Embedded Security for Connected Systems

MODERATOR:

Michael Hange
Federal Office for Informa-
tion Security (BSI)

PANELISTS:

Martin Klimke
Infineon

Andrew Krehmeyer
Continental

Marc Lindlbauer
secunet

Agenda

Emerging Approach: Embedded Security

C S 1: Security for Smart Grids

C S 2: Hardening Automotive Infotainment Platforms

Q & A

Introduction

IT Security Strategy in Germany
- Critical Infrastructures
- The role of embedded security

Federal Office
for Information Security

Smart Grid

Motivation for the smart grid

Climate change by the greenhouse effect and the dwindling fossil energy resources demand
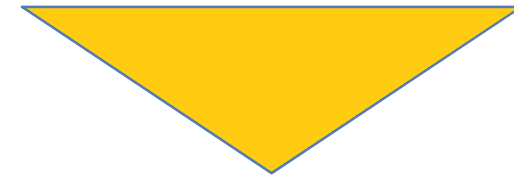
1. Energy reduction by increased efficiency and better end customer awareness.
2. Efficient use of decentrally generated green energy.

➤ Key Technology to achieve these goals is the **"Smart Grid"**.
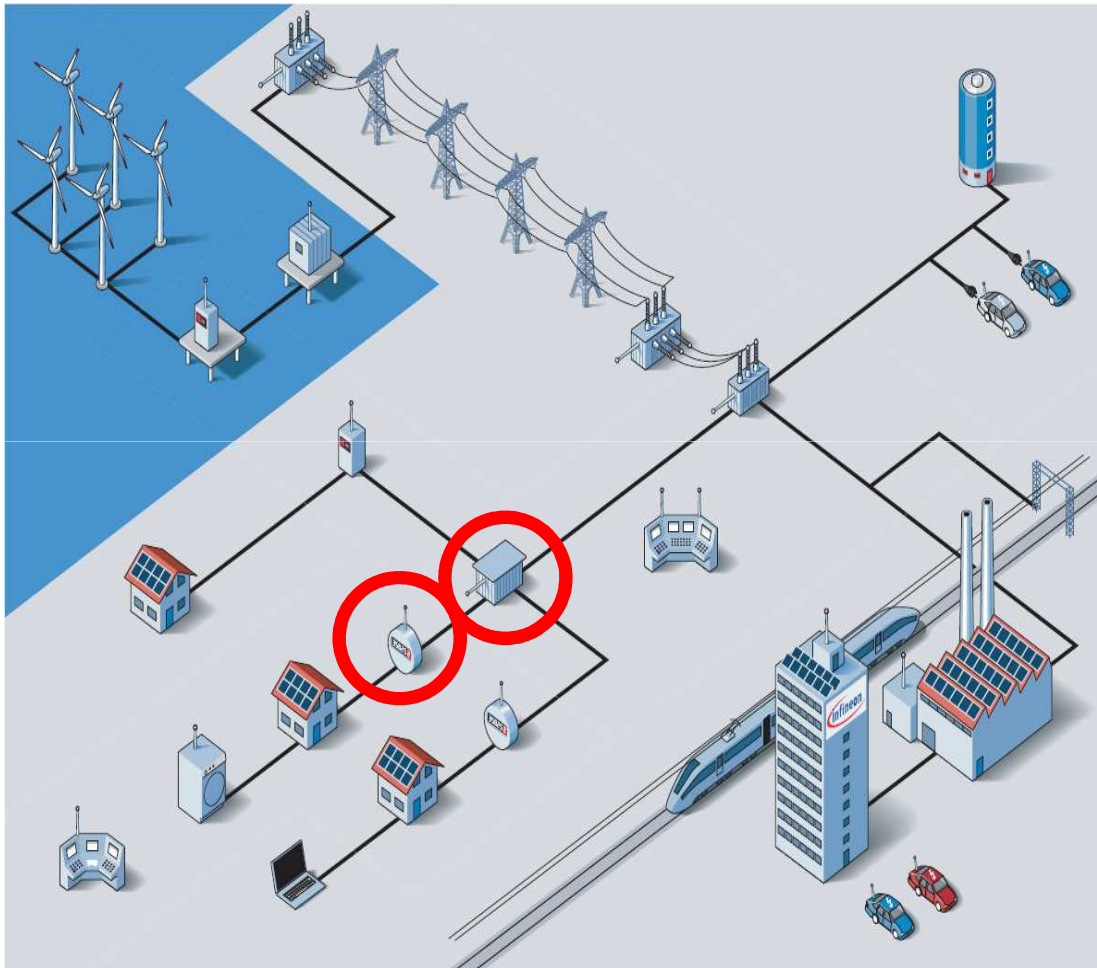
Smart Grid need for security
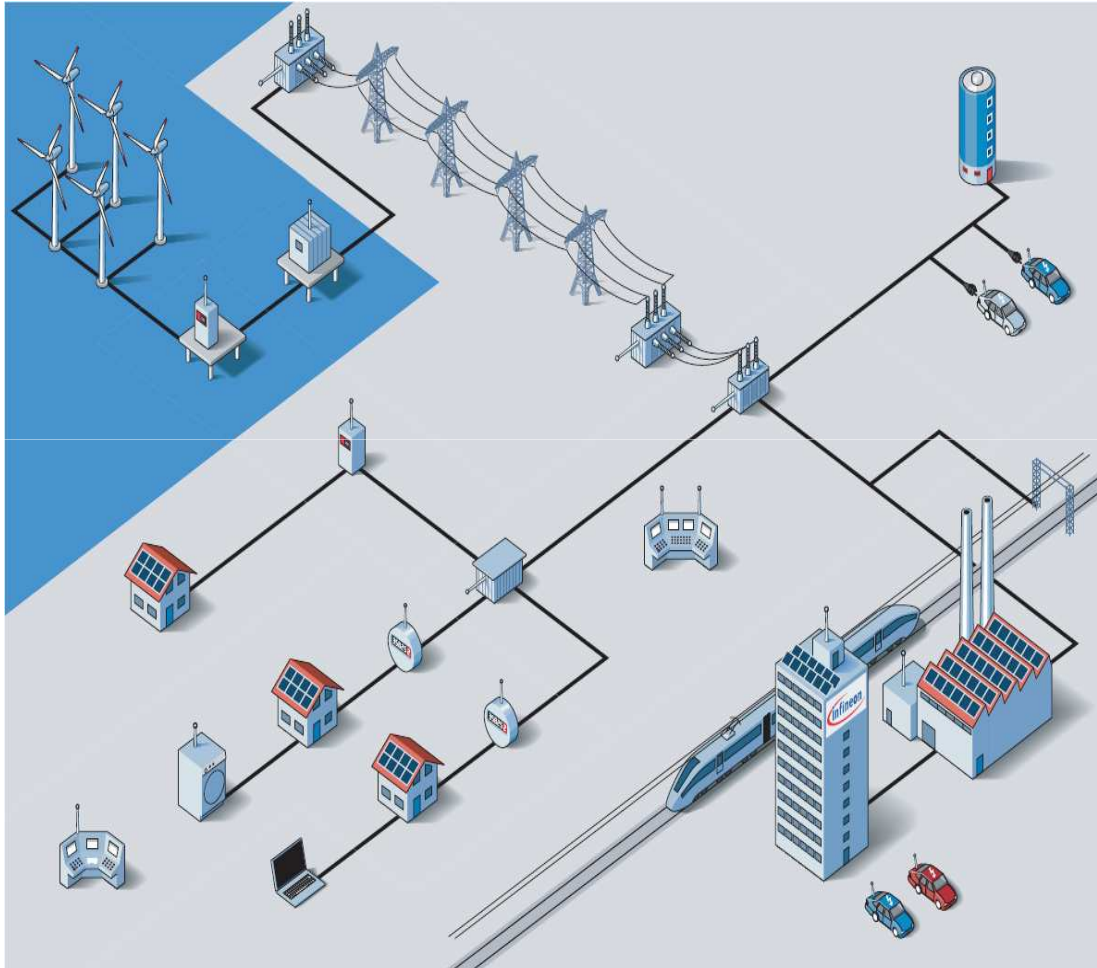
The Smart Grid is critical Infrastructure that assures vital functions of the society

It requires protection against
-Privacy breaches
-Fraud and
-Cyber terrorism

Focus on Smart Meters and Concentrators

- Concentrators and Smart meters are
  - physical unprotected and
  - easily accessible.
- require tamperproof security and
- should be security certified

Security Controllers provide protection in these devices by

- a tamper proof execution environment
- tamper proof data storage
- secure manufacturing processes
- and security certifications

Summary

1 The smart grid is a critical infrastructure that is needs protection

2 Security must be built in from day one

3 Certified Security Controller provide a solid foundation for smart meter security

4 Governments must act now and mandate security certifications

Transformation of Consumer Electronics in the Connected Vehicle

Always On Connections Inside the Car

Consumer Expectations

- Individual & Personalized Solutions
- Easy to Use
- Always On
- Open Platforms
- Download of Functions
- Update Possibilities

Continental

Designing Safe & Easy to Use Human Machine Interfaces

We Design Systems To Simplify Your Drive

Change the profile of
your car at the touch
of a button:

🟢   Eco

🔴   Sport

🔵   Comfort
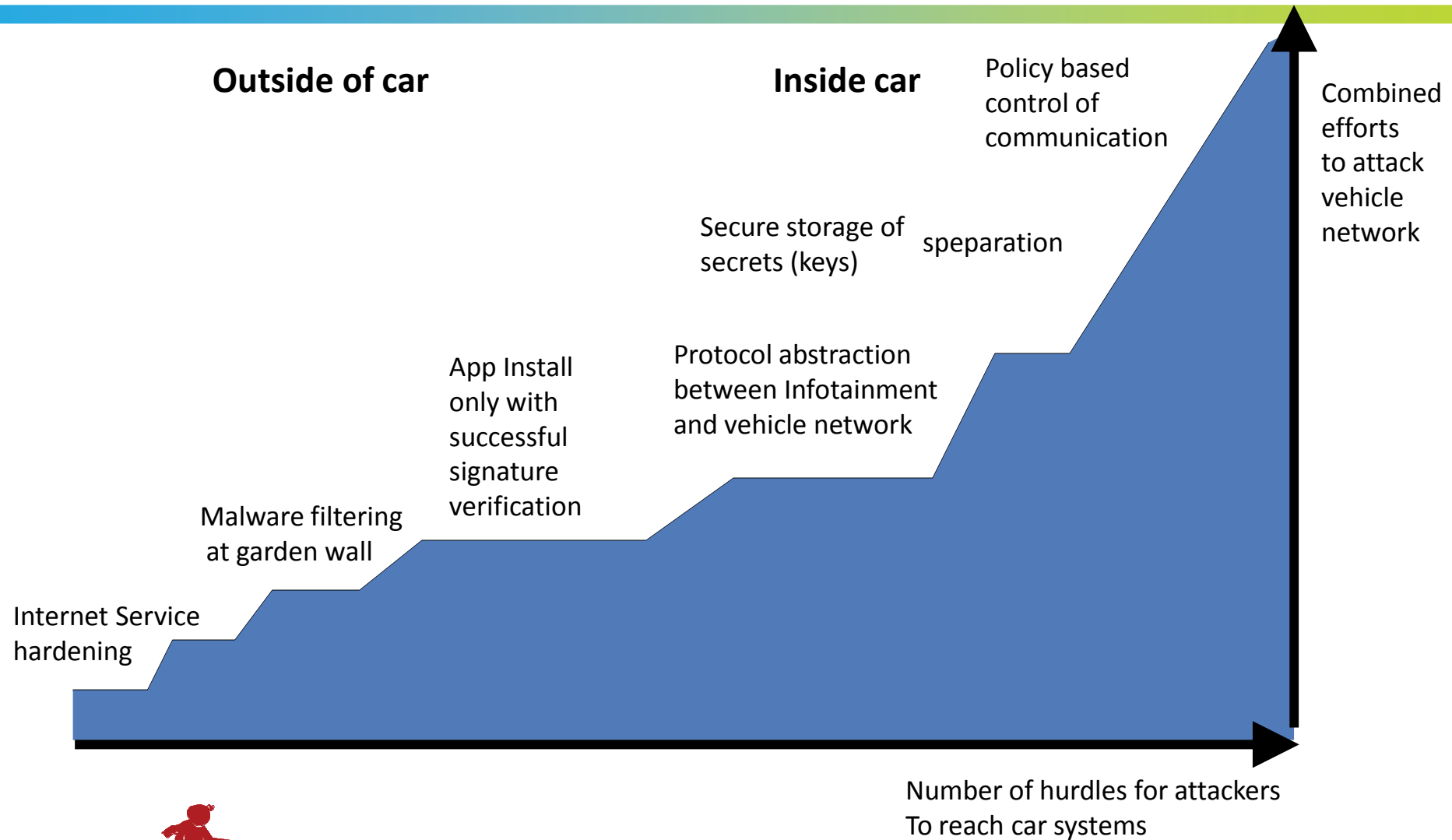
Other profiles are
also Possible.

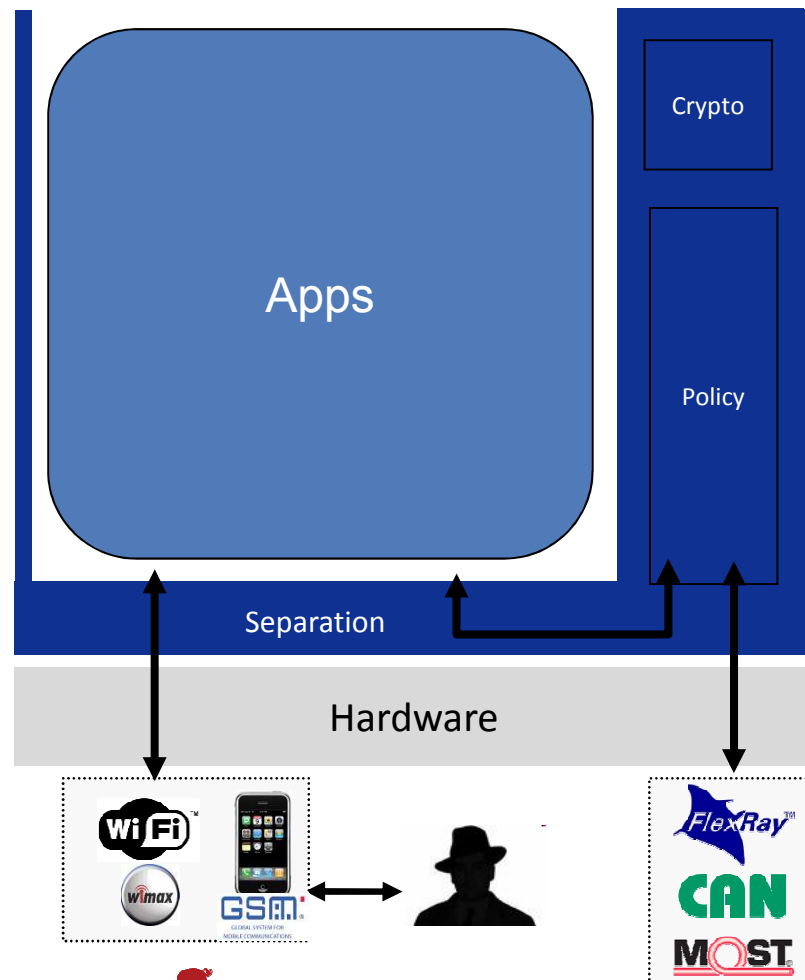# Security Architecture for Infotainment Systems in Cars

Defense in Depth – Selected Features

Outside of car

Inside car

Policy based control of communication

Combined efforts to attack vehicle network

Secure storage of secrets (keys)

speparation

App Install only with successful signature verification

Protocol abstraction between Infotainment and vehicle network

Malware filtering at garden wall

Internet Service hardening

Number of hurdles for attackers
To reach car systems

Security Architecture

Apps

Crypto

Policy

Separation

Hardware

Separtion provides runtime environment for App containment

Policy forwards information after compliance is confirmed

Active corrective Measures If policy violation is detected

Corrective measures independent from Infotainment system

Crypto authenticates Apps and services

Secunet ACU – Application Control Unit

How to roll out such a Security Architecture

Rollout of Connected Vehicles

- Auto connectivity forces the creation of a new generation of apps

- Safety is always the top priority

- Vehicles systems must be highly reliable

- Infotainment functions must be segregated from core vehicle systems

- Qualify information that has to travel from infotainment to vehicle systems

- Setup policy to control this information flow, which is independent from apps
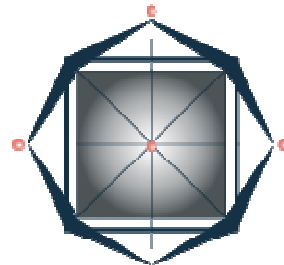
RSA 2011
CONFERENCE

Visit the German pavilion:
Booths 1344 & 1350

Thank You!

RSACONFERENCE2011