TOUCAN: a proTocol tO secUre Controller Area Network

Ilaria Matteucci
Gianpiero Costantino
Giampaolo Bella
Pietro Biondi

Consiglio Nazionale
delle Ricerche

Orbassano, 21/02/2019

Introduction

Vehicles are Cyber-Physical System (CPS):

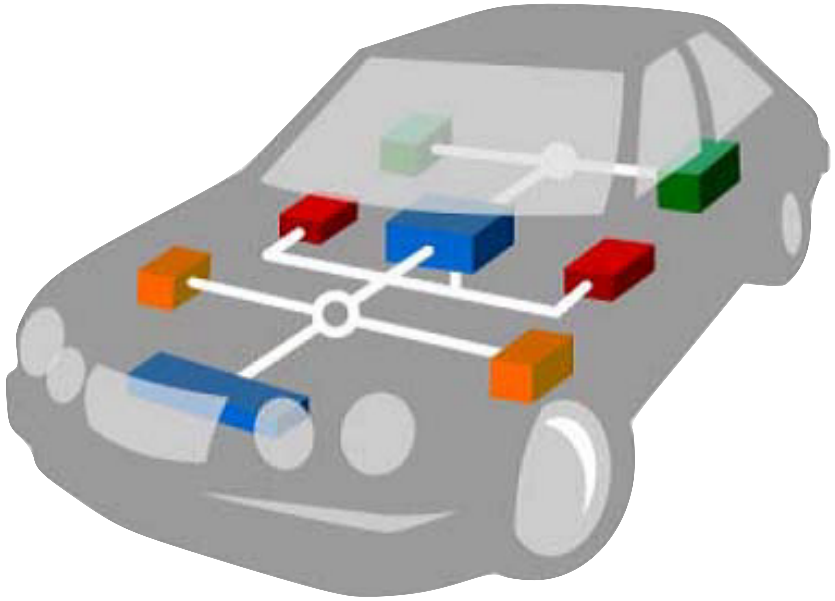
- ➡ Parking sensors
- ➡ Infotainment system
- ➡ Wireless connectivity
- ➡ Lane assistant

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

<table>
<tr><th>0</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th><th>16</th><th>17</th><th>18</th><th>19</th><th>20</th><th>21</th><th>22</th><th>23</th><th>24</th><th>25</th><th>26</th><th>27</th><th>28</th><th>29</th><th>30</th><th>31</th></tr>
<tr><td>SOF</td><td colspan="11">Identifier</td><td>RFR</td><td>IDE</td><td>r0</td><td colspan="4">DLC</td><td colspan="13"></td></tr>
<tr><td colspan="32">Data</td></tr>
<tr><td colspan="32">Data</td></tr>
<tr><td colspan="16">CRC</td><td colspan="2">ACK</td><td>SOF</td><td colspan="7">IFS</td><td colspan="6"></td></tr>
</table>

The CAN bus as is

Cybersecurity analysis:

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

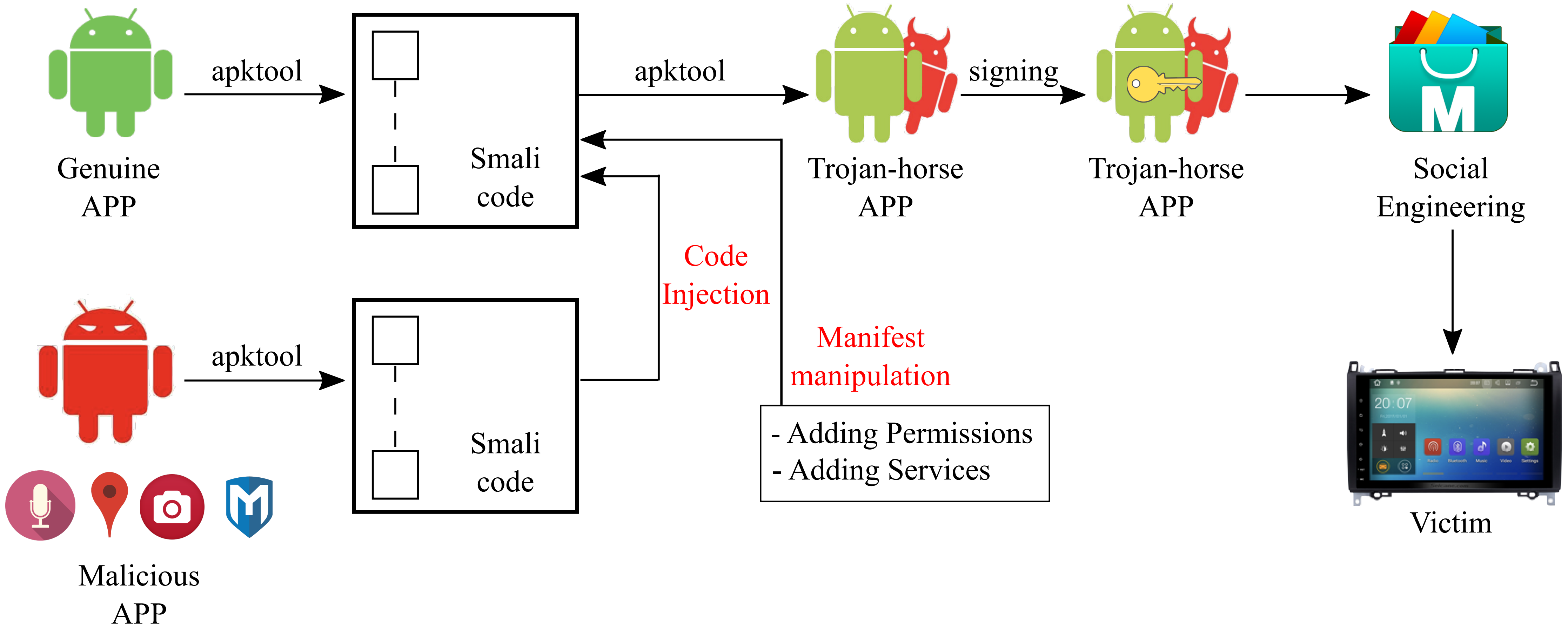
11010110101010010101001010100101010

Attack on Jeep Cherokee

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

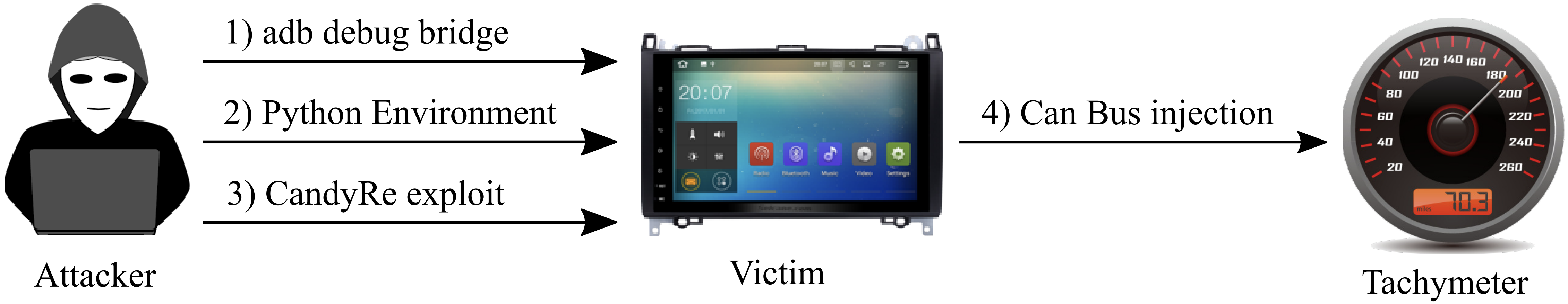
CANDY: haCking infotAiNment AnDroid sYstems

Automotive SPIN 2018



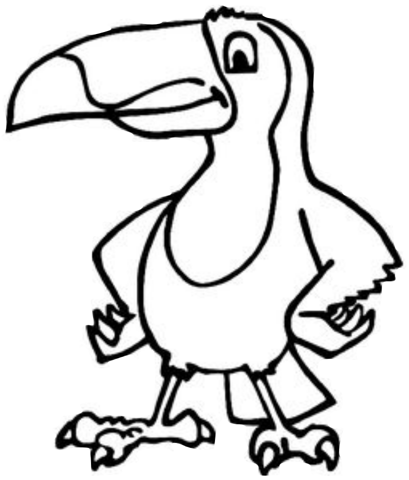
Details on https://sowhat.iit.cnr.it

CandyRE - ha**C**king infot**AiN**ment An**D**roid s**Y**stems **R**emote **E**xploitation



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



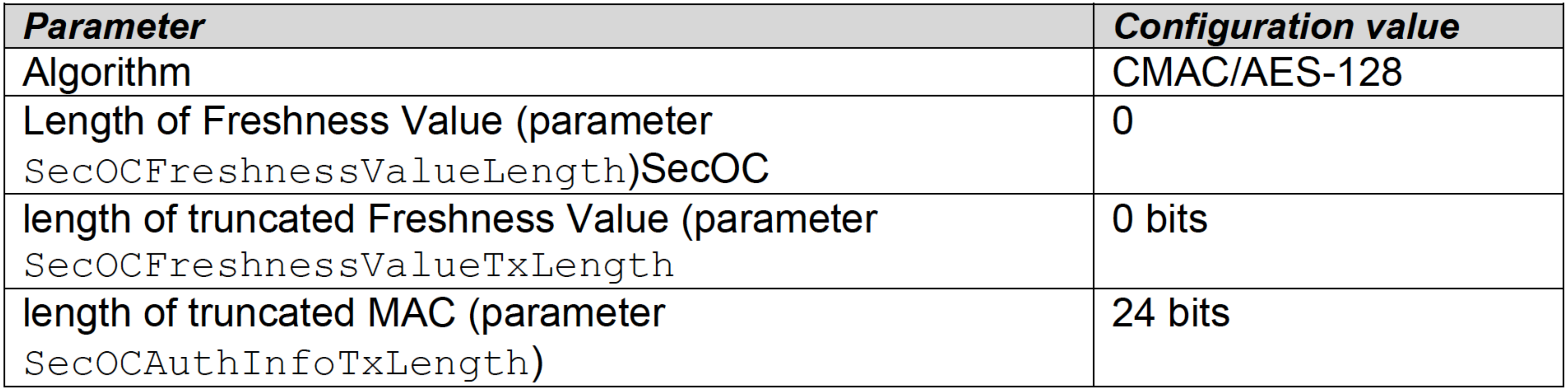
TOUCAN: a proTocol tO secUre Controlled Area Network

Research paper will be presented at
AutoSEC@ACM CODASPY 2019

AUTOSAR Standard Profile

AUTOSAR

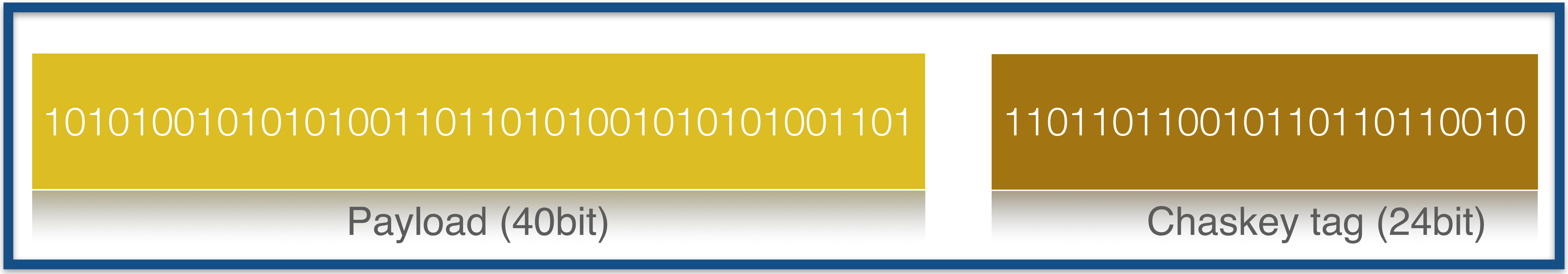
Specification of Secure Onboard Communication
AUTOSAR CP Release 4.3.1



Parameter	*Configuration value*
Algorithm	CMAC/AES-128
Length of Freshness Value (parameter `SecOCFreshnessValueLength`)SecOC	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 $2^{(-|tag|)}$

|tag| = 24 bit → Probability of attack **$0{,}6 \times 10^{-7}$**

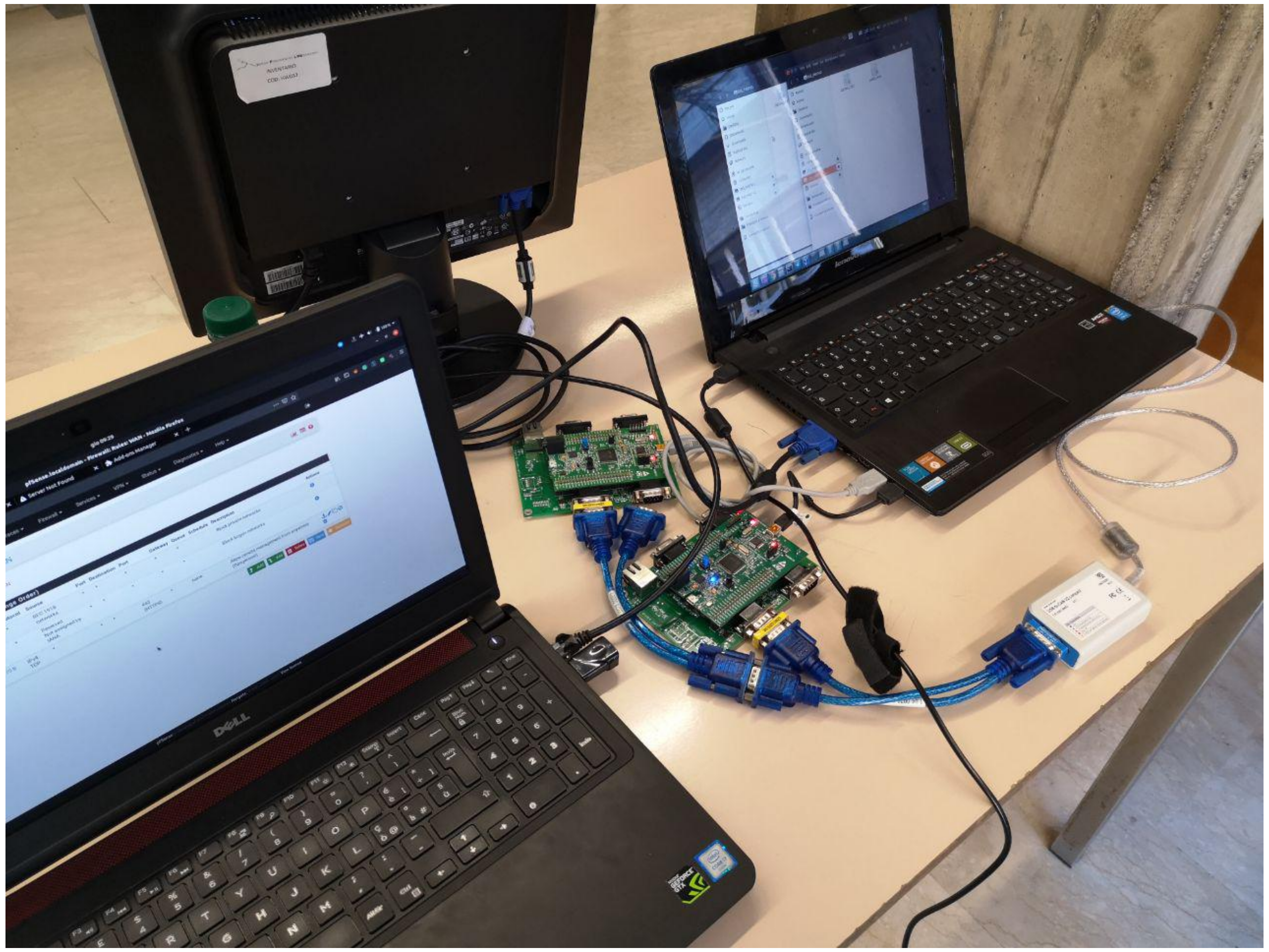
Probability of tag collision (Birthday attack) $2^{(|tag|/2)}$

|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

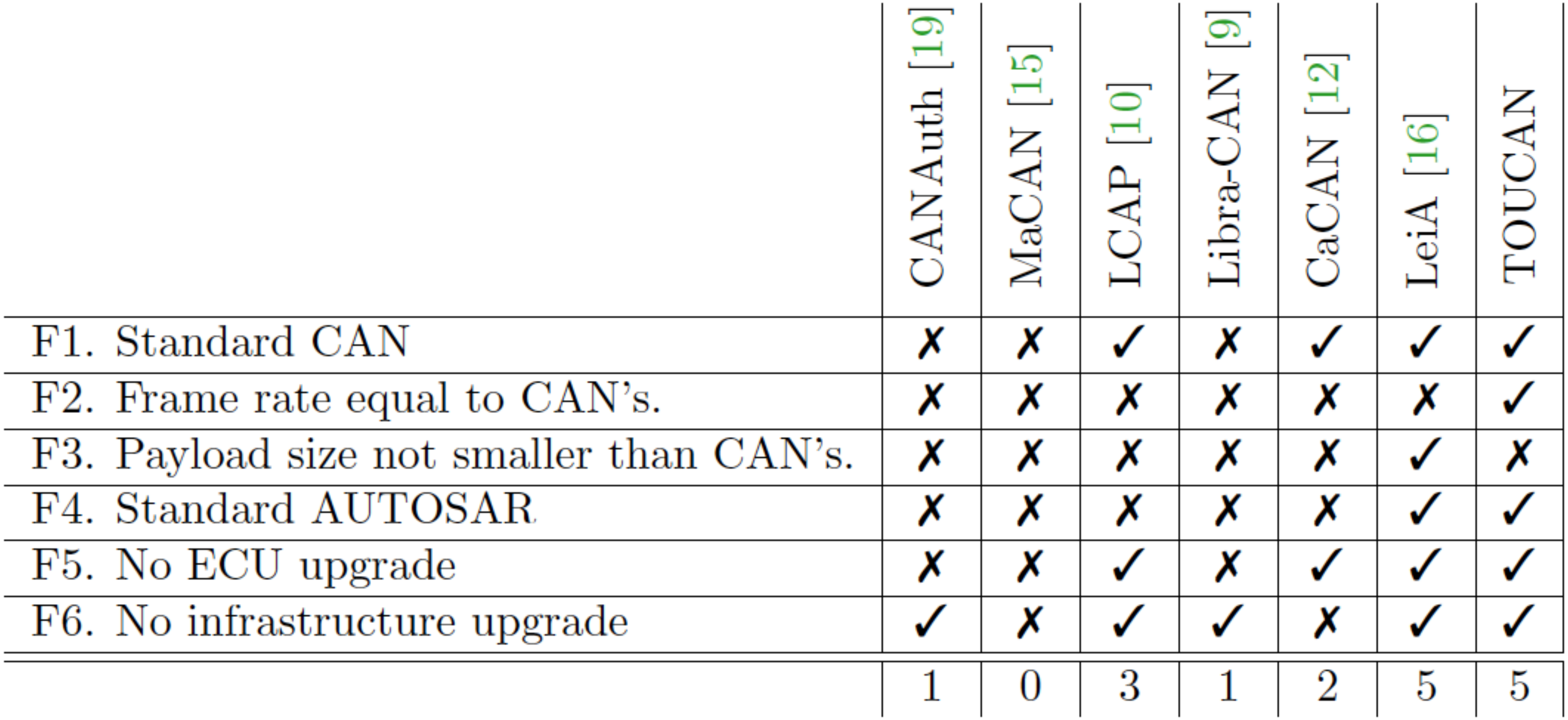
Green led: the payload is Toucan compliant

Red led: the payload is not Toucan compliant

Performances

Algortithm	Board Speed (mhz)	Time(micros)
Chaskey	168	0,429
Speck64	168	5,357

Comparison with SoTA

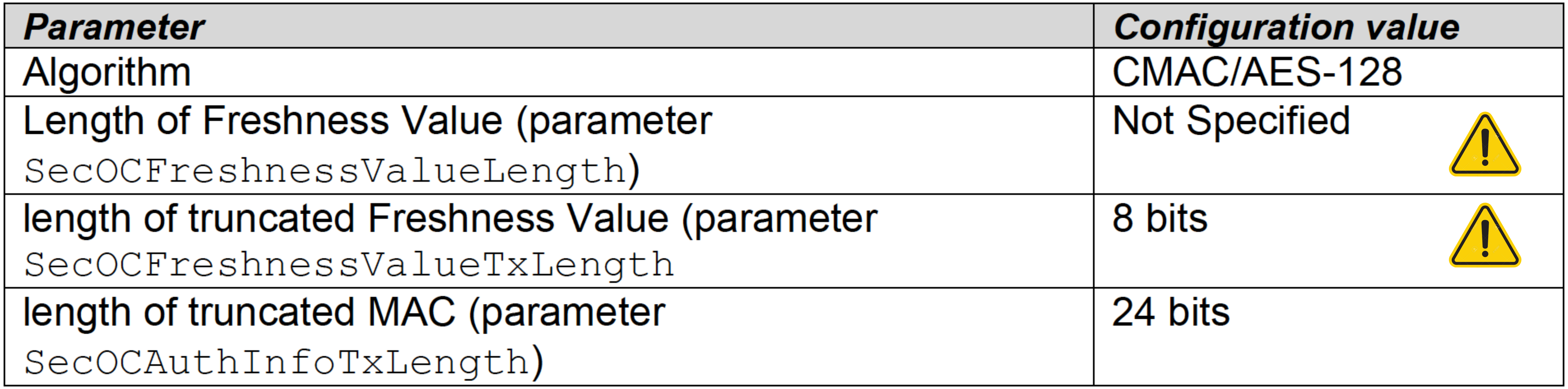


	CANAuth [19]	MaCAN [15]	LCAP [10]	Libra-CAN [9]	CaCAN [12]	LeiA [16]	TOUCAN
F1. Standard CAN	✗	✗	✓	✗	✓	✓	✓
F2. Frame rate equal to CAN's.	✗	✗	✗	✗	✗	✗	✓
F3. Payload size not smaller than CAN's.	✗	✗	✗	✗	✗	✓	✗
F4. Standard AUTOSAR	✗	✗	✗	✗	✗	✓	✓
F5. No ECU upgrade	✗	✗	✓	✗	✓	✓	✓
F6. No infrastructure upgrade	✓	✗	✓	✓	✗	✓	✓
	1	0	3	1	2	5	5

Open Challenge 1:
Managing AUTOSAR profile 1

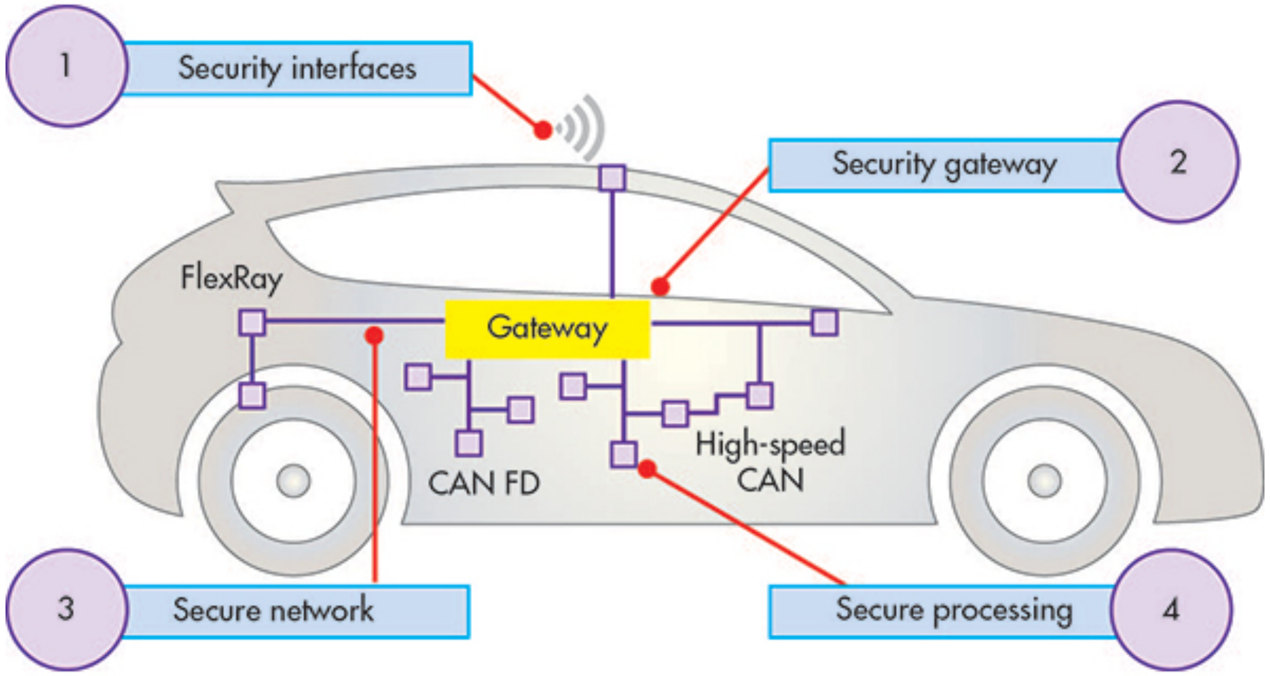
AUTOSAR

Specification of Secure Onboard Communication
AUTOSAR CP Release 4.3.1



Parameter	***Configuration value***
Algorithm	CMAC/AES-128
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

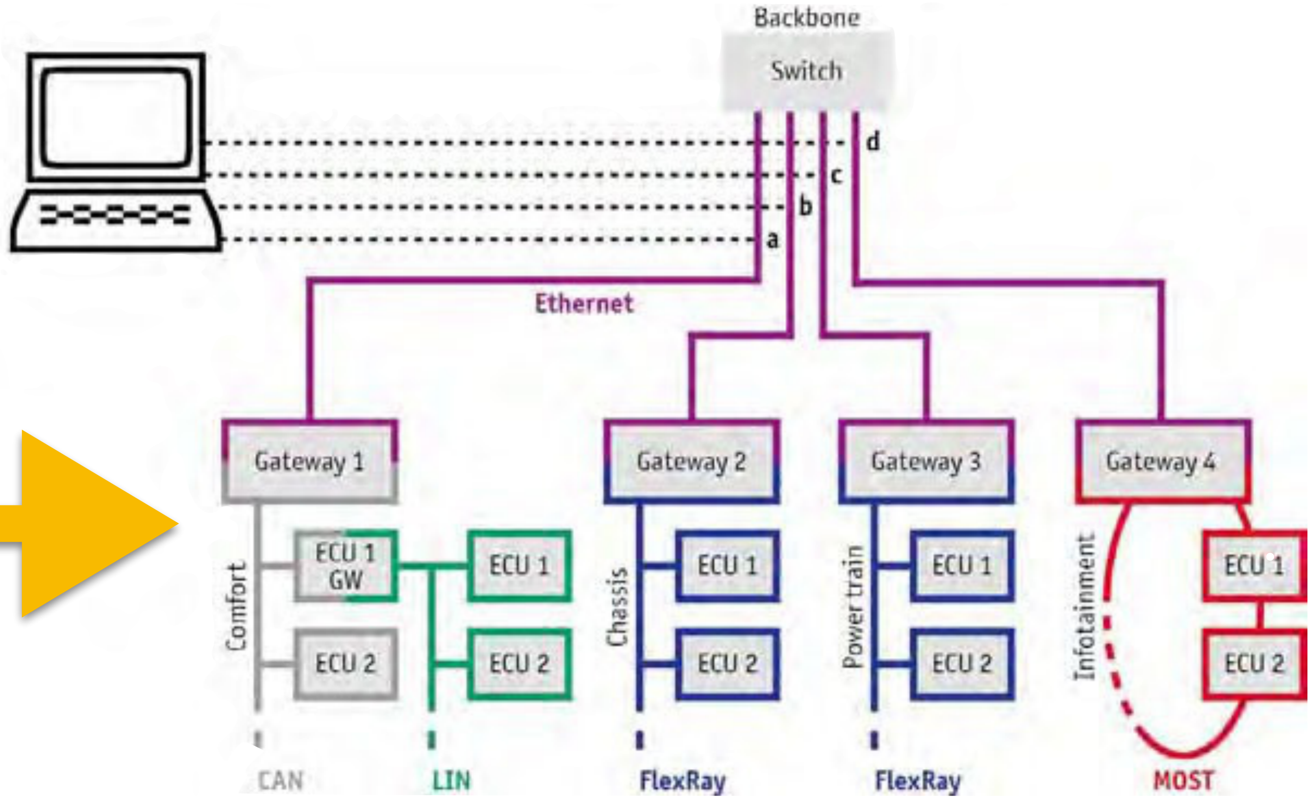
Open Challenge 2:
Managing different network topologies



One Secure Gateway

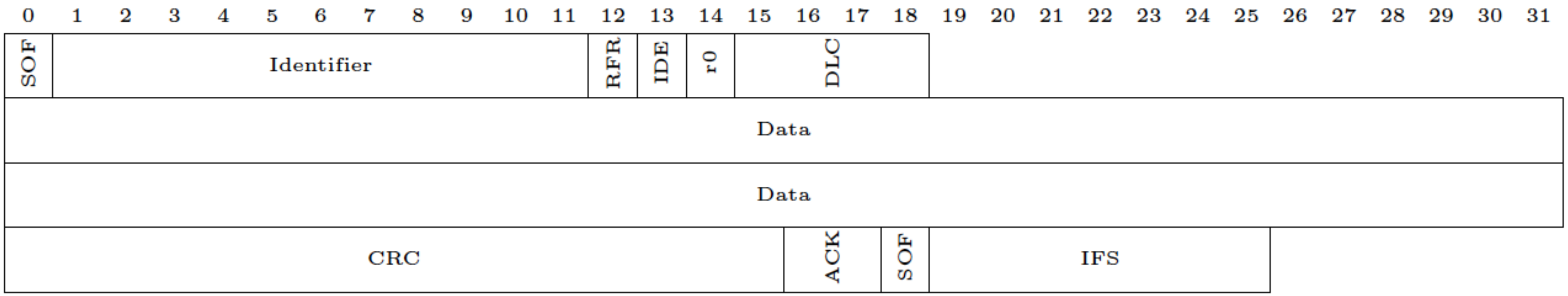
More Secure Gateways

Different Protocols

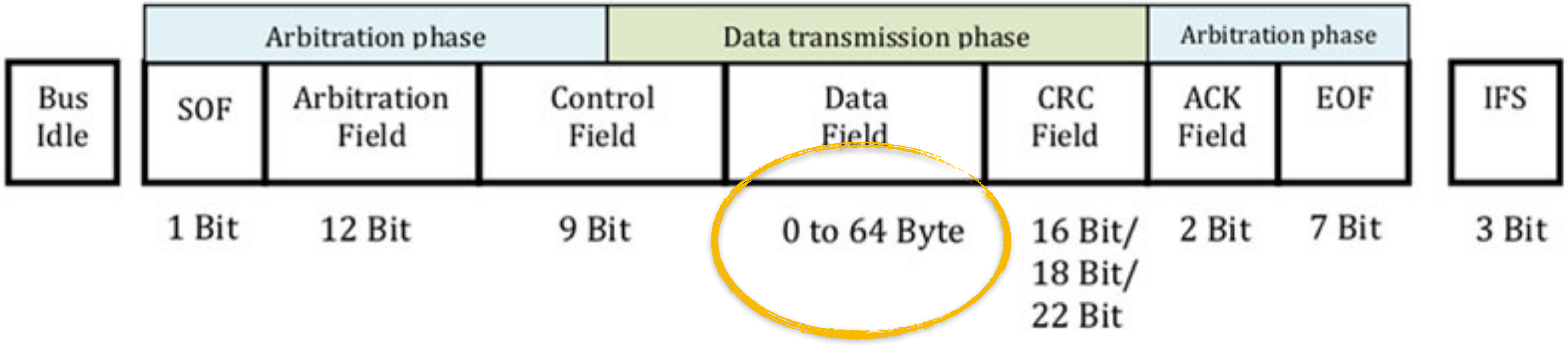


Open Challenge 3:
Managing different communication protocols

CAN 2.0 Frame



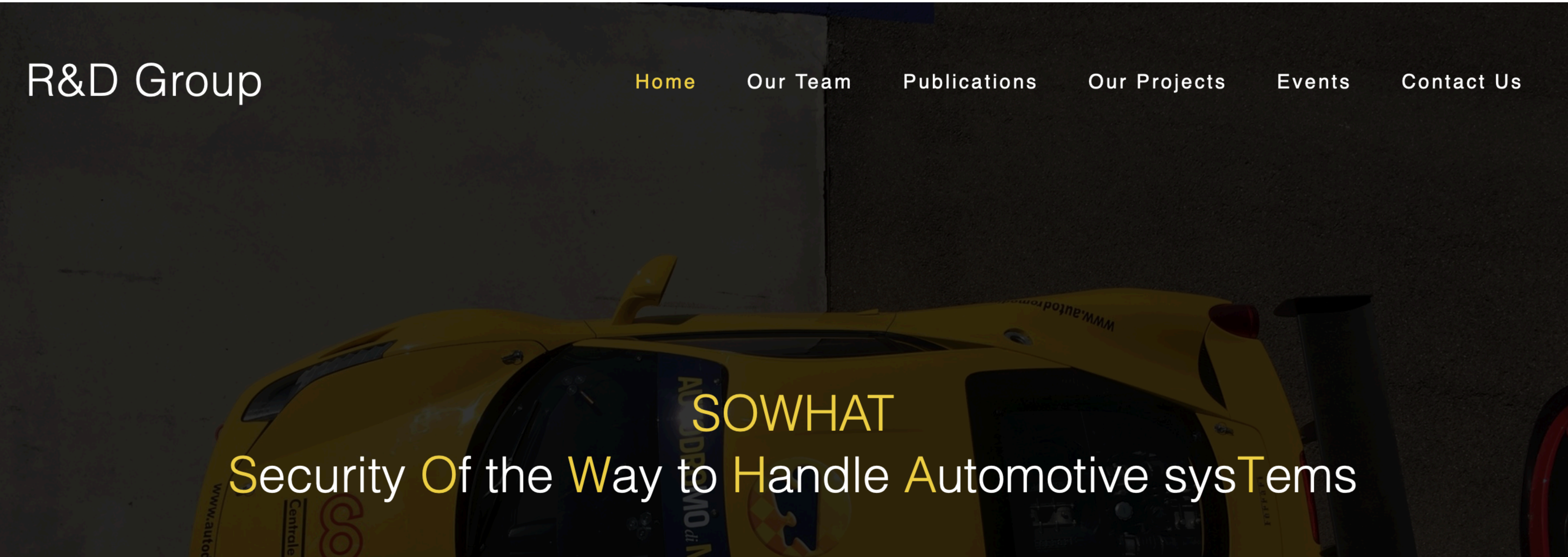
CAN FD Frame



Thank you!

Find us on

https://sowhat.iit.cnr.it



SOWHAT

Security Of the Way to Handle Automotive sysTems