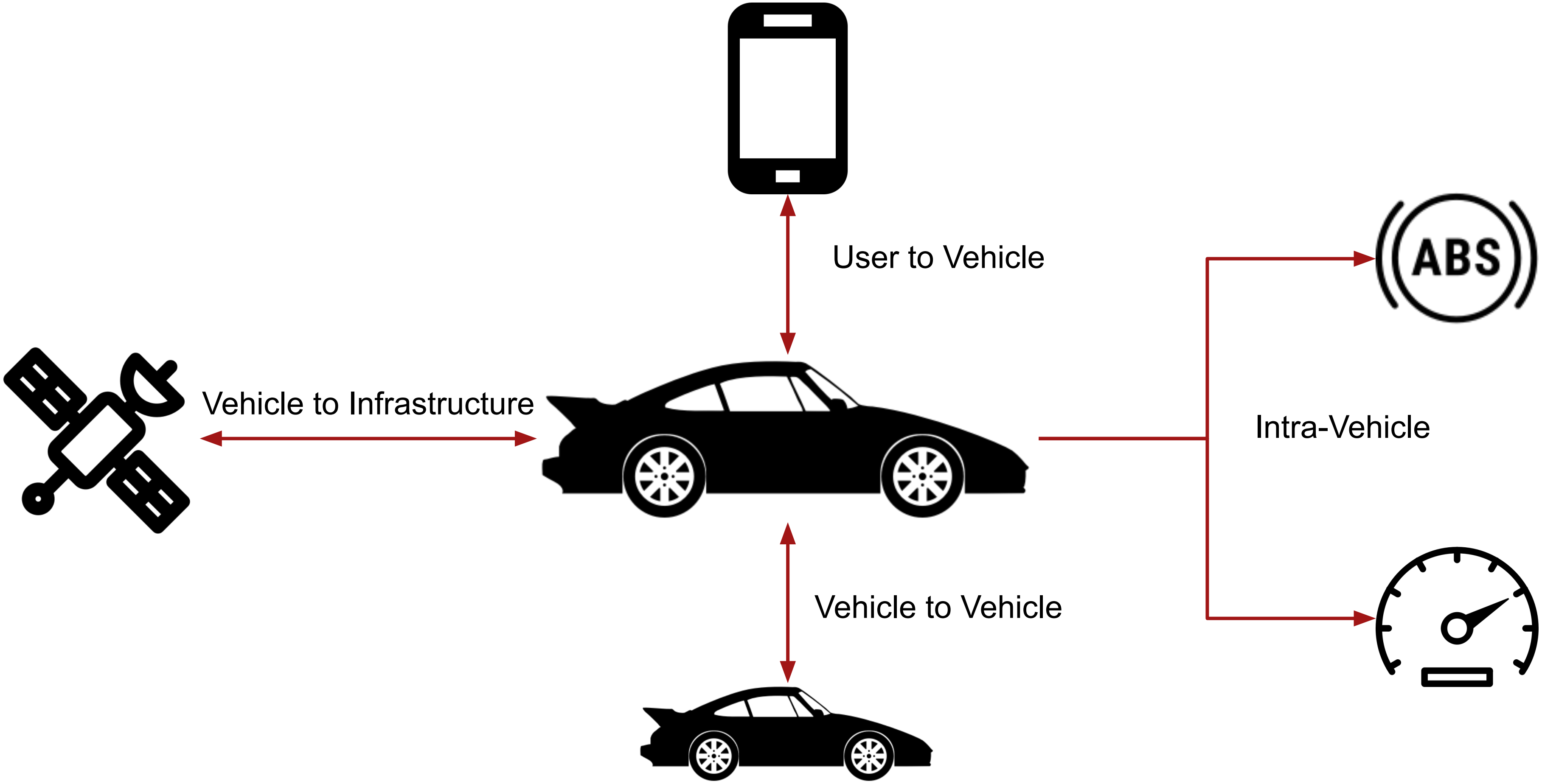
UNIVERSITY OF CATANIA
DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE

# Security of modern vehicles in the IoT world

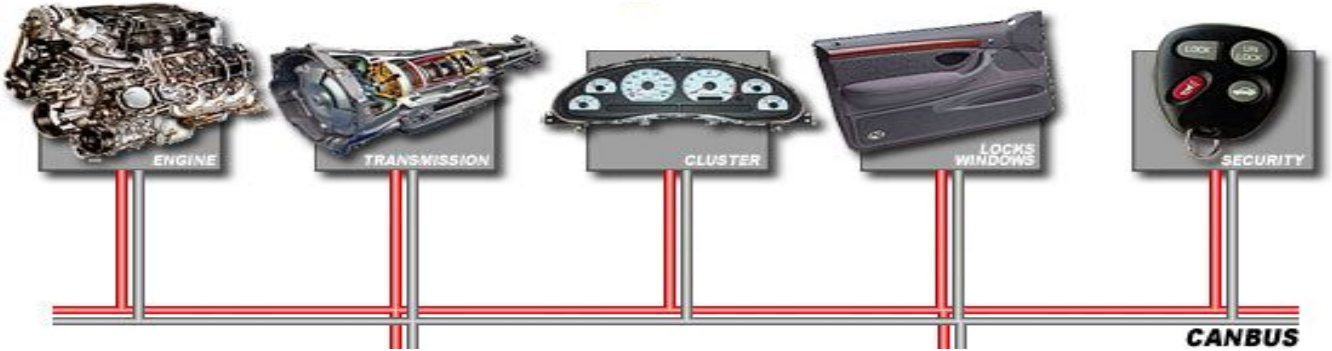
NGIoT e-workshop on ETSI IoT Standard

*Pietro Biondi*

# Automotive communication domains

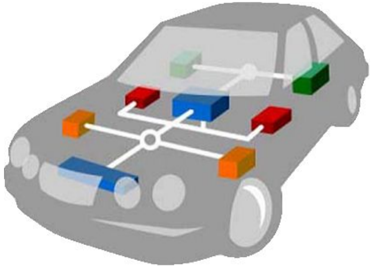


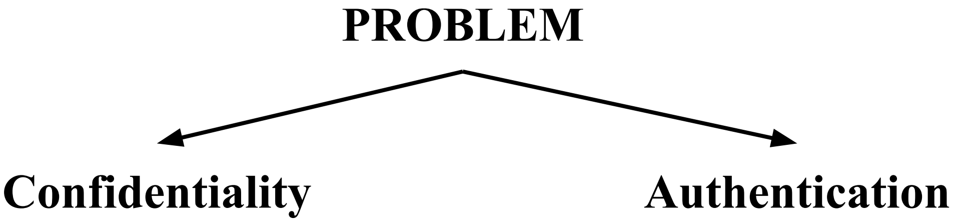
# Controller Area Network



The **Controller area network (CAN-bus)** is provided with:

- Serial communication protocol
- Message anti-collision protection
- Error detection





**PROBLEM**

**Confidentiality**

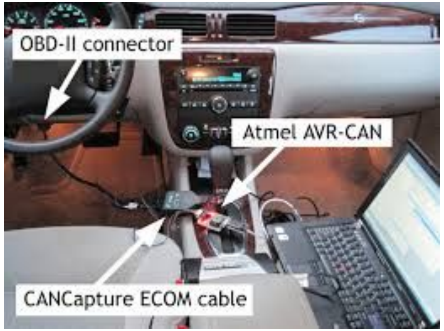
**Authentication**

# Experimental Security Analysis of a Modern Automobile (2010)

K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage

IEEE Symposium on Security and Privacy, Oakland, CA, 2010.

- Wide variety of telematic vulnerabilities on:
  - CD players
  - Bluetooth
  - Cellular radio
- Lack of authentication required to access car systems
- Arbitrary ECUs should not be able to issue diagnostic commands



# Attack on Jeep Cherokee (2015)

Remote Exploitation of an Unaltered Passenger Vehicle
C.Miller and C. Valasek, BlackHat 2015

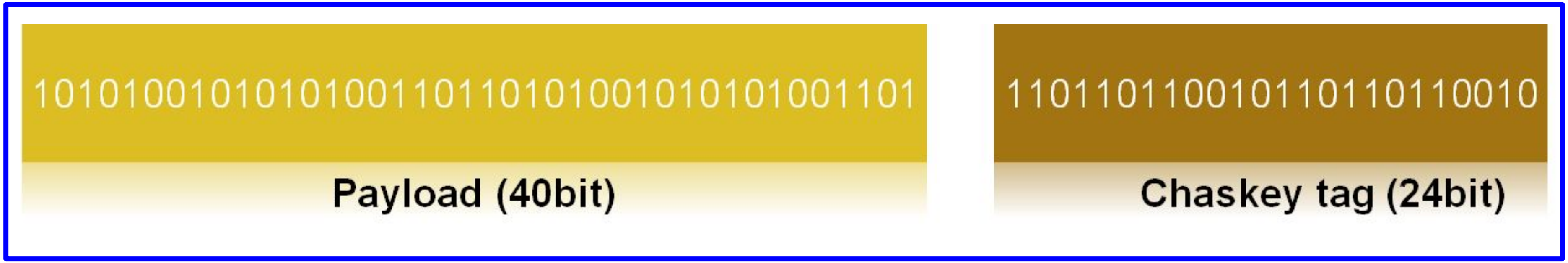
- Remote-attack on a Jeep Cherokee
- Key components of the attack:
    - Reverse engineer the CAN messages sent by individual ECUs – no encryption
    - Inject messages as another ECU – no authentication

# TOUCAN

**proTocol tO secUre Controller Area Network:**

- Safe, CAN and AUTOSAR compliant.
- Guarantees: authentication, integrity and confidentiality
- The hardware update of the ECU is not necessary
- It has a prerequisite that the cryptographic keys are distributed correctly

Transform CAN frames into TOUCAN frames



1010100101010100110110101001010101001101

Payload (40bit)

110110110010110110110010

Chaskey tag (24bit)

**SPECK-64**

# SPECK-64 + Chaskey MAC

**SPECK-64:** Symmetric cipher used in systems with low computational resources.
The features of SPECK are:

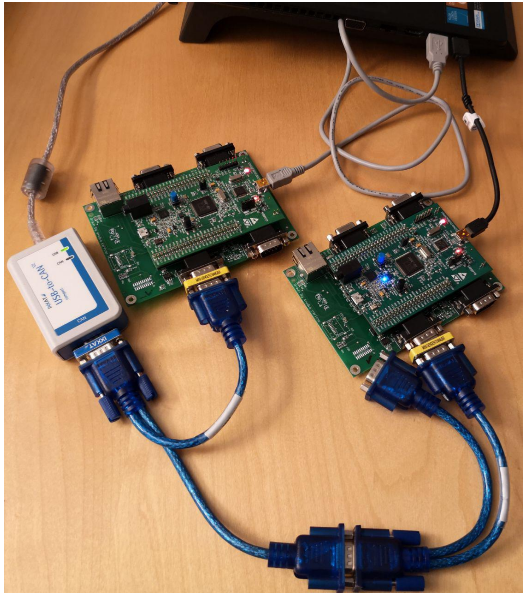
- Block cipher with 64-bit block size
- Supported key lengths: 128, 192 and 256 bit
- Efficiency in software and hardware
- On the ARM platform: about 3 times faster than AES

**Chaskey:** permutation-based MAC algorithm based on Addition-Rotation-XOR (ARX) with some useful features:

- Efficient MAC algorithm for microcontrollers
- It is intended for applications that require 128-bit security
- Robustness under tag truncation

# Implementation of TOUCAN

- **STM32F407 Discovery**
- **Communication between two boards**



## Performances

| **Algorithm** | **Board Speed**[MHz] | **Time**[µs] |
|---|---|---|
| Chaskey MAC | 168 | 0,43 |
| SPECK-64 | 168 | 5,36 |
| SPECK-64 + Chaskey MAC | 168 | 5,79 |

# Conclusions

The automotive safety sector is really expanding precisely because cars tend to be increasingly connected to each other and gradually become part of the IoT world

- Automotive communication domains
- Introduction to the CAN bus and its problems
- The most famous car hacks
- Implementation of TOUCAN, a CAN-based security protocol
  - Requires only the update of the ECUs firmware
  - Based on fast-hashing and symmetric cryptography.
  - The cryptographic functions never exceed the six microseconds of computation

# Thank you for your attention

Pietro Biondi
pietro.biondi94@gmail.com