TOUCAN: a proTocol tO secUre Controller Area Network

Ilaria Matteucci  
Gianpiero Costantino  
Giampaolo Bella  
Pietro Biondi
Introduction

Vehicles are Cyber-Physical System (CPS):

- Parking sensors
- Infotainment system
- Wireless connectivity
- Lane assistant

Safety-critical system are being exposed to security issues:

- Connectivity is the key enabler
In-vehicle network

Vehicles functionalities are managed by Electronic Control Units (ECU)

ECU communicate via CAN bus protocols
The CAN bus as is

Cybersecurity analysis:

- Max data-message length is **64bit**

- Authentication and !Integrity and !Confidentiality
Attack on Jeep Cherokee

C. Miller and C. Valasek, BlackHat 2015
CANDY: haCking infotAiNment AnDroid sYstems

Automotive SPIN 2018

Details on https://sowhat.iit.cnr.it
Exploiting the **Android ADB Debug Port Remote Access** vulnerability of an Android based infotainment system to remotely send crafted CAN messages

Details will be provided soon on https://sowhat.iit.cnr.it
TOUCAN: a proTocol to secUre Controlled Area Network

Research paper will be presented at AutoSEC@ACM CODASPY 2019
# AUTOSAR Standard Profile

**Specification of Secure Onboard Communication**  
AUTOSAR CP Release 4.3.1

## Parameter | Configuration value
--- | ---
Algorithm | CMAC/AES-128
Length of Freshness Value (parameter SecOCFreshnessValueLength) | 0
Length of truncated Freshness Value (parameter SecOCFreshnessValueTxLength) | 0 bits
Length of truncated MAC (parameter SecOCAuthInfoTxLength) | 24 bits
Design of TOUCAN

Turning CAN frames into **TOUCAN** frames

---

**SPECK64**

**Chaskey** - a very efficient permutation-based MAC algorithm based on ARX robust under tag truncation.

**SPECK64** - lightweight block ciphers with a 128bit key
Risk analysis of TOUCAN

- **Risk of guessing the tag** \(2^{-|\text{tag}|}\)
  - \(|\text{tag}| = 24\) bit
  - Probability of attack \(0,6 \times 10^{-7}\)

- **Probability of tag collision (Birthday attack)** \(2^{(|\text{tag}|)/2}\)
  - \(|\text{tag}| = 24\) bit
  - Boundary limit before collision \(4096\) frame

- **Security of SPECK 64/128**
  - 27 Rounds
  - No attacks found
A prototype implementation of TOUCAN

**STM32F407 Discovery**

- **Green led**: the payload is Toucan compliant
- **Red led**: the payload is not Toucan compliant

### Performances

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Board Speed (mhz)</th>
<th>Time (micros)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chaskey</td>
<td>168</td>
<td>0,429</td>
</tr>
<tr>
<td>Speck64</td>
<td>168</td>
<td>5,357</td>
</tr>
</tbody>
</table>
## Comparison with SoTA

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>F1. Standard CAN</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>F2. Frame rate equal to CAN’s.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
</tr>
<tr>
<td>F3. Payload size not smaller than CAN’s.</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>F4. Standard AUTOSAR</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>F5. No ECU upgrade</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>F6. No infrastructure upgrade</td>
<td>✓</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Total</td>
<td>1</td>
<td>0</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
## Open Challenge 1: Managing AUTOSAR profile 1

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm</td>
<td>CMAC/AES-128</td>
</tr>
<tr>
<td>Length of Freshness Value (parameter SecOCFreshnessValueLength)</td>
<td>Not Specified</td>
</tr>
<tr>
<td>length of truncated Freshness Value (parameter SecOCFreshnessValueTxLength)</td>
<td>8 bits</td>
</tr>
<tr>
<td>length of truncated MAC (parameter SecOCAuthInfoTxLength)</td>
<td>24 bits</td>
</tr>
</tbody>
</table>
Open Challenge 2: Managing different network topologies

One Secure Gateway

More Secure Gateways
Different Protocols
Open Challenge 3: Managing different communication protocols

**CAN 2.0 Frame**

![CAN 2.0 Frame Diagram]

**CAN FD Frame**

![CAN FD Frame Diagram]
Thank you!

Find us on
https://sowhat.iit.cnr.it