

escrypt GmbH



Systemhaus
für eingebettete Sicherheit

Embedded Security Chances and Challenges

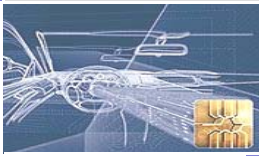
BITKOM Forum Embedded Security
15. Oktober 2009, Nürnberg

Jan Pelzl, escrypt GmbH

escrypt GmbH
Lise-Meitner-Allee 4
44801 Bochum

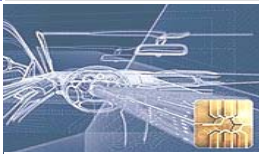
info@escrypt.com
phone: +49(0)234 43 870 209
fax: +49(0)234 43 870 211





Outline

- What is an embedded system?
- Motivation for IT-security in embedded applications
- Challenges in the embedded domain
- Solutions for IT-security
- How much security do we need?



What is an embedded system?



+



=

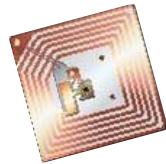
Embedded
System

- „Processor in a product“, or
- „A computer which does not look like a computer“

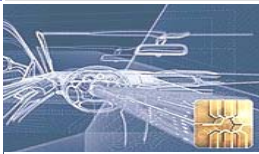


Properties of embedded systems

- Definition: „Device with processor“

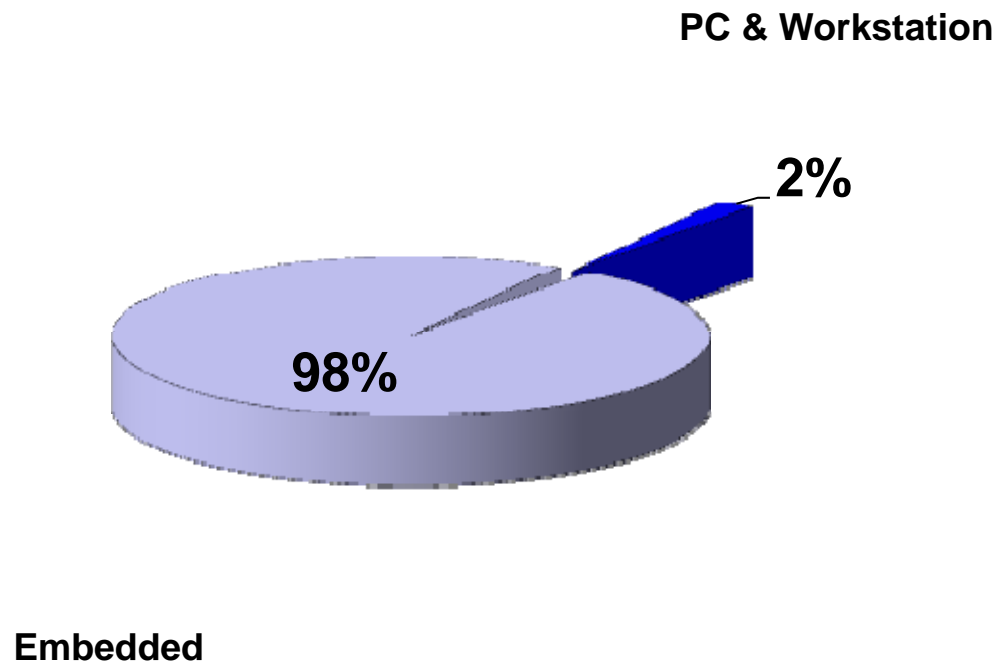


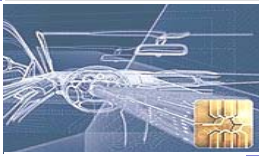
- Intended for a specific application
- Interaction with the outer world
- Optimized for a special purpose



Why is embedded important?

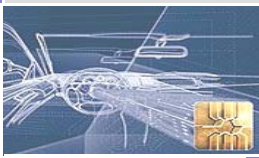
Market Share of 32-bit processors:





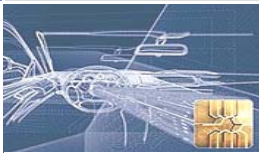
Outline

- What is an embedded system?
- Motivation for IT-security in embedded applications
- Challenges in the embedded domain
- Solutions for IT-security
- How much security do we need?

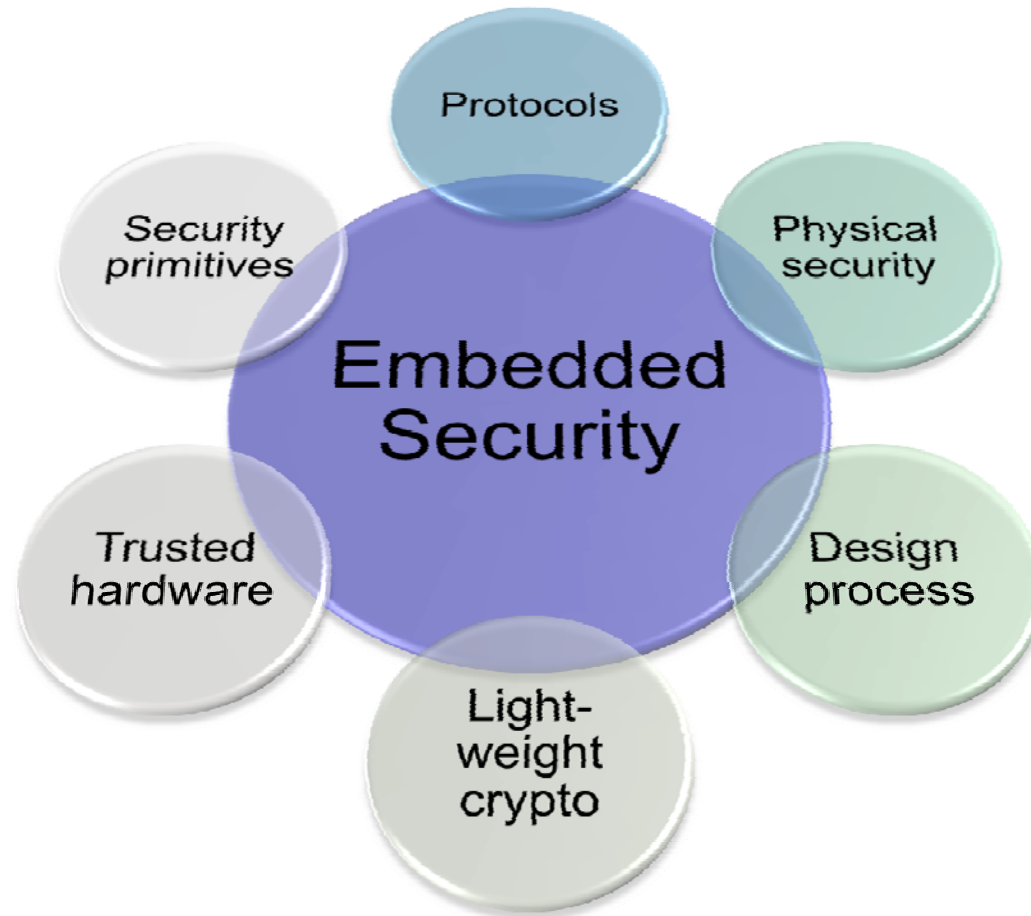


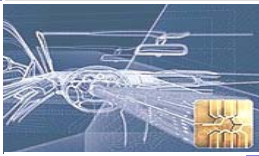
Security Concerns in Embedded Applications

- Pervasive nature and **safety-critical** applications increase risk potential:
Hard disk crash vs. car crash
- Often **wireless channels** \Rightarrow vulnerable
- **Content protection** in many applications: iPod, navigation systems, XBox,, ...
- **Secure SW download**: engine control, cell phones, washing machine,...
- **Component protection**: original spare parts, product privacy protection, ...
- **Privacy issues**: biometrics (face recognition), location, medical sensors, monitoring of home activities, etc.
- **Legislative requirements**: passports, road toll, data event recorders in machines, ...



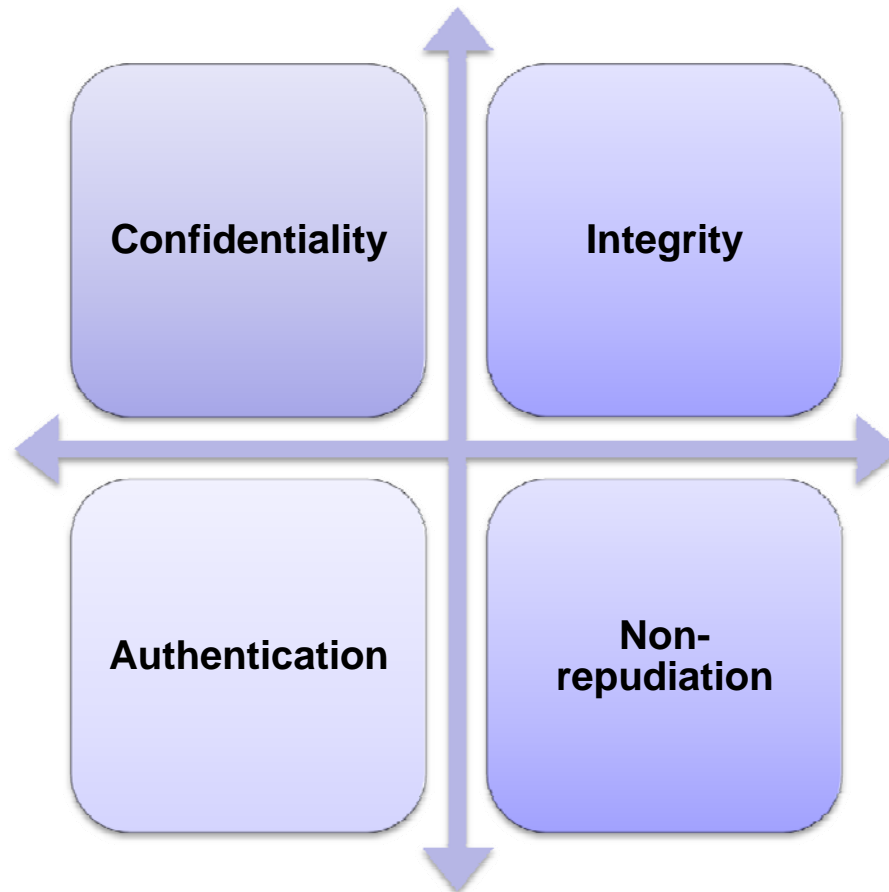
Embedded Security – *An Emerging Discipline*

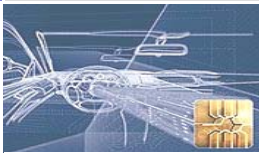




What IT security can do for you

- Important *security services*





Examples from automotive: applications with security needs



Embedded security

- SW updates
- Data event recorders
- Component identification
- X-by-Wire



Communication

- Car to car
- Car to infrastructure
- Internal communication
- Privacy



Legal & regulatory applications

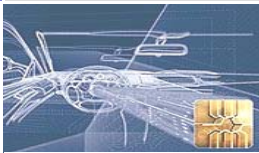
- Toll collection
- Speed monitoring
- Service



Rights Management

- Infotainment
- Embedded SW
- Music & video
- Location-based services





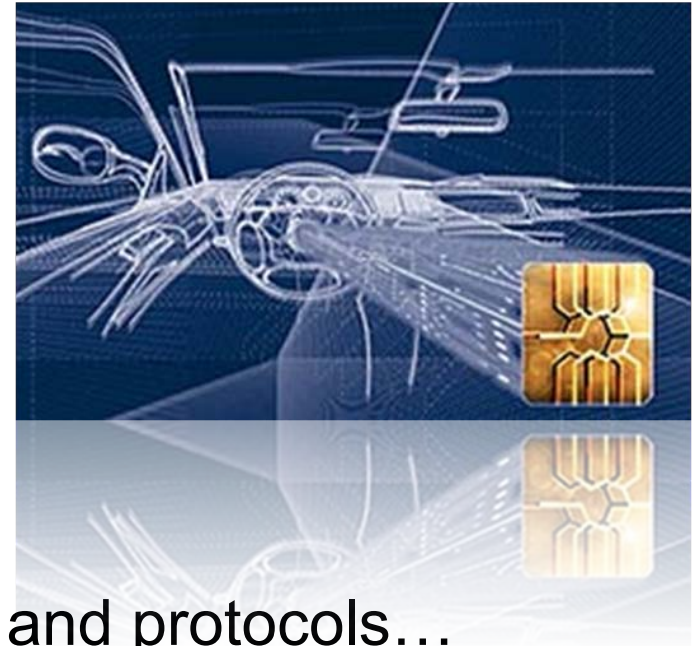
Outline

- What is an embedded system?
- Motivation for IT-security in embedded applications
- Challenges in the embedded domain
- Solutions for IT-security
- How much security do we need?



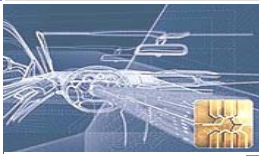
Why IT-Security is difficult

- Modern IT-Security offers:
 - communication security
 - security against manipulation
 - Digital Rights Management



⇒ based on cryptographic algorithms and protocols...

⇒ **all security problems can be solved (theoretically)**

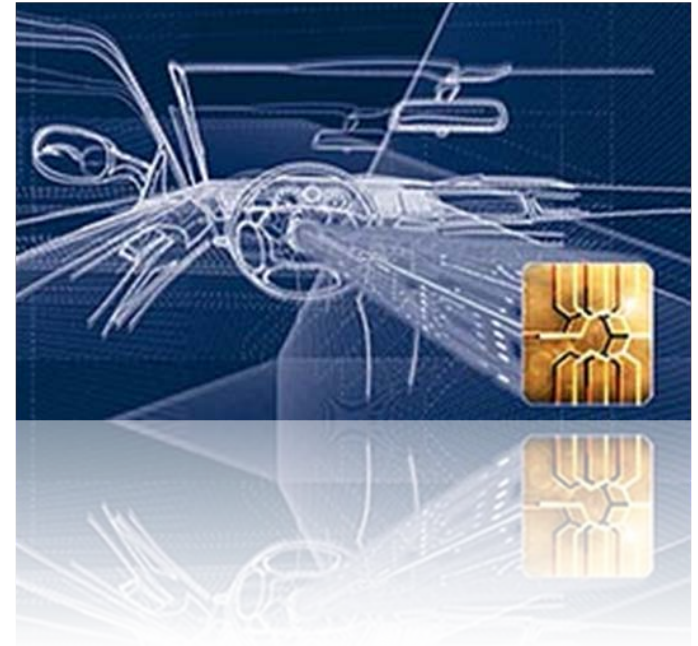


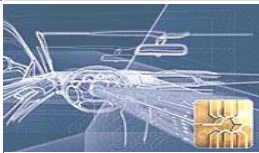
Why IT-Security is difficult

So what is the problem?

Mostly in the domain of
embedded security,

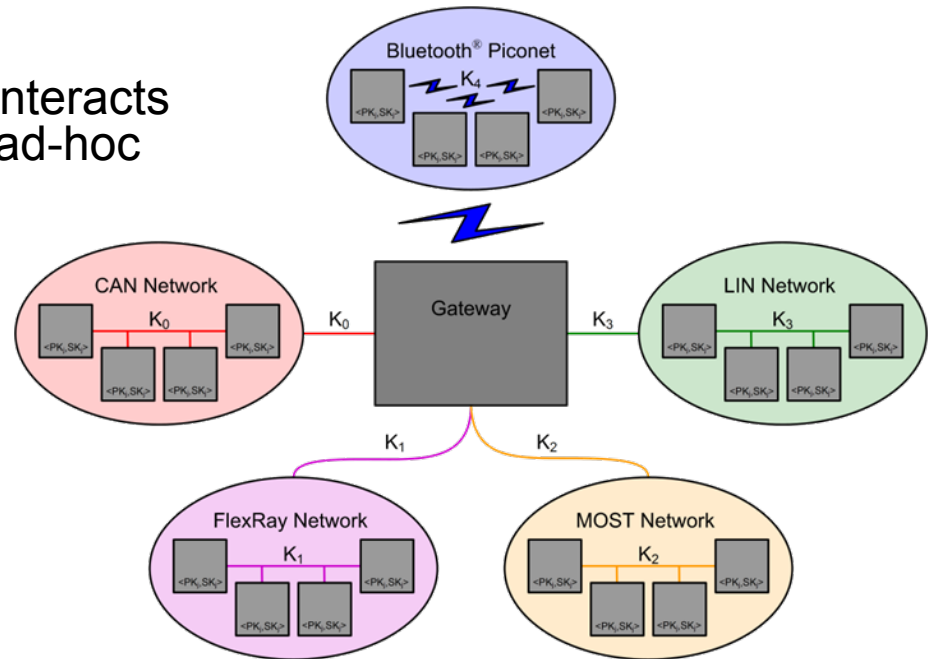
which is quite different from
conventional computer security
(Internet security, firewalls, ...)!



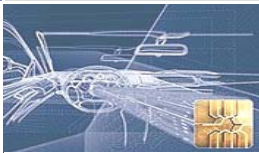


Why IT-Security is difficult

- **Constrained environments:**
8/16 bit μ P for computational intensive crypto algorithms (e.g., 1024-bit arithmetic etc.)
- **Complex networks**
External security (GSM etc.) interacts with internal communication, ad-hoc integration, ...

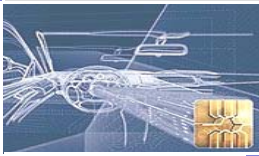


Example: Car network



Why IT-Security is difficult

- **System complexity/ life cycle management:**
Involvement of many layers
(Production, 1...x-th supplier, owner)
- **Attacker has physical access to the device:**
Side channel attacks, reverse engineering, eavesdropping...
- **Processes:**
Change in existing processes merely possible
- **Historical development:**
A system is designed to work properly,
IT-Security is secondary
- **Cultural problems:**
IT engineers have to work interdisciplinary: cryptographic algorithms,
protocols, physical security, ...



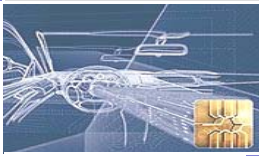
Why IT-Security is difficult

- IT-Security is unlike signal processing: The way of implementing might give raise to security problems

- Side channel leakage



- Efficiency and security sometimes counterproductive
- Security measures seem laborious
- Secure implementations require interdisciplinary knowledge (math, physics, EE, ...)
- Designer requires recent knowledge



Outline

- What is an embedded system?
- Motivation for IT-security in embedded applications
- Challenges in the embedded domain
- Solutions for IT-security
- How much security do we need?

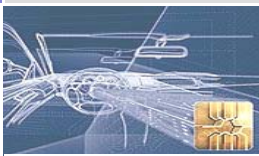


Systematic Approach

- Standard procedure for the analysis (e.g., CC)
- Consideration of all aspects of the entire system (embedded device, back-end, communication, network, key management, ...)

- Approach

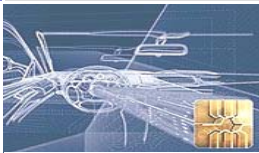




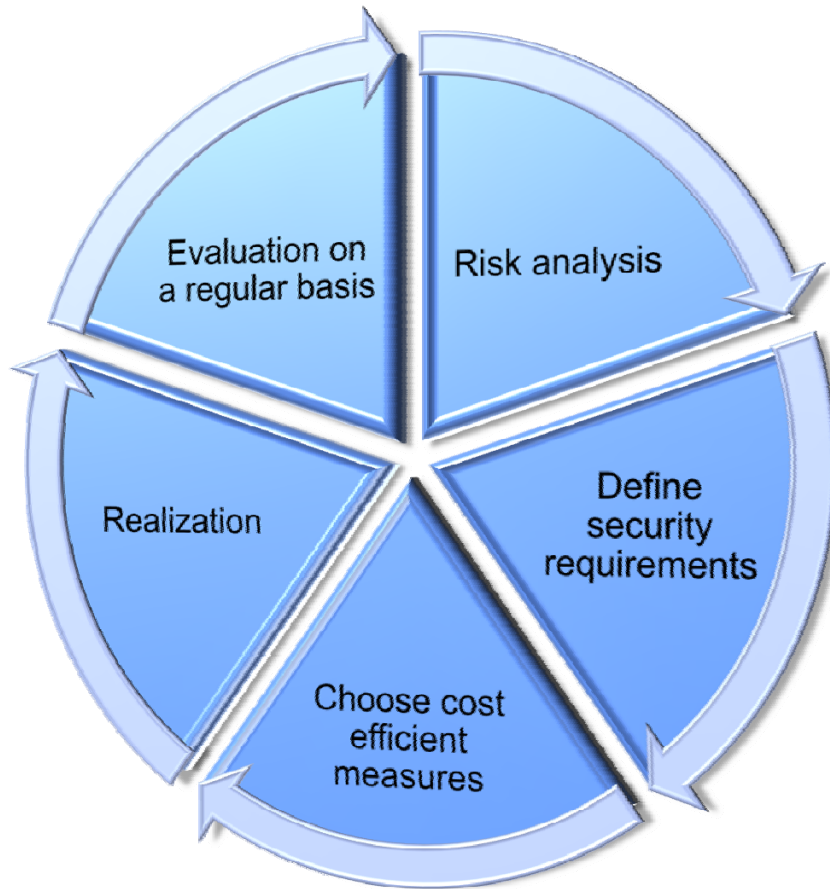
Security needs and security goals

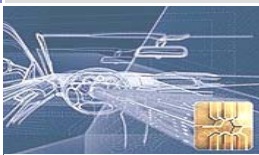
- Identification of use-cases
- Identify realistic weaknesses/ attacks
- Categorize and prioritize weaknesses/ attacks, e.g. according CC:
 - Required time for an attack
 - Expertise of the attacker
 - Required knowledge of the attacker
 - Window of opportunity
 - Required equipment of the attacker
- Development of corresponding solutions





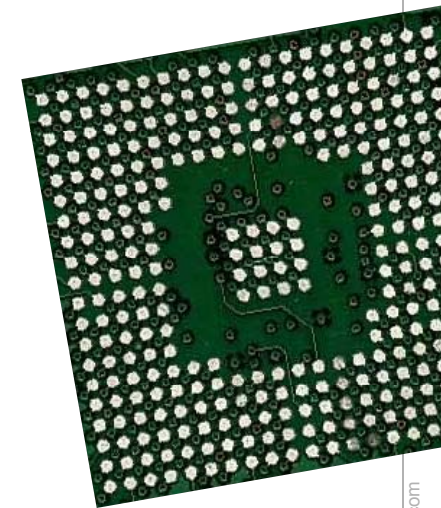
Best Practice

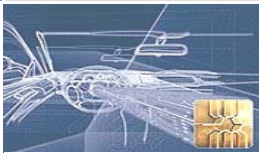




Categorization of methods

- Categories of measures to increase the security:
 - Algorithms in software and hardware
 - Cryptographic primitives and protocols (confidentiality, authenticity, integrity, non-repudiation, ...)
 - resistance against side channel leakage
 - further methods such as “obfuscation”, ...
 - Hardware security
 - Algorithms in hardware
 - Countermeasures against side channel attacks
 - “Tamper-Evidence”
 - “Tamper-Resistance”
 - “Tamper-Responsiveness”
 - Secure casing
 - Secure PCB layout
 - Secure IC design
 - Deactivation of interfaces (e.g., serial, network, USB, JTAG, ...)
 - ...

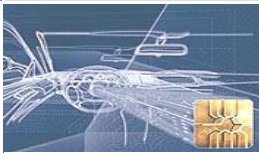




Categorization of methods

- Organization
 - Processes (e.g., key generation, -transport, -injection)
 - Secure environment
 - Security policies

- Ensure trustworthy system
 - “Trusted Computing”
 - Secure boot/ authenticated boot
 - Secure software update



■ Crypto - Toolbox:



Symmetric cryptography

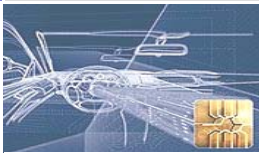
- Block ciphers: AES, 3DES, DES, Blowfish, Mars, ...
- Stream ciphers: RC4, A5/2, SEAL, (eSTREAM-competition) ...
- Hash functions: SHA1, SHA2-family, RIPEMD-family, SHA3, ...
- MACs (from Blockciphers, HMAC)

Asymmetric cryptography

- RSA, DH, ElGamal, DSA, ECDSA, ECC, HECC, ...

Standard protocols

- e.g., PKCS, ISO, IEEE, HIS, ...



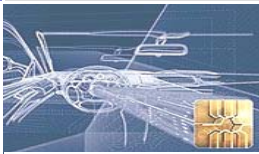
Suitability of symmetric and asymmetric algorithms:

In theory:

- Symmetric: Ensure confidentiality, integrity, authenticity
- Asymmetric: additionally non-repudiation

In practice:

- Symmetric: Very efficient in space and runtime
 - Stream ciphers slightly better than block ciphers
but security not known as good
- Asymmetric: Time and space consuming
 - Uses long number arithmetic
 - Requires implementational know-how



Outline

- What is an embedded system?
- Motivation for IT-security in embedded applications
- Challenges in the embedded domain
- Solutions for IT-security
- How much security do we need?



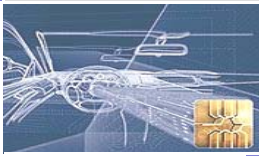
How many key bits do I need?

Recommended key lengths by institutions such as NIST, BSI, etc.:

<i>symmetric</i>	<i>ECC</i>	<i>RSA, DL</i>	<i>comment</i>
64 bit	128 bit	≈ 700 bit	short-term security (< 10 years) (can be broken with some effort)
80 bit	160 bit	≈ 1200 bit	mid-term security (10-20 years) (except 'big agencies')
128 bit	256 bit	≈ 3072 ... 4096 bit	long-term security (except quantum computers)

Key size mainly determined by

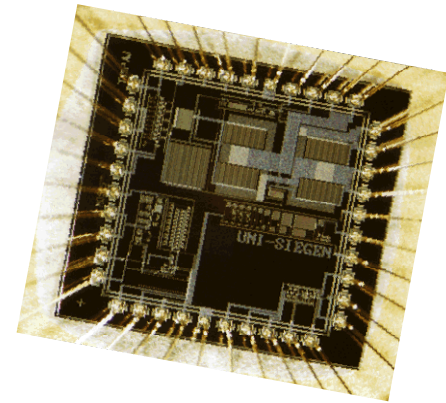
- life-cycle of an application
- security requirements of application

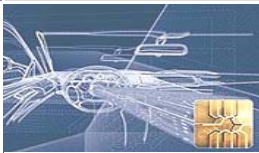


Hardware vs. software security

- Why security in hardware?
 - Isn't cryptography, protocols and secure system design sufficient?

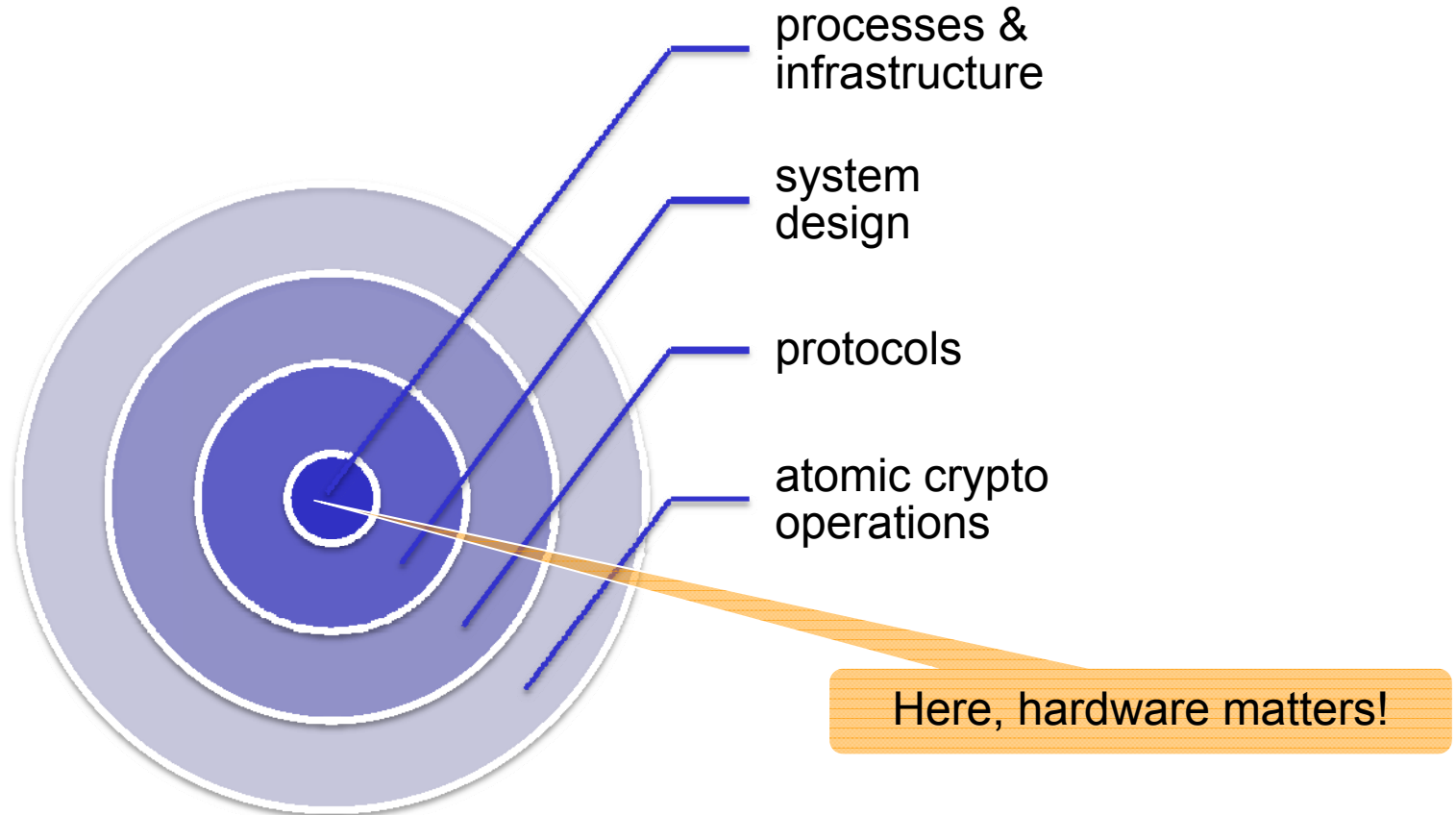
- Main reasons for secure hardware:
 1. **Performance:** HW much faster than SW
 2. **Security:** Manipulation in HW much harder
 3. **Costs:** HW cheap at large quantities

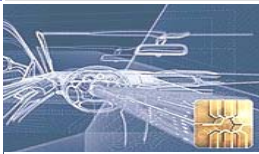




Hardware- vs. software-security

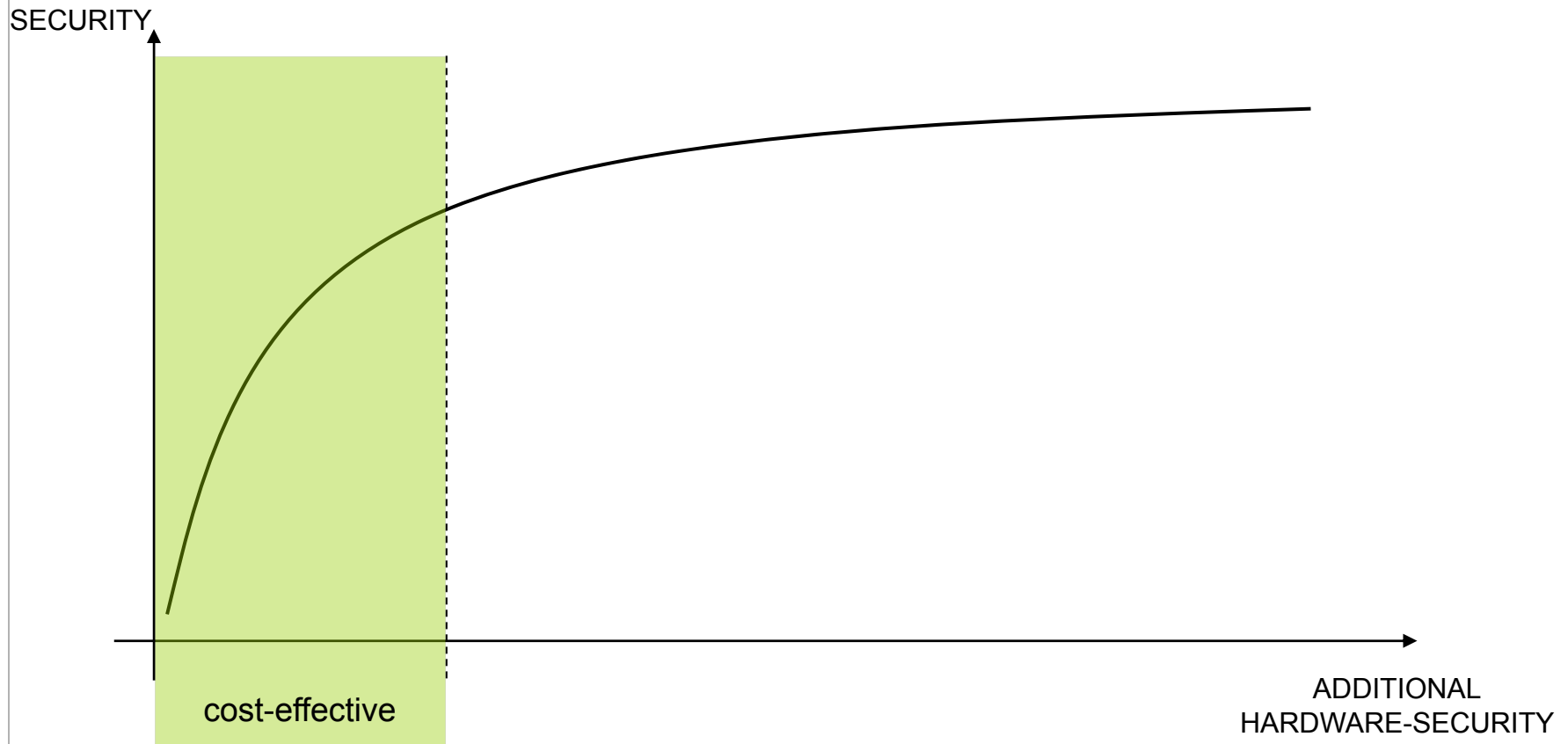
How do we achieve security in applications
(e.g., secure flashing, immobilizer, trusted platform, ...)?

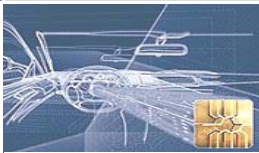




How much security hardware do we need?

Security vs. utilization of security hardware





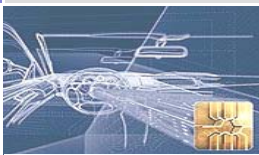
Practical approach



“Economic security”:
approach to allow for a cost-
effective security enhancement

- Identify level of protection
- Define adequate level of security
- Derive meaningful countermeasures against weaknesses
- Focus on cost-efficient realization
- Build upon existing processes

▶ optimal security level at low costs



Conclusions: Embedded Security

- **IT-Security will be of central interest in future applications**
E.g., telecommunication, telematic, ad-hoc networks, flahsing, infotainment, ...
 - **IT-Security demands for careful design**
Several examples from practice show how badly design solution have been broken.
 - **„Embedded security“ has very specific requirements**
Constrained environments, side channel leakage, ...
 - **New business models possible**
Pay-per-view, feature activation, new services, ...
 - **Merging of the classical IT community and the security community**
Many chances but (currently) cultural differences
- ⇒ **Embedded security is enabling technology for future applications!**



Upcoming Embedded Security Events

escar 2009 - Embedded Security in Cars
Düsseldorf, Germany, 24/25. November 2009



CHES 2010- Cryptographic Hardware and Embedded Systems
Santa Barbara, California, USA

ECC 2010 - Elliptic Curve Cryptography

esgeo 2010 (Embedded Security in Geoinformationssystemen)

ES

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

Embedded Security

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