NORMALIZACIÓN EN CIBERSEGURIDAD PARA LA MOVILIDAD CONECTADA [...]
WHO WE ARE

A GLOBAL TECHNOLOGY GROUP

- Multinational technology group
- Headquarters in Spain (Madrid)
- Over 2,000 employees
- Private capital
- Subsidiaries in 10 countries
- Roots tied to the Space and Defense industry
- Founded in 1984
- Engineering, development and integration of systems, software, hardware, specialized products and services
WHO WE ARE

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’S MY POSITION AT GMV?
WHAT’S MY POSITION AT GMV?

THREATS EVOLUTION
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

THREATS EVOLUTION
THREATS EVOLUTION

BUS-OFF ATTACK
INFO INJECTION
THREATS EVOLUTION

ECU BRICK
PARK ASSIST

THREATS EVOLUTION
THREATS EVOLUTION

GPS SPOOFING
## CYBERSECURITY VS SAFETY

### #SAFETY_FIRST

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>High Level Threats</strong></td>
<td><strong>Threats</strong></td>
<td><strong>Threat details</strong></td>
<td><strong>Threat description</strong></td>
<td><strong>Scenario</strong></td>
</tr>
<tr>
<td>Network outage</td>
<td>Outage of cable networks</td>
<td>Unavailability of communication links</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outage of wireless networks</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Outage of mobile networks</td>
<td>N/A</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>GNSS outage</td>
<td>Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interception of information</td>
<td>Threat of interception of information improperly secured in transmission or improperly actions of staff</td>
<td>Espionage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zero-delay SCER attack</td>
<td>Interference signal and try to avoid them</td>
<td>Spoofing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replay attack</td>
<td>Analog measurement</td>
<td>Measuring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Digital measurement</td>
<td>Measuring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Network measurement</td>
<td>Measuring</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Record and replay measurement</td>
<td>Measuring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Received power monitoring</td>
<td>No signal decrease</td>
<td>Spoofing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Doppler frequency anomalies</td>
<td>The spoofer exploits the redundancy of some of the symbols transmitted by the satellites</td>
<td>Spoofing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>False PN signals</td>
<td>This method performs a brute-force search for each signal over the entire range of possible code phases and carrier Doppler shifts</td>
<td>SCER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forward estimation attack (FEA)</td>
<td>Exploits the redundancy of some of the symbols transmitted by the satellites</td>
<td>SCER</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Relaying attack</td>
<td>Man-in-the-middle</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
#SAFETY_FIRST

CYBERSECURITY VS SAFETY

AWS

SAFETY FIRST
CRITICAL
AVAILABILITY VS INTEGRITY

Confidentiality

Integrity

Availability
PaaS & SECaaS AS REQUIREMENT

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

Carlos Sahuquillo Pascual
Automotive CyberSecurity Consultant
@csahuqui on Twitter
https://sahuquillo.org