RUHR-UNIVERSITÄT BOCHUM

RUB

Applied Automotive Security

Secure Integration of Mobile Devices for novel Automotive Services

Roman Kochanek
Student of IT-Security

December 21, 2011

POLITECNICO MILANO

hgi
Horst-Görtz Institut
für IT Sicherheit

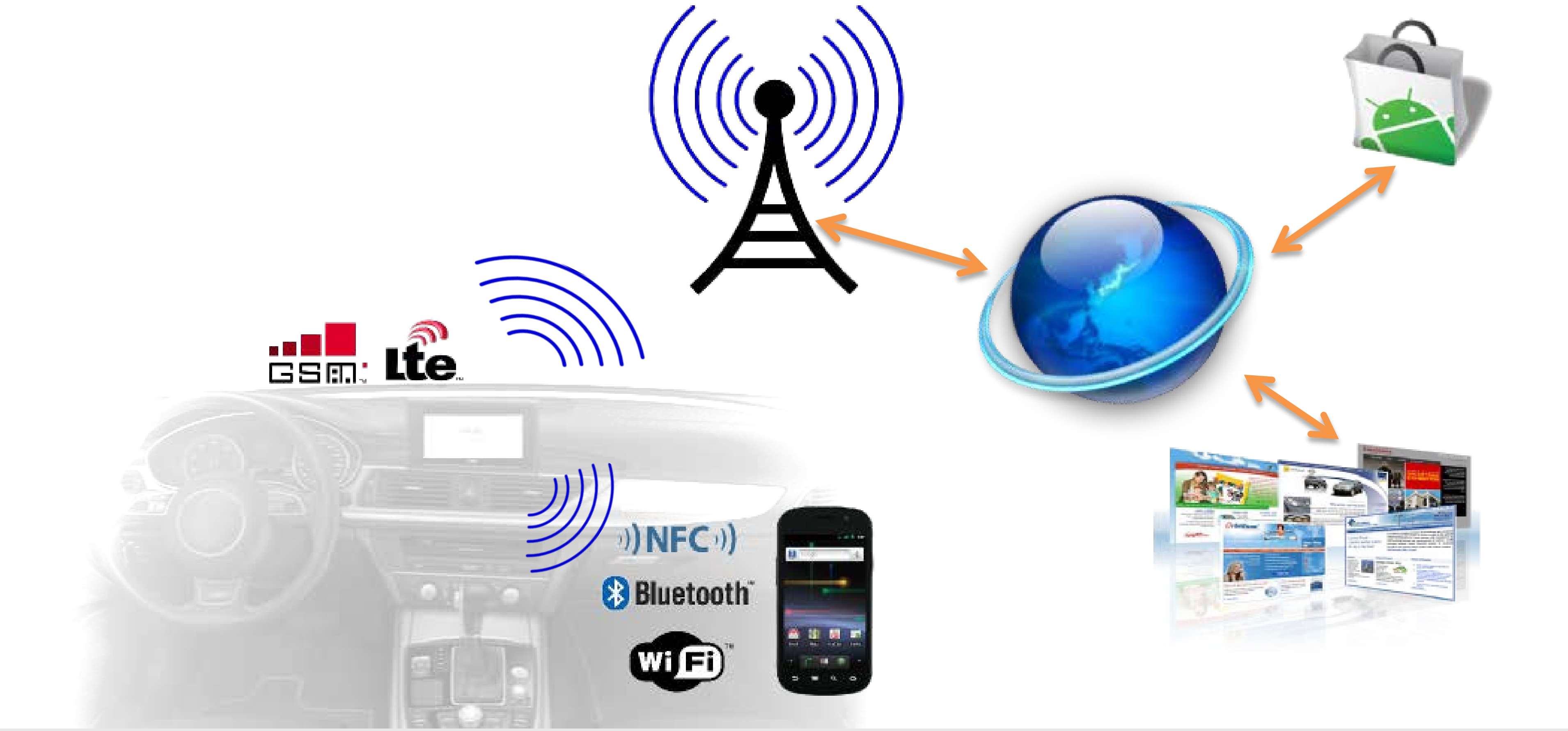
syssec

move

Overview

- Introduction
- Use Case
- Security by Design
- Conclusion

Introduction
The Brave New World

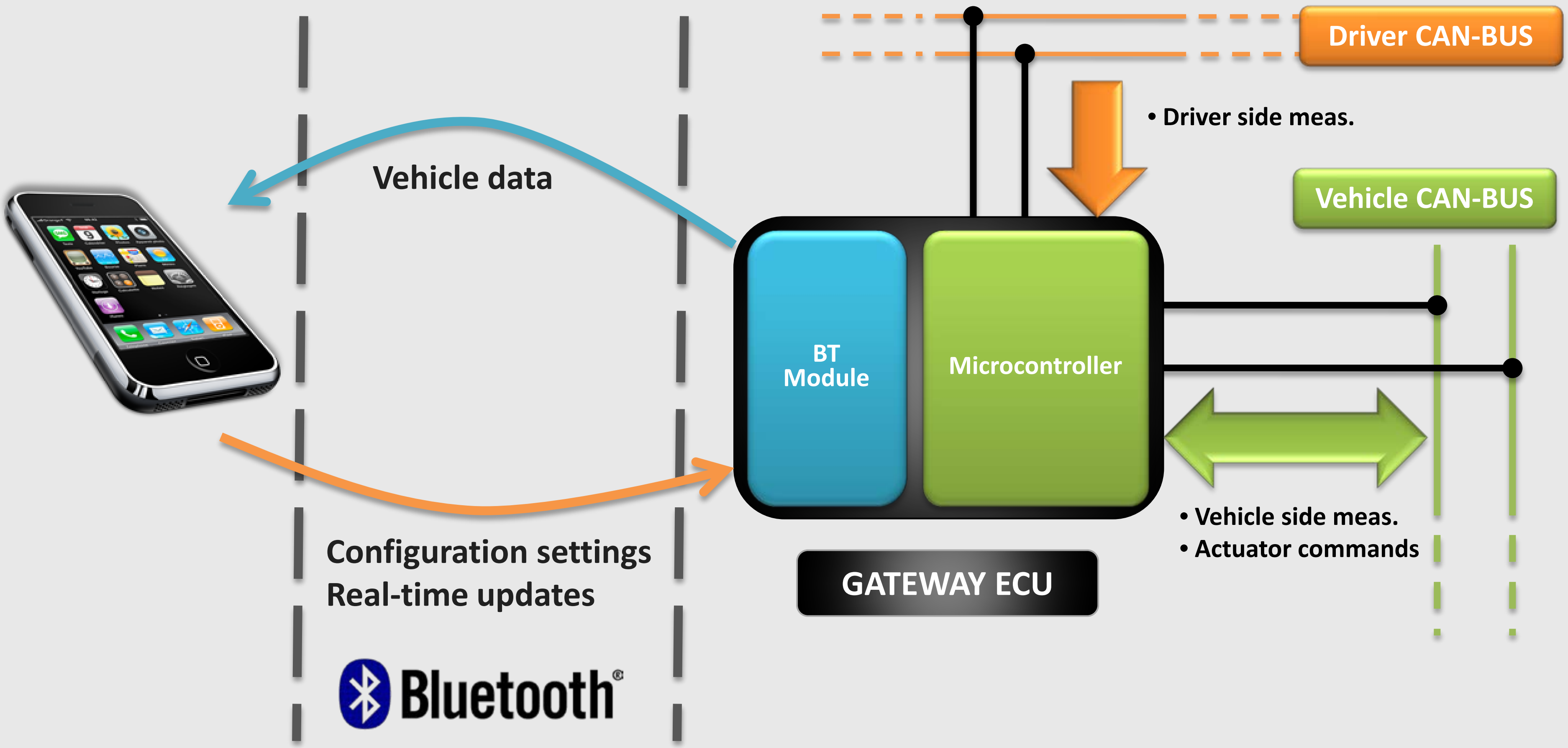


Introduction
From a Security Point of View

- Malware on mobile devices
  - Botnets, Trojans, or premium services
  - Android is called the new Window XP
- Industrial Control Systems under dedicated attacks
  - Stuxnet and Duqu
- A number of CAs (Certificate Authority) become compromised
  - DigiNotar and GlobalSign
- Privacy issues
  - Tracking users
  - Analyzing behaviour and creating forecasts

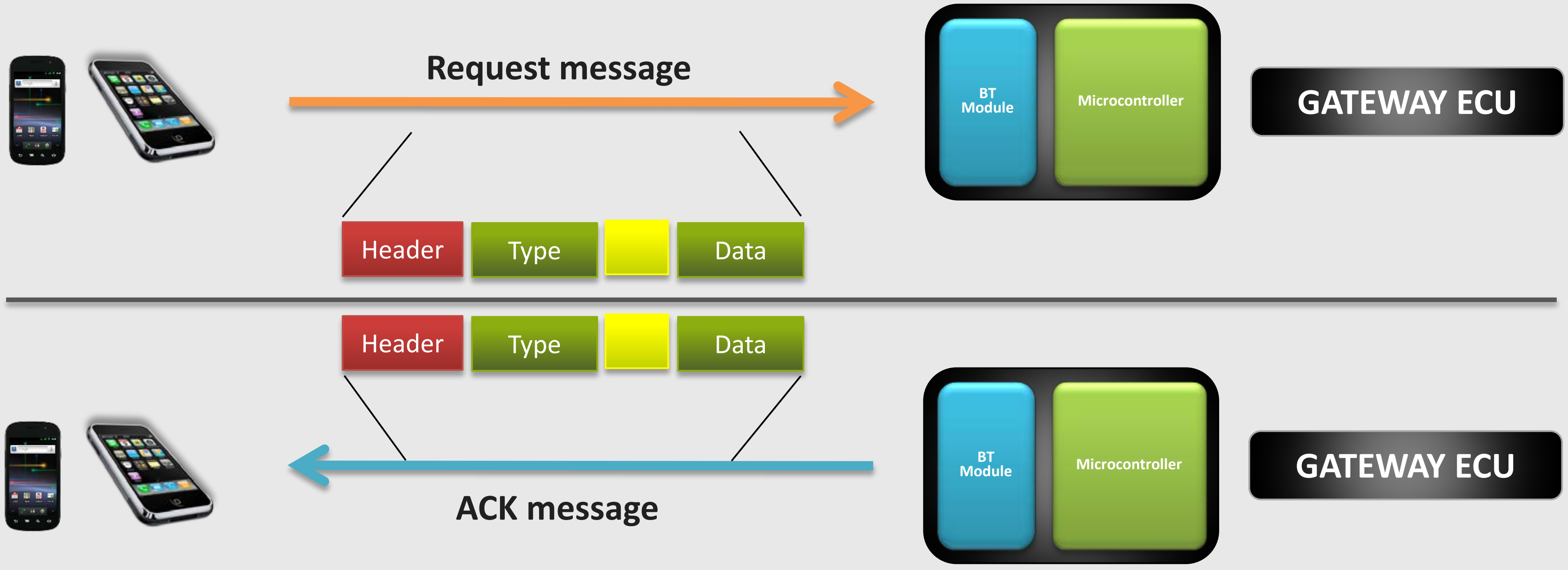
Use Case

Automatic management of autonomy for electric vehicles



Use Case

Communication Protocol

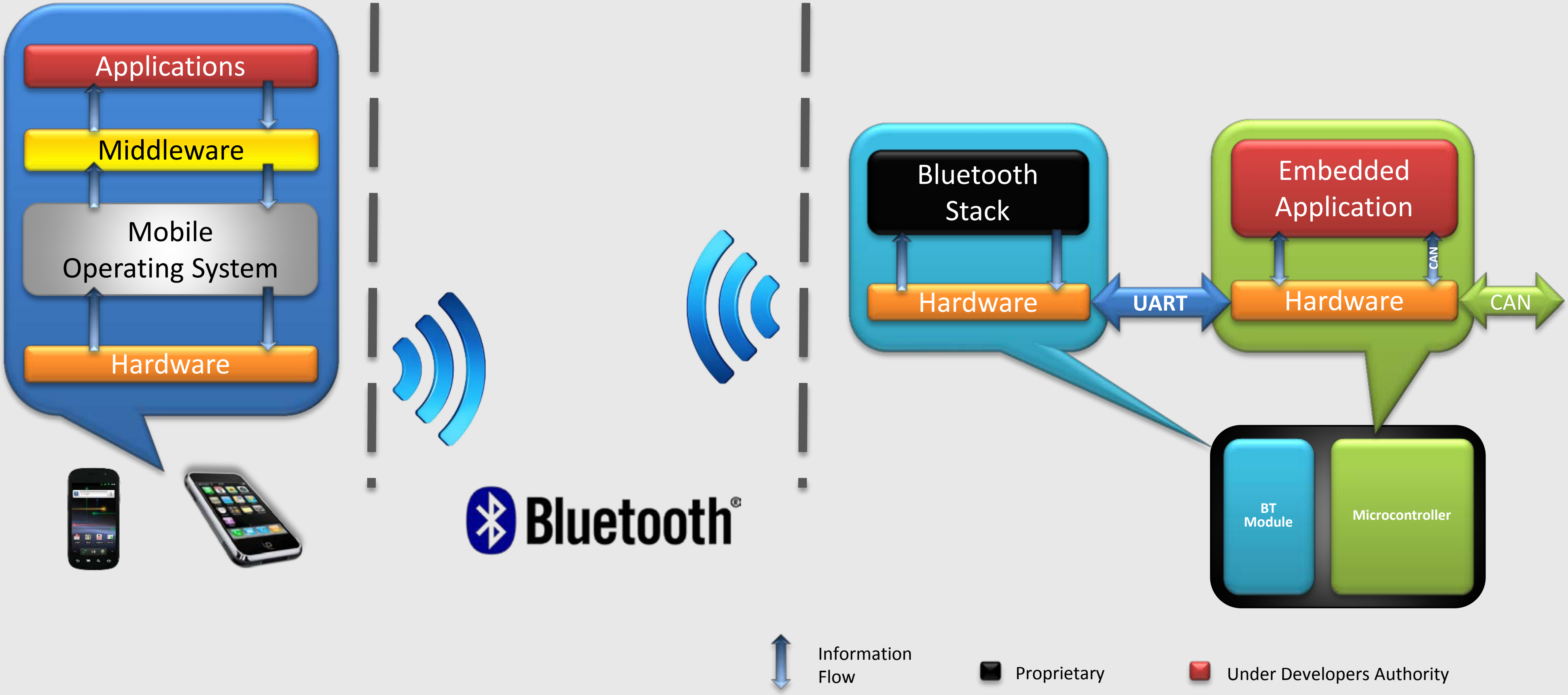


- ACK mechanism **only** during initialization phase
- **Bi-directional** communication w/o ACK mechanism, i.e., Gateway ECU or Smartphone just sending messages

🟥 Packet Delimiter 🟨 Data Delimiter 🟩 Data

Use Case

Information Flow



Use Case

Security Goals

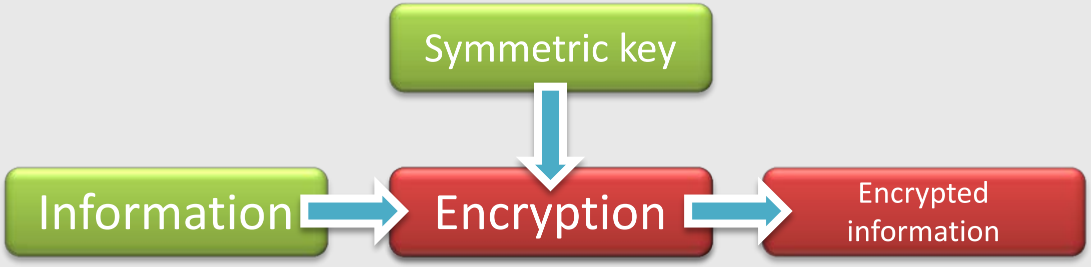
- Information Security: “preservation of **confidentiality**, **integrity** and **availability** of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved” in [ISO/IEC 27001:2005]
- **Confidentiality**: Ensuring that information is accessible only to those authorized to have access.
- **Integrity**: Safeguarding the accuracy and completeness of information and process methods.
- **Availability**: Ensuring that authorized users have access to information and associated assets when required.
- **Authentication** [NIST 800-27 Rev-A] : Authentication refers to the verification of the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
- **Authorization** [ISO 7498-2] : Authorization is the granting of rights, which includes the granting of access based on access rights.

Use Case

Security Toolbox

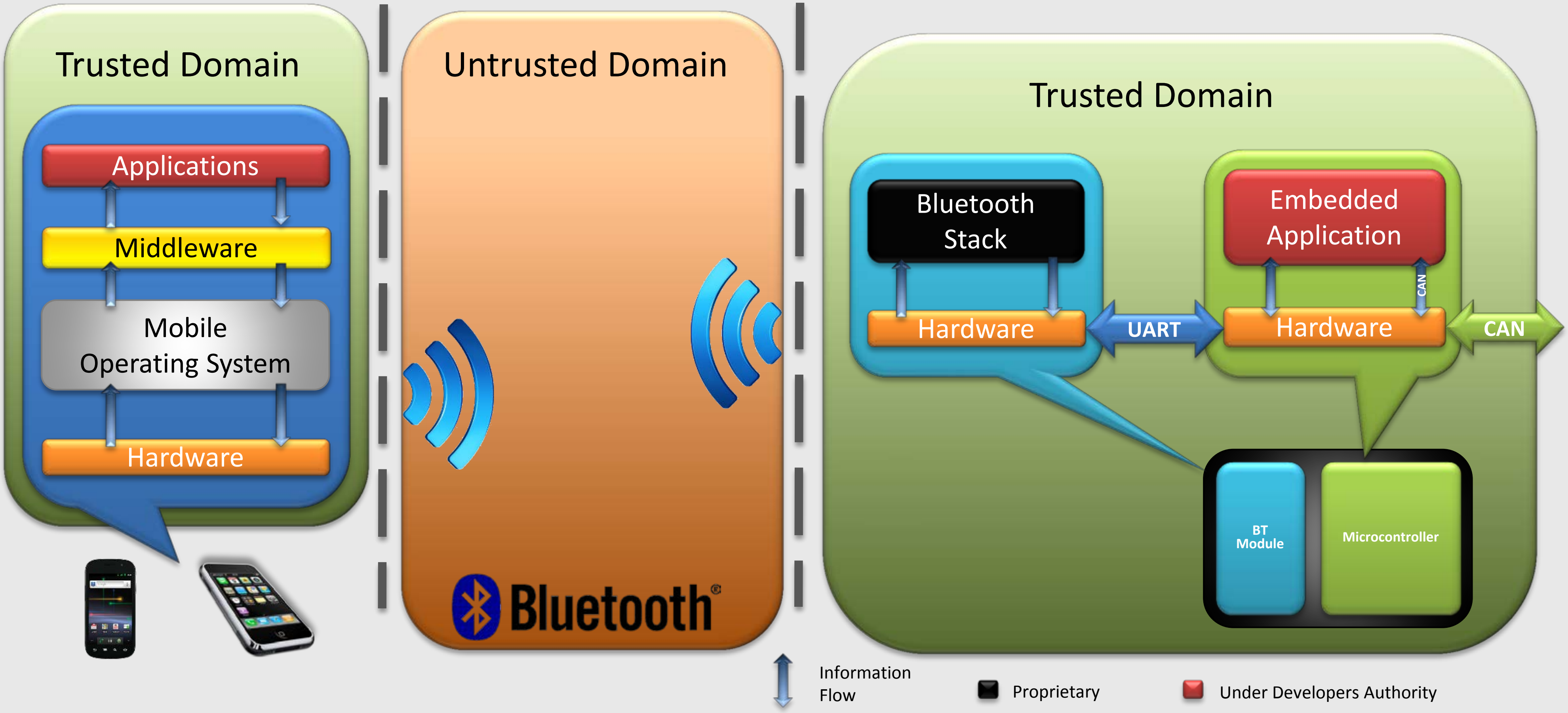
- Cryptographic primitives
  - Symmetric/Asymmetric cryptography
  - Hash functions
  - Digital signatures
- Cryptographic protocols
  - Key-Agreement
  - Key-Transport
  - Authentication
- Based on mathematical problems, e.g., factorization of huge numbers or the discrete logarithm problem

Example: Symmetric cryptography



Use Case

Information Flow



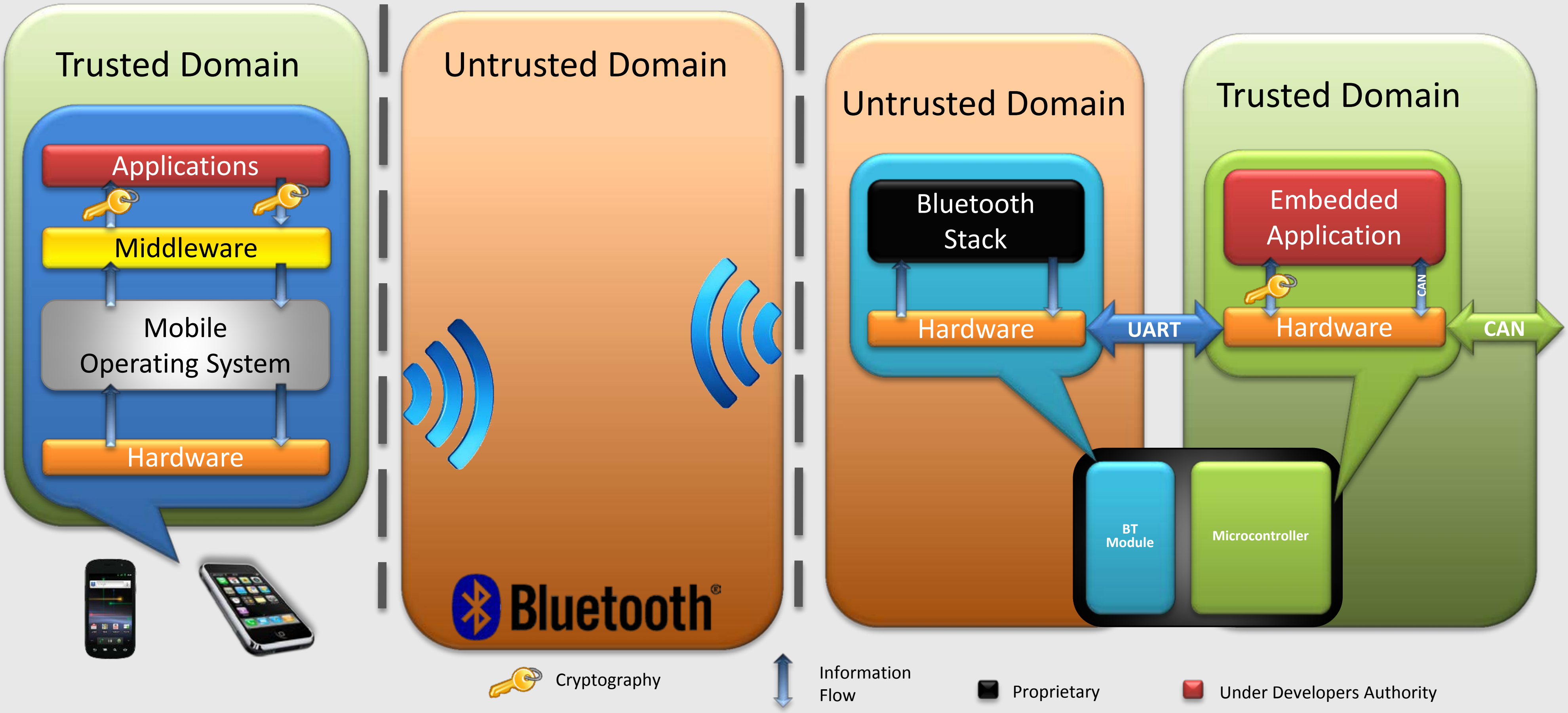
Use Case

Bluetooth Security – Current State

- **Static PIN**
  - **No mutual authentication** due to the input capabilities of the Gateway ECU
  - **No authorization** of a certain device possible
  - **Confidentiality** and **integrity** is based on a four-digit number
- **Proprietary** Bluetooth Stack Implementation
  - Unknown implementation flaws could compromise the information security
- **No extended security** standards (**Secure Simple Pairing** defined in Bluetooth v2.1) in the **current module** (Bluetooth v2.0) **available**
- **Theoretical/practical attacks**
  - Every Bluetooth-capable device can transmit arbitrary data towards the Gateway ECU
  - Execution of arbitrary code on the MCU possible due to potential implementation flaws
  - Bluetooth Security has been fully compromised, even sub-parts of the extended version

Security by Design

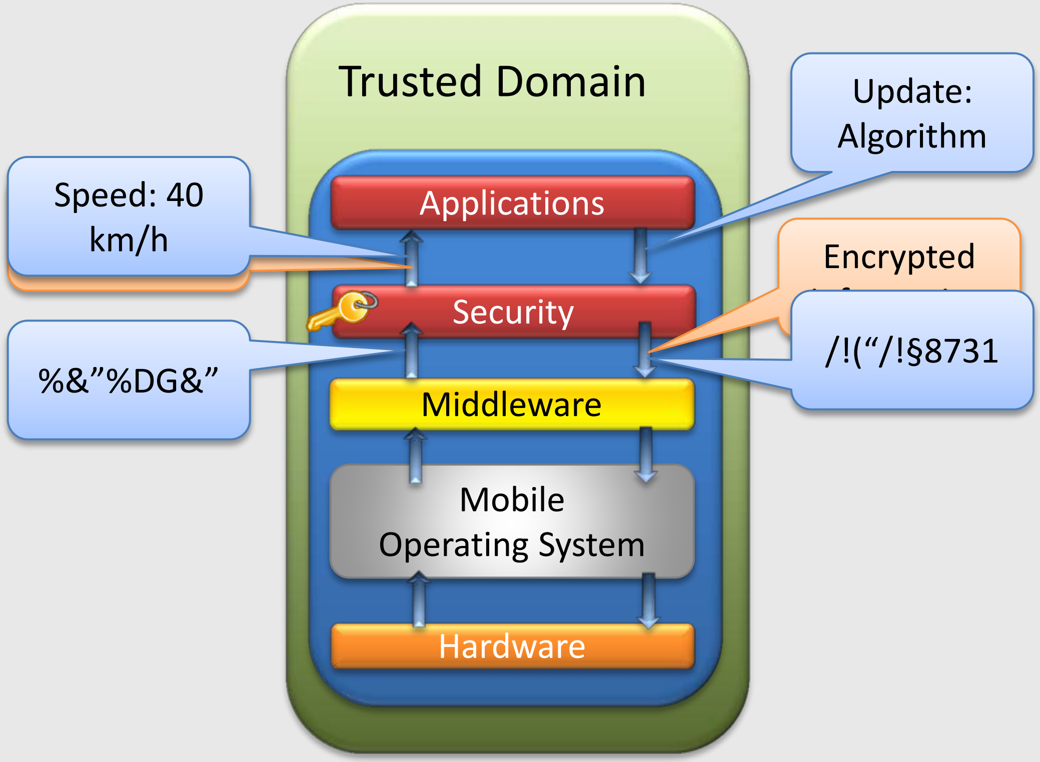
Security Concept



Security by Design

Software Architecture

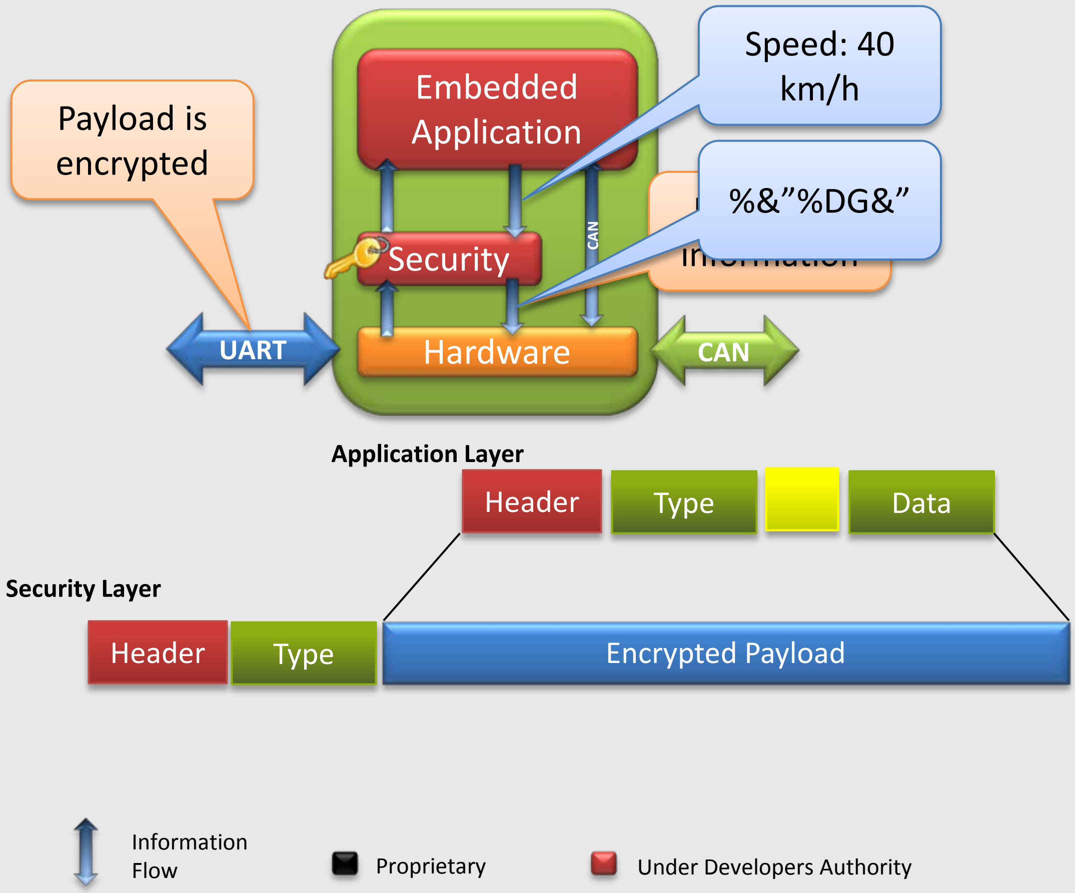
- Introduction of a **security layer** on both devices
- Deployment of **standardized cryptographic mechanisms**
- Benefits
  - **Decoupling** of **execution** based on its **context**
  - Security is applied in a **transparently** way
  - Providing **real** end-to-end security and trustworthiness between both application layers
  - **No** trusted relationships to proprietary devices, services, or software are needed
  - **Security** is under the **developers authority**



🔑 Cryptography ↕ Information Flow ■ Proprietary 🟥 Under Developers Authority

Security by Design
Software Architecture

- Introduction of a **security layer** on both devices
- Deployment of **standardized cryptographic mechanisms**
- Benefits
  - **Decoupling** of **execution** based on its **context**
  - Security is applied in a **transparently** way
  - Providing **real** end-to-end security and trustworthiness between both application layers
  - **No** trusted relationships to proprietary devices, services, or software are needed
  - **Security** is under the **developers authority**



Security by Design
Use case

- **Mobile Device Authorization** – Asymmetric Cryptography
  - Diffie-Hellman Key Exchange over Elliptic Curves (ECDH)
  - Standardized protocol according to NIST 800-56A
  - Both devices share each other's public key
- **Session Encryption** – Symmetric Cryptography
  - Both entities compute the same fresh key by a hash function
  - Inputs of the hash functions
    - IDs of the entities, shared secret based on ECDH, nonce
  - Output of the hash function
    - Symmetric key for the Advanced Encryption Standard (AES)

Security by Design

Cryptographic mechanisms

- Symmetric cryptography
  - AES-128 in Cipher Block Chaining Mode
- Asymmetric cryptography
  - Elliptic Curve on standardized curve, i.e., NIST P192
- Hash function
  - SHA-1
- Cryptographic protocol
  - Diffie-Hellman key exchange
- Implemented in **Assembly**, **C**, and **Objective-C** code
- Integration in a **real-world** application on **different** platforms

Conclusion

Results

- Introduced the approach of **context-based execution**
  - Deployment of **standardized cryptographic mechanisms** on Smartphone/Gateway ECU are feasible
  - Mitigation of security threats
  - **Authorization** of a **certain mobile device**
- Pending work
  - Evaluate further security concepts against
    - Side-channel attacks on Gateway ECU
    - Embedded malware on Smartphone
  - Virtualization on embedded devices
  - Secure runtime environments, e.g., Google Wallet

Department of Computer Engineering | Prof. Dr. Stefano Zanero
Department of Computer Engineering | Dr. Federico Maggi
Chair for System Security | Prof. Dr. Thorsten Holz

Applied Automotive Security

Live Demonstration

> “Attacks are sexy but countermeasures are the more challenging task.”