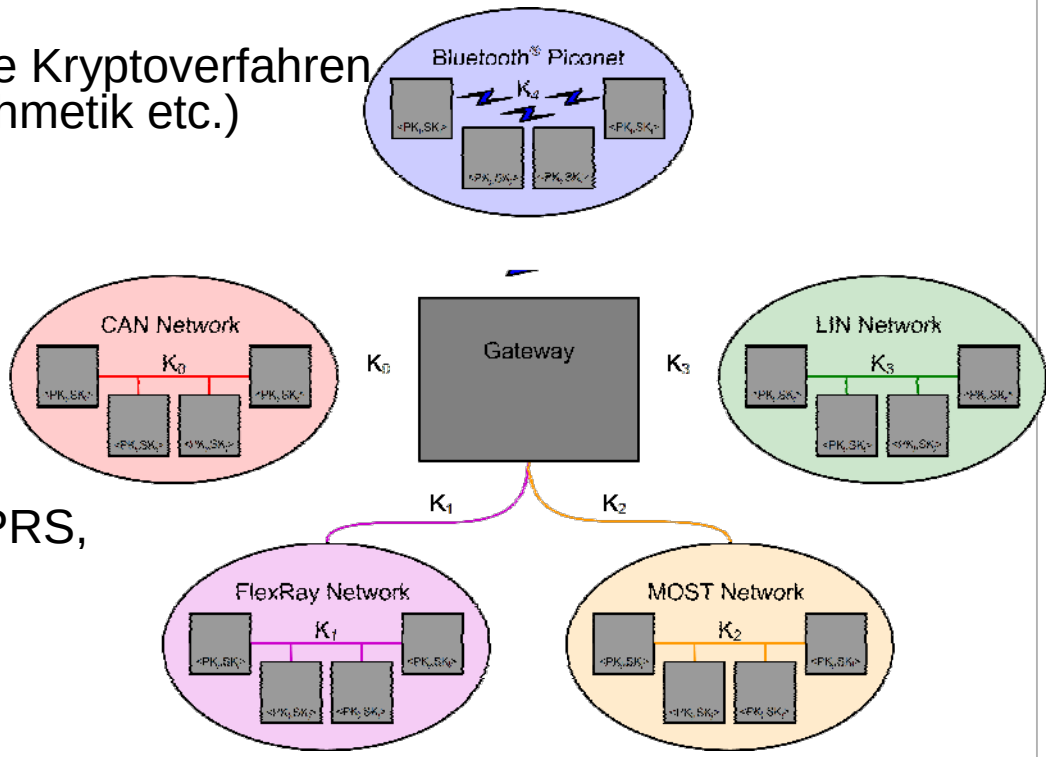
Am häufigsten bei der **Embedded Security**, die sich stark von konventioneller Computersicherheit (Internetsicherheit, Firewalls, ...) unterscheidet!

info@escrypt.com

Herausforderung der eingebetteten IT-Sicherheit

Beschränkte Umgebungen

- 8/16 bit µP für rechenintensive Kryptoverfahren (Algorithmen mit 1024 Bit Arithmetik etc.)
- Energieeffizienz
- ROM/ RAM Beschränkung



Vielfältige Vernetzung

- Interaktion mit Außenwelt (GPRS, WLAN, DSRC, ...)
- Ad-hoc Anbindungen
- Diagnose
- Kommunikation der Steuergeräte untereinander
- ...

Herausforderung der eingebetteten IT-Sicherheit

- **Systemkomplexität/ Life Cycle Management**:
  Viele verschiedene Schichten sind involviert
  (Produktion, 1…x Zulieferer, Eigentümer)
- **Angreifer hat direkten Zugriff auf das Auto**:
  Seitenkanalangriffe, Reverse Engineering, Abhören…
- **Prozesse:**
  Änderung bestehender Prozesse im Bereich Automotive kaum möglich
- **Historische Entwicklung:**
  Zuverlässigkeit ist primäres Ziel,
  IT-Sicherheit ist zweitrangig
- **Kulturelle Probleme:**
  IT-Ingenieure müssen interdisziplinär arbeiten: Kryptografische Algorithmen, Protokolle, physikalische Sicherheit, …

info@escrypt.com

escrypt
Embedded Security

Herausforderung der eingebetteten IT-Sicherheit

- IT-Sicherheit ist anders als z.B. Signalverarbeitung: Die genaue Art der Implementierung ist entscheidend für die Sicherheit
- Beispiel: Seitenkanäle

- Effizienz und Sicherheit manchmal kontraproduktiv
- Sicherheitsmechanismen erscheinen oft umständlich
- Sichere Implementierung erfordern interdisziplinäres Wissen (Mathematik, Physik, Ingenieurwissenschaften, Informatik, ...)
- Entwickler benötigen aktuelles Wissen

info@escrypt.com

Lösungsansätze mit IT-Sicherheit

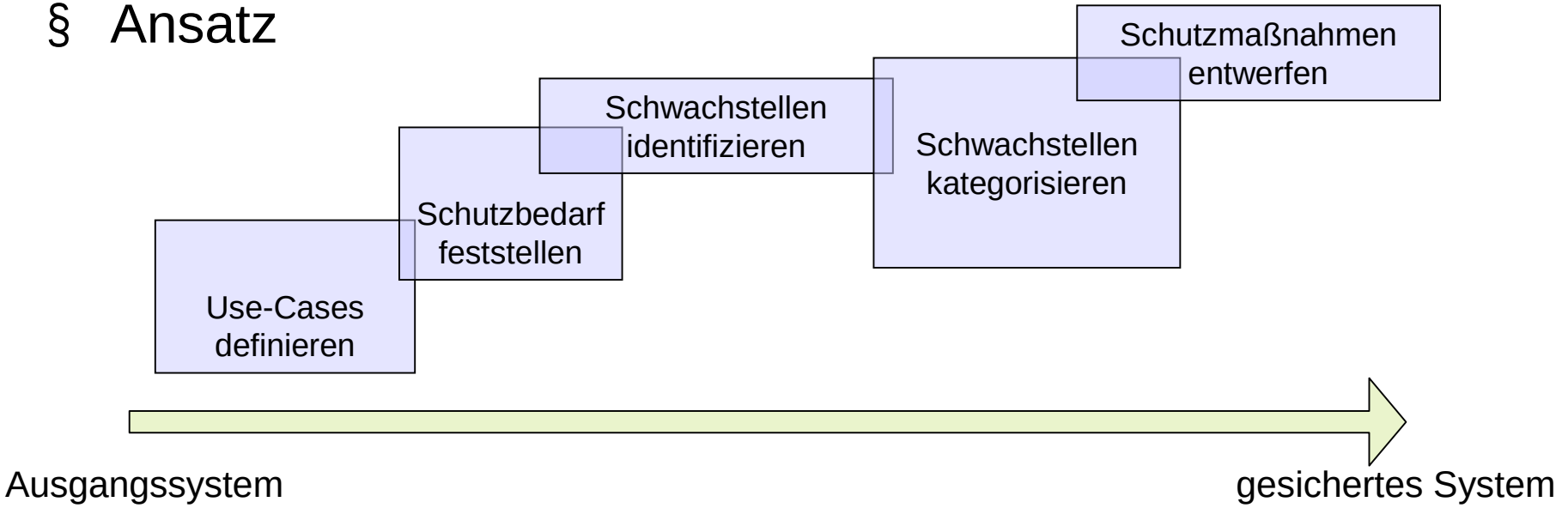
- Organisatorische Maßnahmen
  - Sicherung des Backends (z.B. für Diagnose, Fernwartung, Freischaltung, ...)
  - Security-Policy
  - Rollen und Prozesse
- Technische Maßnahmen
  - Sicheres Systemdesign (ganzheitliche Sicherheit)
  - Realisierung von
    - Authentizität
    - Integrität
    - Vertraulichkeit
    - Nicht-Zurückweisbarkeit
  - Software Krypto-Toolbox
  - Hardware-Maßnahmen

info@escrypt.com

Strukturierte Vorgehensweise

- Systematische Vorgehensweise
  - Standard-Vorgehen bei Schwachstellenanalyse
  - Ganzheitliche Analyse unter Betrachtung aller Aspekte (Automobil, Back-end, Kommunikation/ Netzwerk, Schlüsselmanagement)

- Ansatz



Sicherheitsziele und Schutzbedarf

§ Identifikation von Anwendungsfällen (Use-Cases)

§ Identifikation von Schwächen und Angriffspfaden

§ Kategorisierung von Schwächen und Angriffen, z.B. nach CC:

- § “Required time for an attack”
- § “Expertise of the attacker”
- § “Required knowledge of the attacker”
- § “Window of opportunity”
- § “Required equipment of the attacker”

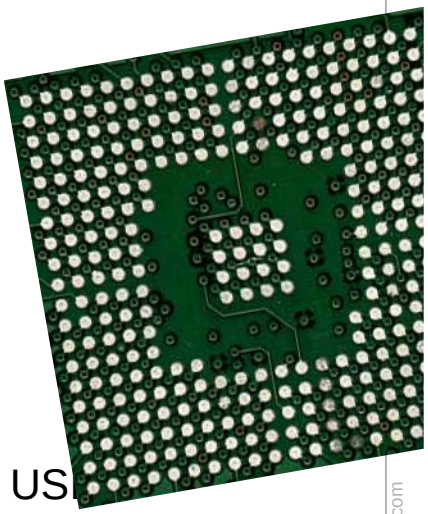
§ Entwurf angemessener Sicherheitsmaßnahmen

info@escrypt.com

Auswahl an Sicherheitsmaßnahmen

- Algorithmen in Software und Hardware
  - Kryptographische Primitive und Protokolle (Vertraulichkeit, Authentizität, Integrität, Nicht-Zurückweisbarkeit, ...)
  - Seitenkanal-Resistenz
  - Weitere Methoden (“obfuscation”, ...)

- Hardware Sicherheit
  - Algorithmen in Hardware
  - Gegenmaßnahmen zu Seitenkanälen
  - ”Tamper-Evidence”
  - “Tamper-Resistance”
  - “Tamper-Responsiveness”
  - Absicherung des Gehäuses
  - Sicheres PCB Layout
  - Sicheres IC Design
  - Abschalten von Interfaces (z.B. serielle Schnittstelle, Netzwerk, USB, JTAG, ...)
  - ...



info@escrypt.com

escrypt
Embedded Security

Best Practice: Economical Security

“Economical Security”:
Ansatz für kosteneffiziente Sicherheitsmaßnahmen

§ Schutzbedarf identifizieren

§ Sinnvolle Maßnahmen einführen

§ Fokus: Kosteneffiziente Realisierung

§ Aufsetzen auf existierende Prozesse

► Optimum an Sicherheit bei minimalem monetären Aufwand

info@escrypt.com

Case Studies

- Secure Flash-Update
- Secure Feature Activation
- Hardware Security
- IP Protection

info@escrypt.com

Case Study: Secure Flashing (1)
Motivation and Attack Scenarios

- Motivation
  - more and more control units allow software updates (flashing)
  - allows extended possibilities such as
    - Bug fixing in the field
    - Customization
    - New products (SW tuning kits)
    - …

- Threats
  - Attacker (=owner?) flashes malicious software onto device
    - system becomes unreliable
    - endangerment of safety (e.g., car electronic)
    - endangerment of business cases (loss of revenue)
    - ...

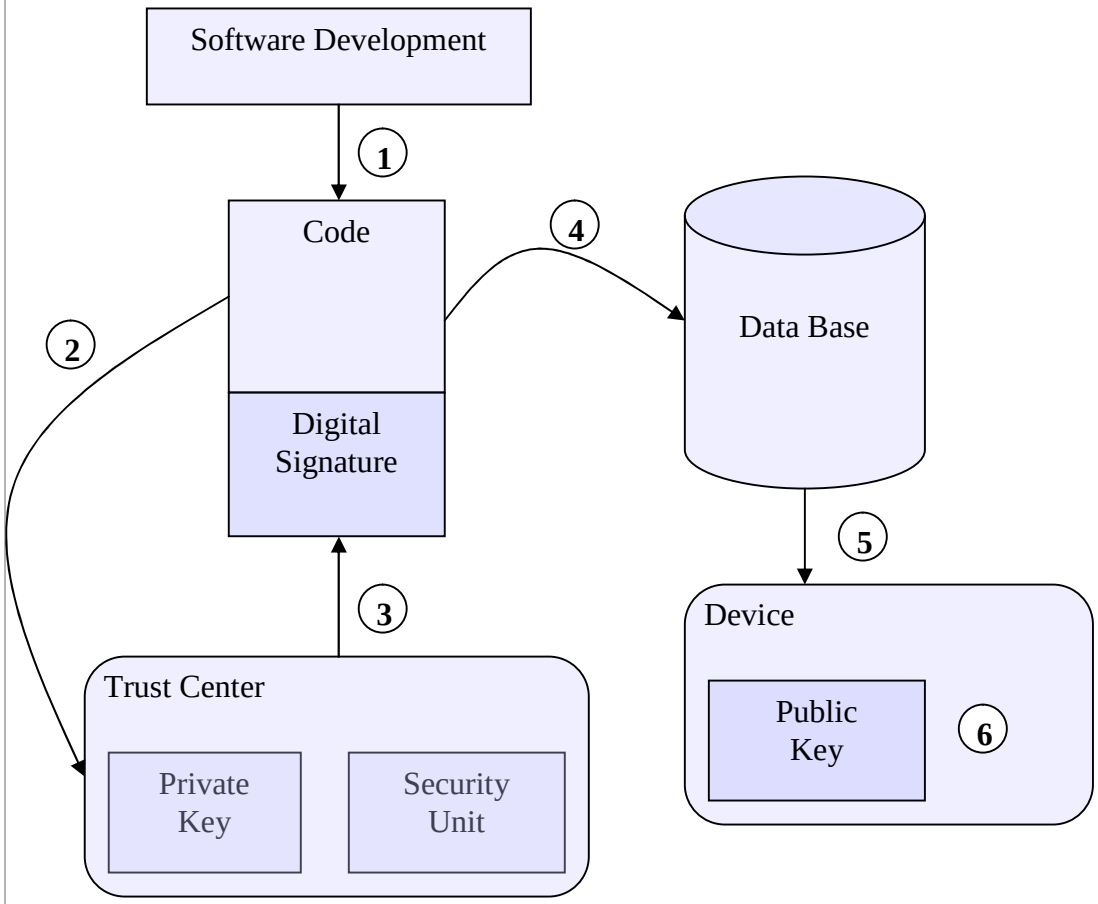
Case Study: Secure Flashing (2) Security Goals and Solution

- Security goals
  - check integrity and authenticity of software
  - optional: provide confidentiality (IP protection etc.)

- Solution
  - Cryptographic functions during boot
  - Challenges:
    - embedded crypto (small, fast, cost-efficient)
    - side-channel resistant
    - resistant against reverse engineering

info@escrypt.com

Case Study: Secure Flashing (3) System

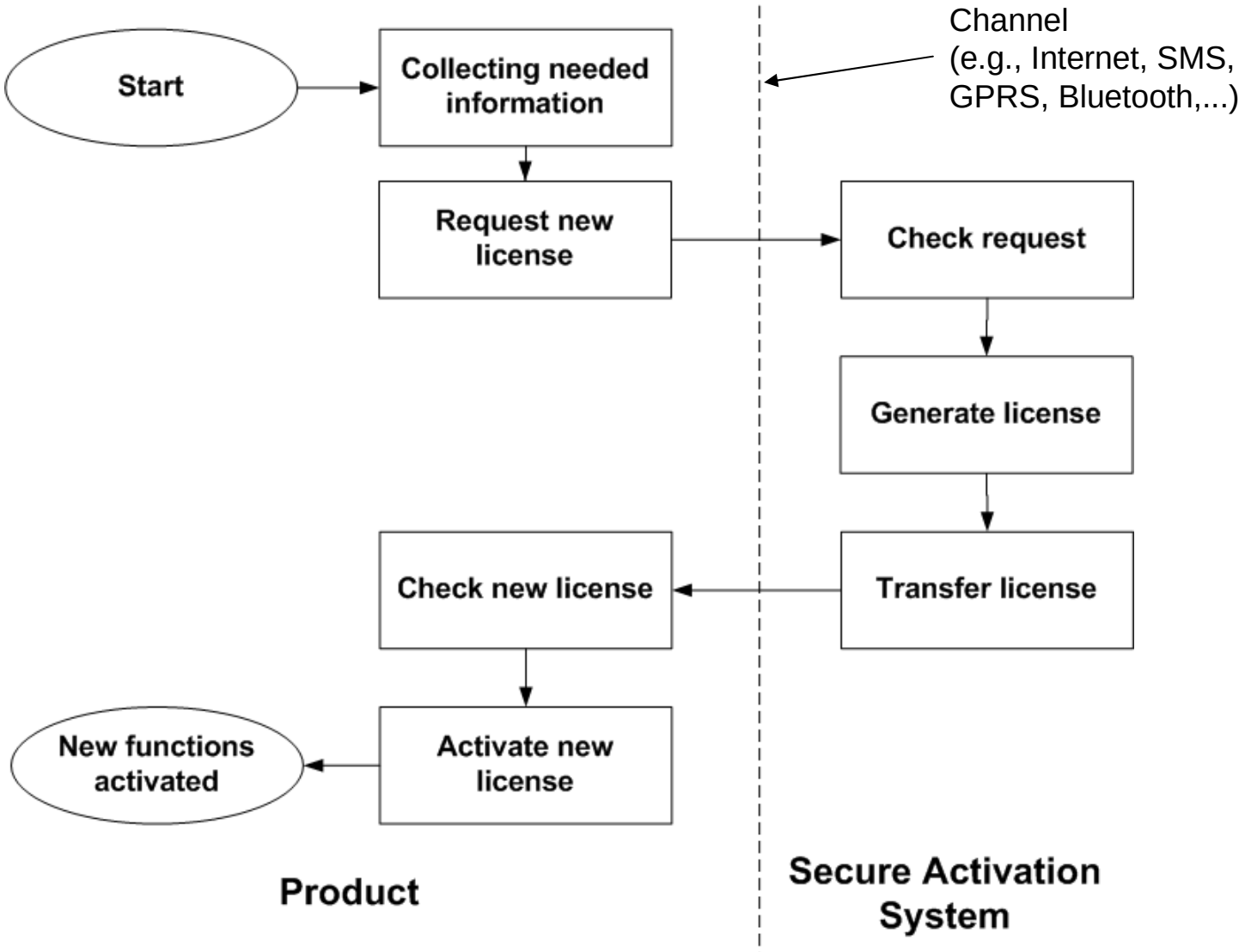


1. Generation of code
2. Trust center signs code
3. Append signature to program code
4. Store program code and signature in data base
5. Flash operation
6. Verification of flash image **inside** the device with public key of trust center

Case Study: Secure Feature Activation (1)
Motivation and Requirements

- Motivation
  - Variable functional range in products
  - Functional range in products defined with (temporary) licenses/ activation codes
  - Function activation later in the field (by costumer/ manufacturer)
  - New business models for manufacturers
  - Produce one product, sell several products with different functionality

Case Study: Secure Feature Activation (2) Principle

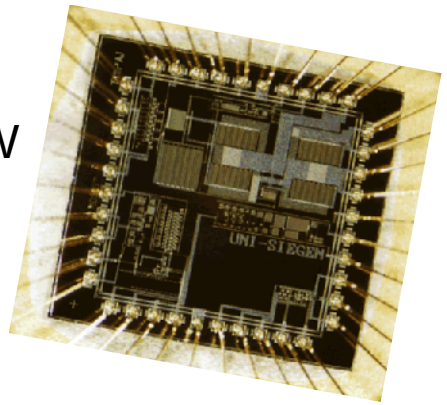


Case Study: Hardware Security (1)

- Why security in hardware?
  - Isn‘t cryptography, protocols and secure system design sufficient?

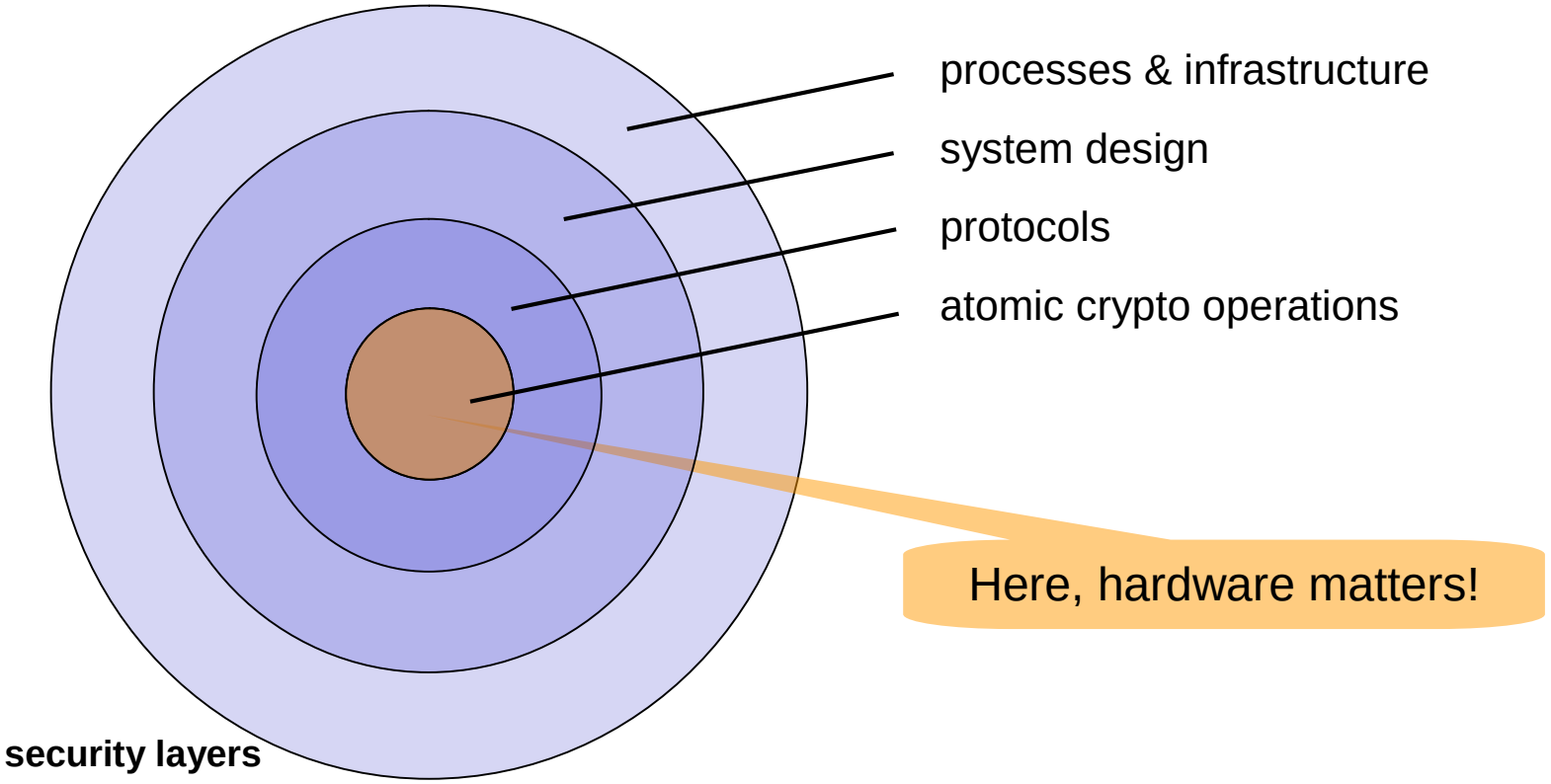
- Main reasons for secure hardware:

1. **Performance:** HW can be much faster than SW
2. **Security:** Manipulation in HW harder
3. **Costs:** HW cheap at large quantities



Case Study: Hardware Security (2)

How do we achieve security in applications
(e.g., secure flashing, immobilizer, trusted platform, …)?



Case Study: Hardware Security (3)
Security Techniques for the Automotive Domain

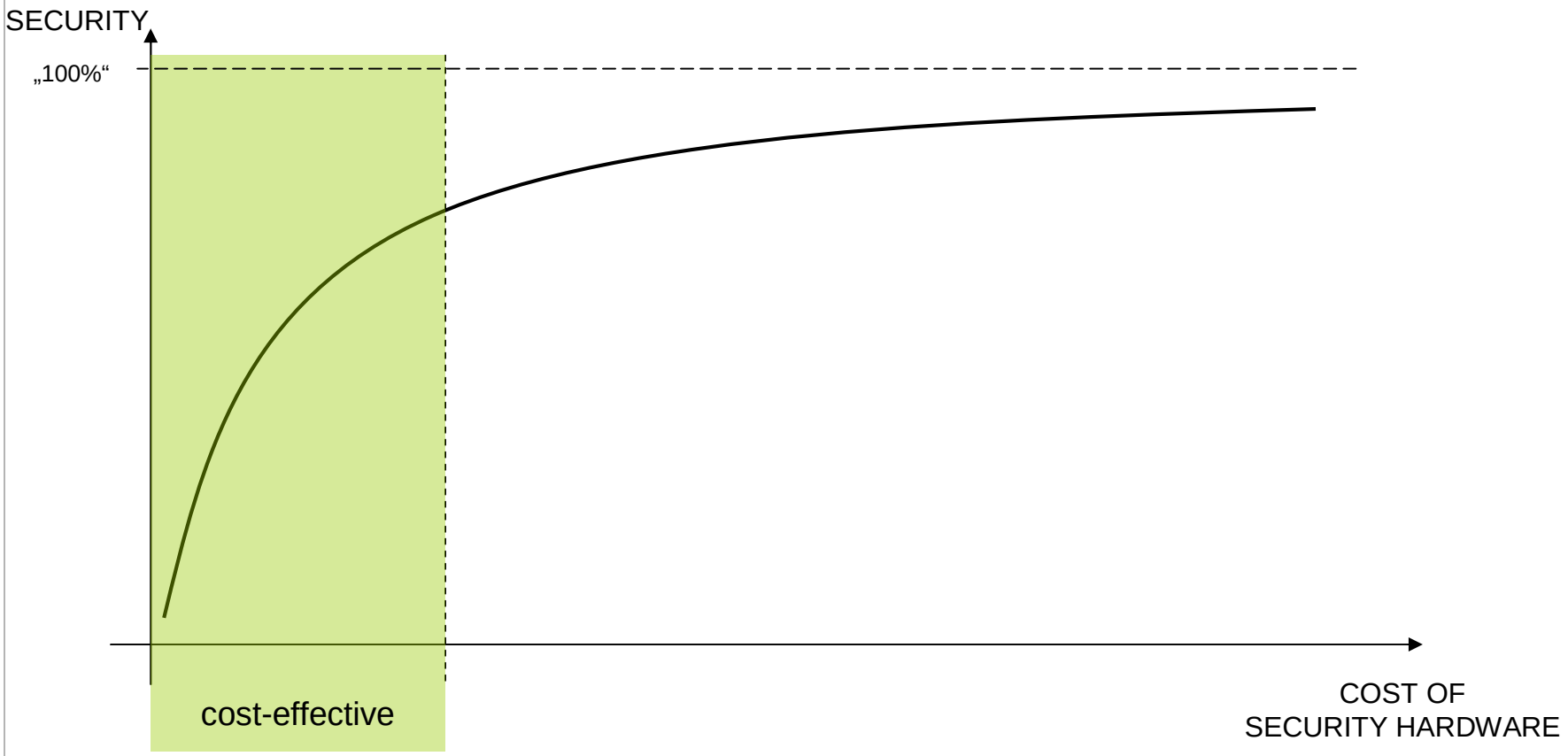
- **Binding** of arbitrary software to a certain vehicle hardware/software configuration
- Secure **separation** of processes (user space vs. safety critical apps.)
- Access possible only by previously **authorized** hardware/software configuration
- Software **distribution** using a fully non-trusted infrastructure
- **Limiting** software updates to a certain vehicle brand, vehicle type or even to a single car
- **Prevention** of unauthorized updates, modifications, copies, and configurations

info@escrypt.com

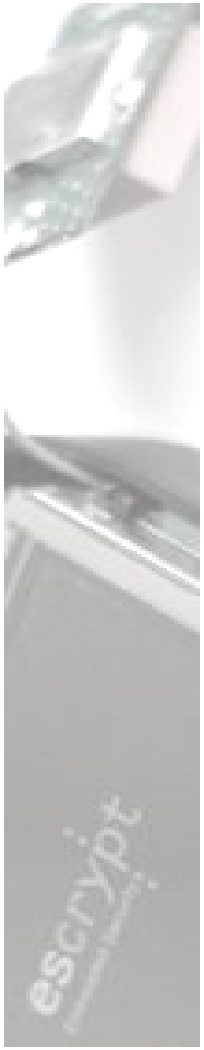
escrypt
Embedded Security

Case Study: Hardware Security (4)
How much Security Hardware do we need?

Security vs. utilization of security hardware



Case Study: IP Protection (1)



- Motivation
  - more and more control units allow software updates (flash technology)
  - High proportion of total costs for software development
  - Prevention of copying/ cloning necessary
- Threats
  - (Flash) Memory easily accessible for attackers
    - Cloning of flash images
    - Modification of software
    - Illegal use of IP for other products
  - Cloning/ copying threatens ROI of SW-Development
  - Loss of lead over competitors
  - ...

info@escrypt.com

escrypt
Embedded Security

Case Study: IP Protection (2) Solutions

- Security goals
  - Confidentiality of software
  - Integrity of software
- Practical approach
  - Encryption of software or parts, e.g.
    - at boot up time
    - each time before execution
  - Signing of software or parts
- Requirements
  - “Trusted platform” (i.e., boot code must be trustworthy)
  - Functions for security checks
  - More advanced: Hardware security, PUFs, ...

info@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
Embedded Security

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

escrypt

System Provider for Embedded Security

- **International provider of solutions for embedded security**
- **Security products and consulting services**
- **Target industries: automotive, industrial, consumer electronics, health, mobile, smart card, RFID, etc.**
- **escrypt provides solutions and services to global leading companies**
- **Areas of competence: system design, lightweight security, trusted computing, cryptographic hardware, security analysis, secure back-end solutions** […]