NORMALIZACIÓN EN CIBERSEGURIDA PARA LA MOVILIDAD CONECTADA [...]

UNE NormalizaciónEspañola

gmv INNOVATING SOLUTIONS

A GLOBAL TECHNOLOGY GROUP

Multinational technology group

Headquarters in Spain (Madrid)

Over 2,000 employees

Aeronautics, Space, Defense, Security, Transportation, Healthcare, Banking & finances, and ICT industries.

Private capital

Subsidiaries in 10 countries

Roots tied to the Space and Defense industry

Engineering, development and integration of systems, software, hardware, specialized products and services

Founded in

1984

INTERNATIONAL TECHNOLOGY LEADERSHIP

#1 Worldwide Satellite Control Center provider to commercial telecom operators (+300 Satellite missions worldwide)

First ever **worldwide** intraoperative radiotherapy planning system

Responsible of safety critical systems of European GNSS systems (EGNOS and Galileo)

Leader of Intelligent Transportation Systems for the **public transport sector** (+100 cities in Europe, Asia and America)

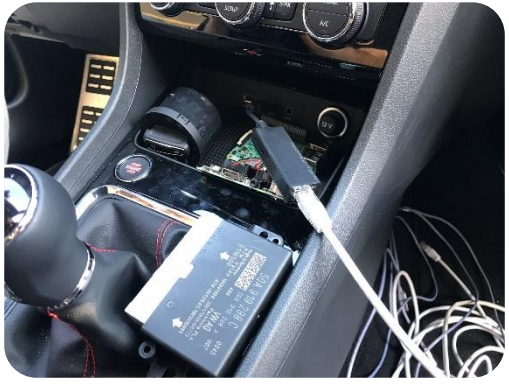
GMV's ***checker ATM security*** is the **worldwide leader** as multivendor cyber security protection for **ATMs**

WHAT WE ARE

OUR CLIENTS

ACIÓN EN CIBERSEGURID A
Y MAT
VEHÍCULOS Y SU ENTORNO

WHAT'S MY POSITION AT GMV?



WHAT'S MY POSITION AT GMV?

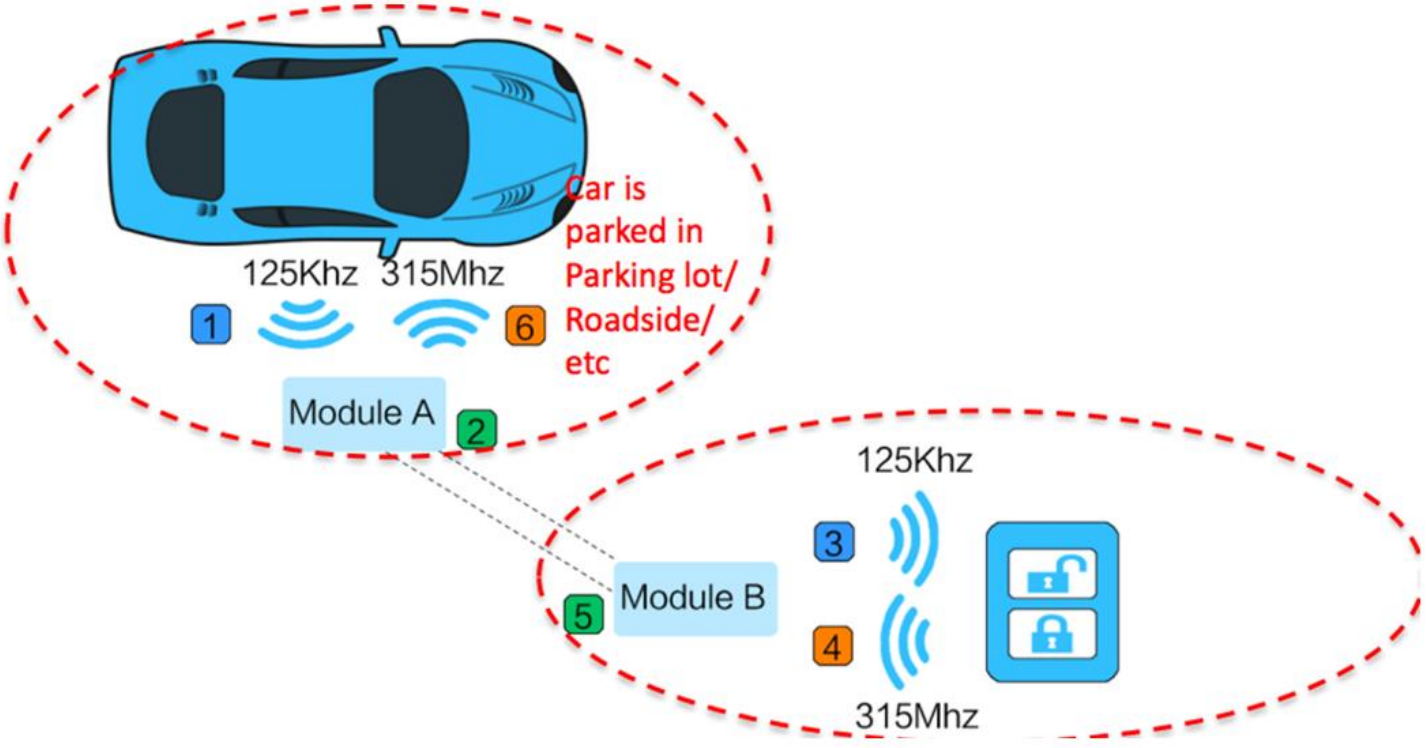
WHAT'S MY POSITION AT GMV?

- Hackers Can steal a Tesla Model S in seconds by cloning its key fob: https://www.wired.com/story/hackers-steal-tesla-model-s-seconds-key-fob/

WHAT'S MY POSITION AT GMV?

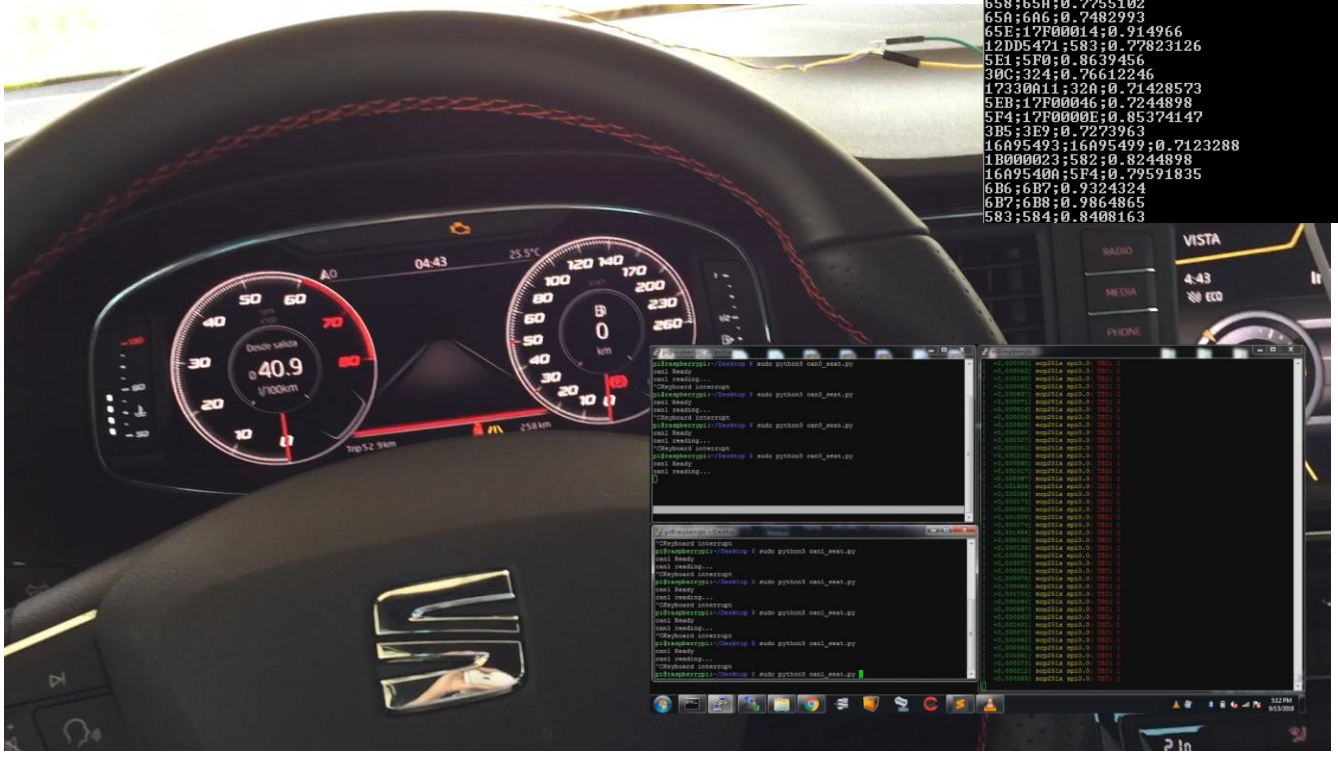
- Ingenious BMW theft attempt: https://mrooding.me/a-dutch-first-ingenious-bmw-theft-attempt-5f7f49a96ec8

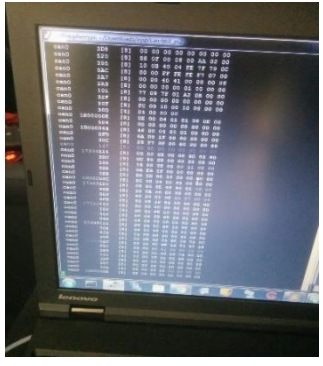
RELAY STATION ATTACK



BUS-OFF ATTACK

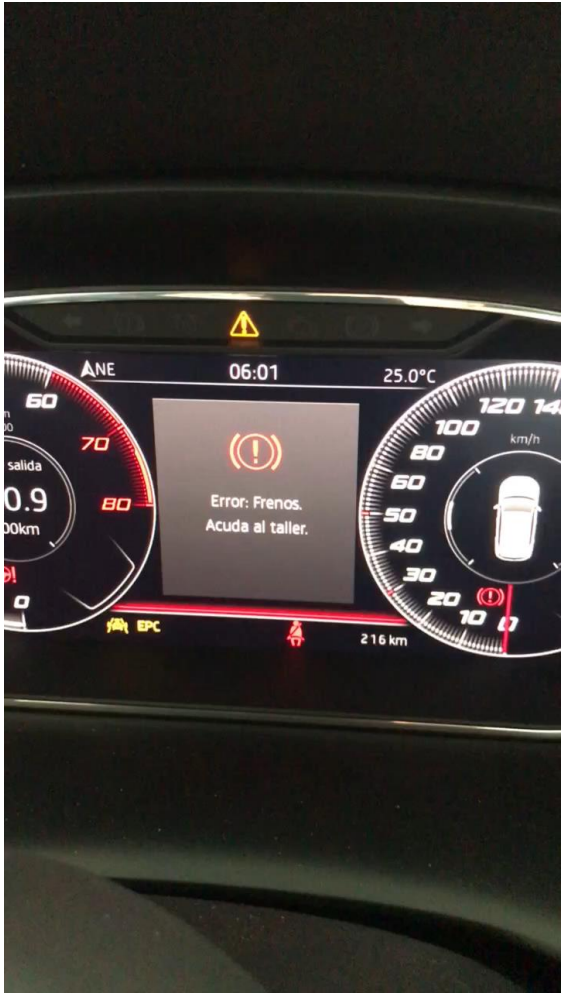
```
C:\Users\dprocar\Desktop>java -jar transition.jar candump-2018-09-04_150133.log
3E5;3CE;0.7618725
643;16A95497;0.93877554
658;65A;0.7755102
65A;6A6;0.7482993
65E;17F00014;0.914966
12DD5471;583;0.77823126
5E1;5F0;0.8639456
30C;324;0.76612246
17330A11;32A;0.71428573
5EB;17F00046;0.7244898
5F4;17F0000E;0.85374147
3B5;3E9;0.7273963
16A95493;16A95499;0.7123288
1B000023;582;0.8244898
16A95400;5F4;0.79591835
6B6;6B7;0.9324324
6B7;6B8;0.9864865
583;584;0.8408163
```





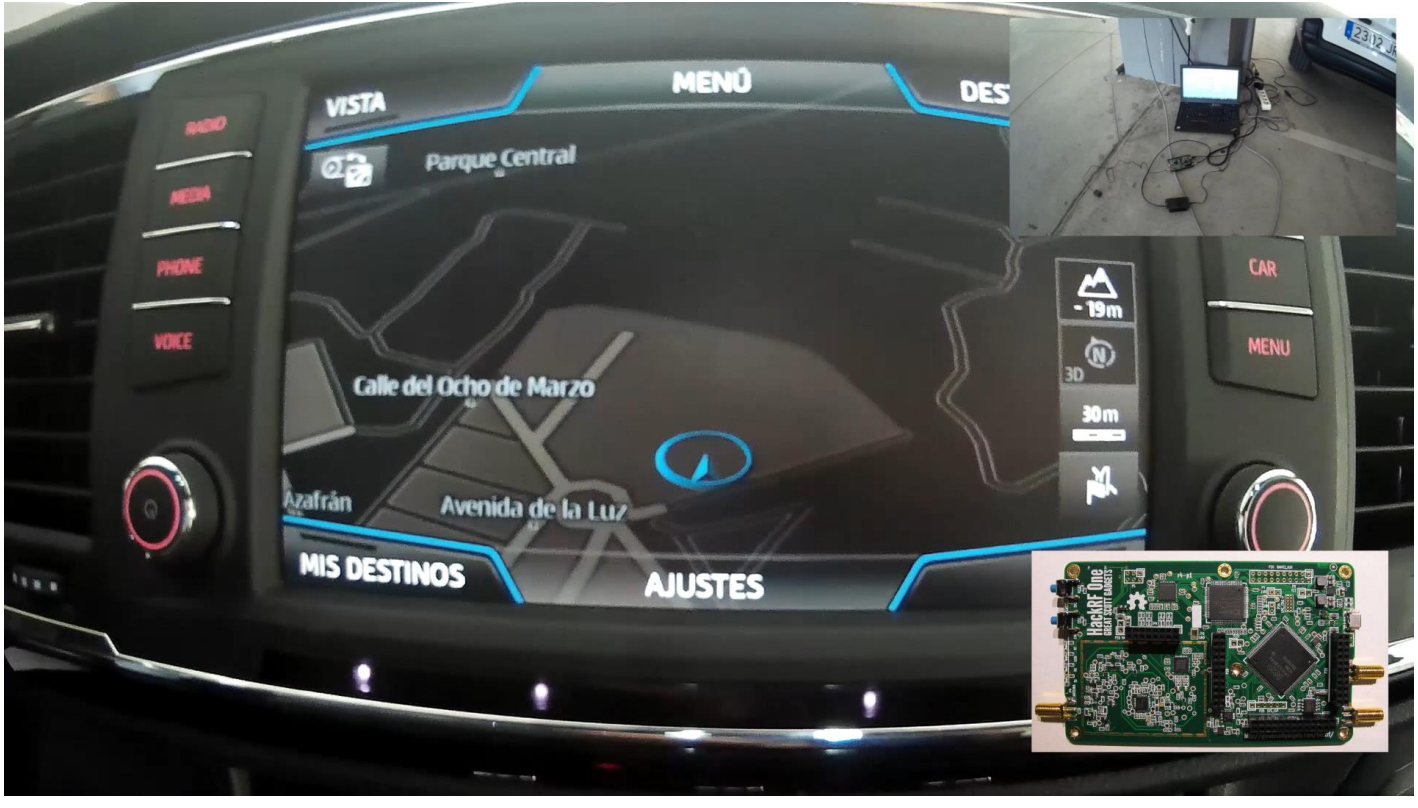
INFO INJECTION

ECU BRICK



PARK ASSIST

GPS SPOOFING



#SAFETY_FIRST

	B	C	D	Q	R
1					
2	High Level Threats	Threats	Threat details	Threat description	Scenario
78		Network outage	Outage of cable networks	Unavailability of communication links	N/A
79			Outage of wireless networks		N/A
80			Outages of mobile networks		N/A
81					N/A
82			GNSS outage		Failure
83	Eavesdropping/ Interception/ Hijacking	War driving		Threat of locating and possible exploite connection to the wireless network	N/A
84		Intercepting compromising emissions		Threat of disclosure transmitted information using interception and analysis of compromising emission	SCER
85		Interception of information	Corporate Espionage	Threat of interception of information improperly secured in transmission or improperly actions of staff	Espionage
86			Nation state espionage		Espionage
87			Information leakage due to unsecured Wi-Fi, rogue access points		N/A
88		Zero-delay SCER attack			Spoofing
89		Replay attack		Interference signal and try to avoid them	SCER
90		Meaconing	Analog meaconing	The replay of the signal is performed with hardware components such as an antenna and cables	Meaconing
91			Digital meaconing	In this case the signal is first down-converted and digitalized and after that, it is retransmitted using a software-defined-radio (SDR) kind of device.	Meaconing
92			Network meaconing	The signal is recorded at one place and transmitted to another place through the internet to be retransmitted and forge the users PVT.	Meaconing
93			Record and replay meaconing	The signal is recorded and then replayed after a specific time.	Meaconing
94		Received power monitoring			Spoofing
95		nulling	C/no signal decrease		Spoofing
96		Doppler frequency anomalies		The spoofer exploits the redundancy of some of the symbols transmitted by the satellites	Spoofing
97		Fake PRN signals		This metod performs a brute-force search for each signal over the entire range of possible code phases and carrier Doppler shifts	SCER
98		Forward estimation attack (FEA)		Exploits the redundancy of some of the symbols transmitted by the satellites.	SCER
99		Relaying attack			Man-in-the-middle

#SAFETY_FIRST

AVAILABILITY VS INTEGRITY

PaaS & SECaaS AS REQUERIMENT

- Reasonable Availability
- Own methodology for TARA
- Rights for Internal Audit
- Third party audit rights
- Monitoring of safety-related tasks

www.gmv.com

THANK YOU

Carlos Sahuquillo Pascual

Automotive CyberSecurity Consultant

@csahuqui on Twitter

https://sahuquillo.org

gmv BLOG