GMV

IN THE AUTOMOTIVE CYBERSECURITY SECTOR

WHO WE ARE

GMV – KEY FIGURES

OVER 1,600 EMPLOYEES

Over 33 Years of experience

GLOBAL PRESENCE

10 research and development locations in 5 continents

PRESENT IN 40 COUNTRIES

More than 1,600 customers worldwide

+50 CYBERSECURITY EXPERTS

+200 EXPERTS IN ITS AND AUTOMOTIVE

>160 Millions EUR of Turnover in 2017

10% Research & Development Investment

More than 30 patents worldwide

AUTOMOTIVE EXPERIENCE

THE COMBINATION THAT MAKES US UNIQUE

Reference supplier for on-board GNC/AOCS subsystems

European leader **in satellite navigation** processing ground segment (EGNOS and Galileo)

Big Data solutions: network anomaly detection, client segmentation

Unique product protecting critical infrastructures

Simulation

Over 15 years of automotive experience

Safety critical software (DO-178)

National Security

Leader in **Intelligent Transport Systems for Public Transportation**

Safety critical hardware (DO-254)

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

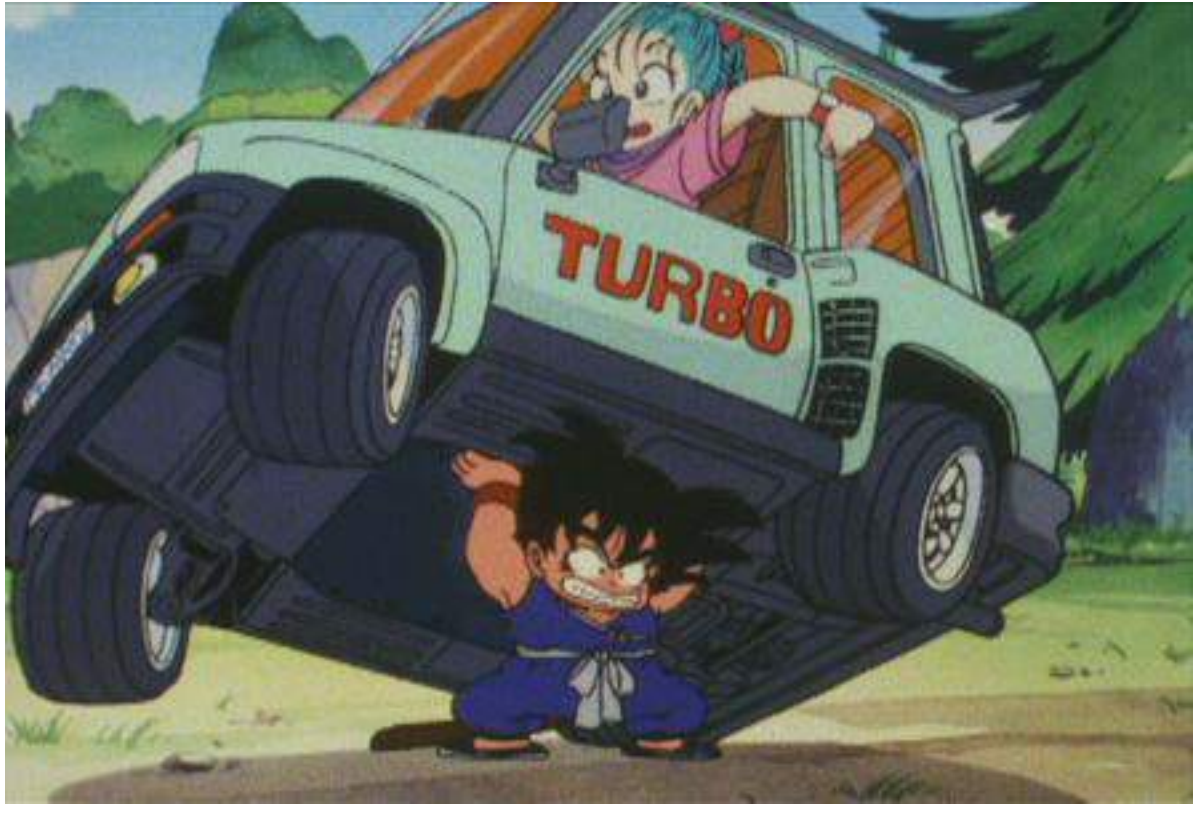
Major provider of EO Services and Applications

Specialized **cyber security** services for operators

HW & SW for railway

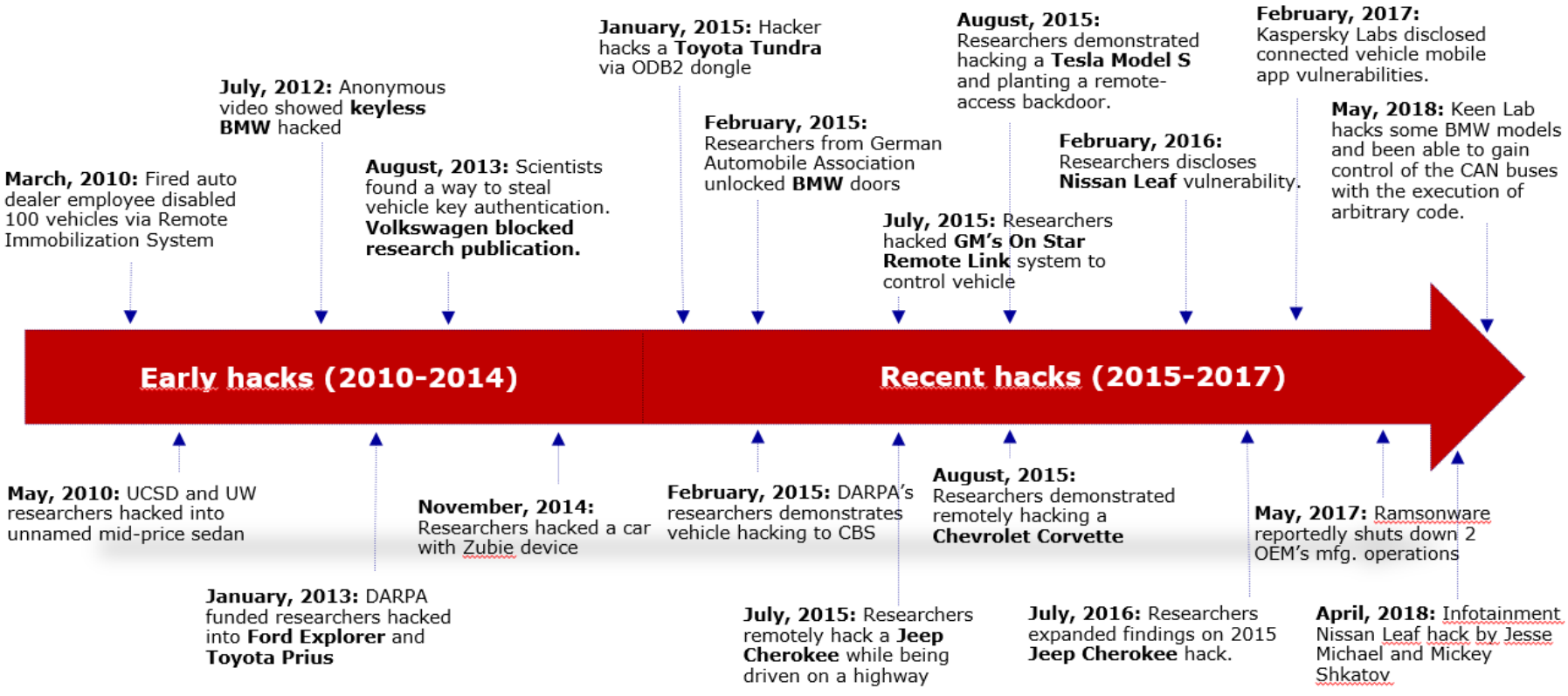
EVOLUCIÓN DE LAS AMENAZAS

THREAT EVOLUTION



EVOLUCIÓN DE LAS AMENAZAS

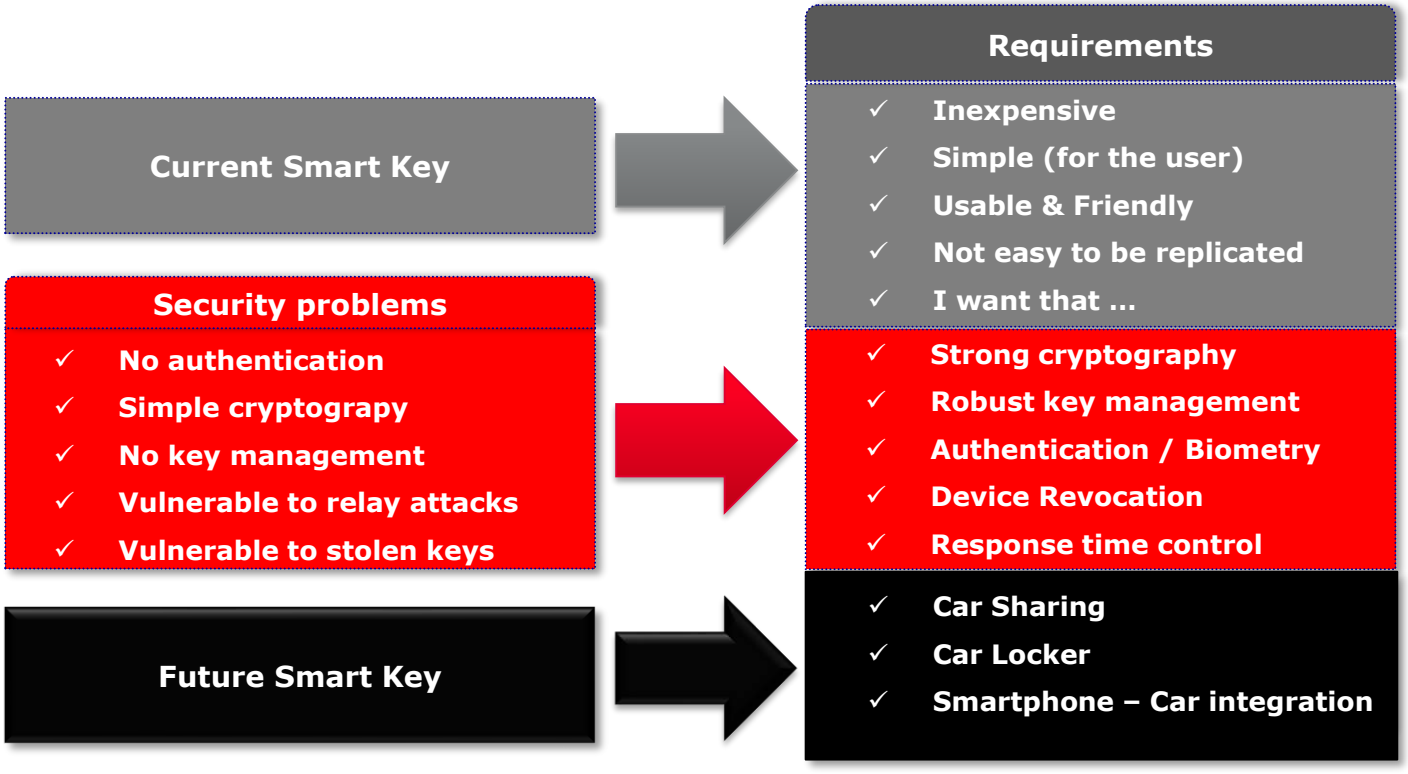
THREAT EVOLUTION



TESLA

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/

SECURE DIGITAL KEY



BMW?

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

LABORATORY

BUS-OFF ATACK

PARK ASSISTANT

GPS SPOOFING

MULTI-VECTOR ATTACKS

Local: Data filtering

Real Time: CANBUS Packet Inspection

Local: CAN interfaces

Remote: WiFi / Bluetooth

Remote: GPS

Real Time: Context Analysis

Local: Encryption

Local: Secure Channel

Local: Hardware Security Module (HSM) integration

Remote: GSM/3G

Local: Anti-Replay

Local: Trusted Software Validation

Remote: Applications

Cyber-Intelligence services

Local: WiFi / Bluetooth

Local: CA Certificate

Local: Anti-Tampering

Real Time: Zero days detection (based on behavior analysis)

Remote: Secure Hardening for connected services (Servers and Services)

Local: ECU & TCU (Secure Boot, Hardening, Trust Firmware Signature)

Local: Media infotainment (USBs, SD Cards)

THE FUTURE

THE FUTURE

PAY PER USE?

DENIAL OF SERVICE (DoS)

DISTRIBUTED DENIAL OF SERVICE (DDoS)

CYBERSECURITY FOR CAV

CYBERSECURITY PRODUCT SUITE

GMV Intrusion Detection and Prevention System

An IDS is a set of SW and/or HW components aimed to:

- monitor the traffic of a network
- raise an alert in case of malicious activities or anomalous behaviou
- record the identified intrusions

The IPS will prevent vulnerability exploits.

Secure Smart Key

- ✓ **Replaces key fob with an Smartphone.**
- ✓ **Biometry (fingerprint) as a second factor for authentication.**
- ✓ **Bluetooth LE (Low Energy) as transport layer**
- ✓ **NFC Card with Biometry as backup system**

www.gmv.com

Carlos Sahuquillo Pascual

Automotive CyberSecurity Consultant

@csahuqui on Twitter