Automotive Security: Solutions and Open Challenges

Gianpiero Costantino
Ilaria Matteucci
Fabio Martinelli

Pisa, 08/02/2019
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

- Max data-message length is **64bit**
- Authentication and Integrity and Confidentiality

```
11010110101010010101001010100101010
```
Attack on Jeep Cherokee

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

Local Vs Remote
CANDY: haCking infotAiNment AnDroid sYstems
CANDY

Hacking intra-vehicular CAN bus communications by injecting a RAT on an Android-based infotainment system
Attack Work-flow

I. **Remotely accessing** the In-Vehicle Infotainment system
II. **Recording** driver’s voice
III. **Taking** photos and **grabbing** vehicle’s trajectories
IV. **Collecting** information spread on the CAN bus
Photos from parking-camera
Vehicle’s trajectories
https://www.youtube.com/watch?v=AW0D-I0GD7E

LA TUA AUTO TI SPIA
Stealing CAN bus information

The **attacker** downloads and modifies the original APP to store the CAN bus information on files that later on can be downloaded.

<table>
<thead>
<tr>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Water temperature</td>
</tr>
<tr>
<td>Seat belt attached or not</td>
</tr>
<tr>
<td>Handbrake pulled or not</td>
</tr>
<tr>
<td>Car doors status</td>
</tr>
<tr>
<td>Remaining fuel</td>
</tr>
<tr>
<td>Voltage of the battery</td>
</tr>
<tr>
<td>Engine rpm</td>
</tr>
<tr>
<td>Car speed</td>
</tr>
<tr>
<td>Air conditioning system status</td>
</tr>
<tr>
<td>Distance from an obstacle</td>
</tr>
</tbody>
</table>
CAN bus data
Recognition Module: *how it works*
Driver Recognition

start → parameter acquisition via CAN → do parameter belong to the driver? → YES → end

NO → notify the driver

? ? ?
Attacks on Can bus

- **DoS attack**: injecting messages of ‘0000’ CAN ID every 0.3 milliseconds.
- **fuzzy attack**: injecting messages of totally random CAN ID and DATA values every 0.5 milliseconds.
- **spoofing attack (RPM/gear)**: injecting messages of certain CAN ID related to RPM/gear information every 1 millisecond.

Datasets were constructed by logging CAN traffic via the OBD-II port from a real vehicle while message injection attacks were performing.
Classification Analysis

Fuzzy classification algorithms;
• FuzzyRoughNN
• NN
• DiscernibilityClassifier
• FURIA

90% training – 10% testing
We obtained following results:

- a precision equal to 0.963 and a recall equal to 1 in the identification of dos attack;
- a precision equal to 0.85 and a recall equal to 1 in the identification of fuzzy attack;
- a precision equal to 1 and a recall equal to 1 in the identification of gear and rpm attacks.

\[
PR = \frac{TP}{TP + FP}; \quad RC = \frac{TP}{TP + FN}; \\
Fm = \frac{2PR \cdot RC}{PR + RC}; \quad Acc = \frac{TP + TN}{TP + FN + FP + TN}
\]
TOUCAN: a protocol to secure Controlled Area Network
## AUTOSAR Standard Profile

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

<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)SecOC</td>
<td>0</td>
</tr>
<tr>
<td>Length of truncated Freshness Value (parameter SecOCFreshnessValueTxLength)</td>
<td>0 bits</td>
</tr>
<tr>
<td>Length of truncated MAC (parameter SecOCAuthInfoTxLength)</td>
<td>24 bits</td>
</tr>
</tbody>
</table>
MAC + Encryption

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

Recommendation for block cipher modes of operation:
The emac mode for authentication
Dworkin - NIST Special Publication

\[ \text{Size}(\text{tag}) \geq \log \left( \frac{\text{MaxInvalids}}{\text{Risk}} \right) \]

**Example:**
Size(tag)=24 bit
MaxInvalids= 30 ($2^5$) frames

Size(tag)=24 bit
Risk= $2^{-11}$

Risk= 0.00019%

MaxInvalids= 8192 ($2^{13}$) frames
A prototype implementation of TOUCAN

**STM32F407 Discovery**

*Green led:* the payload is correctly encrypted  
*Red led:* the payload is not correctly encrypted

**Performances**

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Board Speed (mhz)</th>
<th>Time (micros)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chaskey</td>
<td>84</td>
<td>11,90</td>
</tr>
<tr>
<td>Speck64</td>
<td>84</td>
<td>11,58</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>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>F2. Frame rate equal to CAN’s.</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>F3. Payload size not smaller than CAN’s.</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>F4. Standard AUTOSAR</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>F5. No ECU upgrade</td>
<td>✗</td>
<td>✗</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>
</tbody>
</table>

| Total    | 1 | 0 | 3 | 1 | 2 | 5 | 5 |
Open Challenge 1:
Managing AUTOSAR profile 1

Specification of Secure Onboard Communication
AUTOSAR CP Release 4.3.1

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

More Secure Gateways

Different Protocols
Open Challenge 3: Managing different communication protocols

CAN 2.0 Frame

```
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| SOF | Identifier | RTR | IDE | FC | DLC |
|     | Data        |     |     |     |     |
|     | Data        |     |     |     |     |
|     | CRC         | ACK | SOF | IFS |
```

CAN FD Frame

```
Arbitration phase

- Bus Idle
- SOF
- Arbitration Field
- Control Field

Data transmission phase

- Data Field
- CRC Field
- ACK Field
- EOF

Arbitration phase

- IFS

Field sizes:

- 1 Bit
- 12 Bit
- 9 Bit
- 0 to 64 Byte
- 16 Bit
- 18 Bit
- 22 Bit
- 2 Bit
- 7 Bit
- 3 Bit
```
Thank you!

Gianpiero Costantino  gianpiero.costantino@iit.cnr.it
Ilaria Matteucci      ilaria.matteucci@iit.cnr.it
Fabio Martinelli      fabio.martinelli@iit.cnr.it