TOWERSEC

AUTOMOTIVE CYBER SECURITY

# From vehicle cyber-attack to threats on Critical Infrastructure

**Asaf Atzmon, VP Business Development**

TowerSec proprietary. The contents shall not be copied, reproduced, changed or communicated to another - either in whole or in part.

# TOWERSEC Overview

**BUSINESS PROFILE**

Providing security solution to protect vehicles and related on-board components against hacking and intrusions.

**PRODUCTS**

ECUSHIELD

Ready to embed software solution for integration into ECUs, Smart Gateways and other CAN related systems

TCUSHIELD

Designed to be integrated in Telematics devices, IVIs, dongles and other after-market OBDII related products.

**ORGANIZATION**

Founded in 2012, TowerSec brings together Detroit's automotive industry's knowledge with Israeli Cyber Security experience.

Offices Ann Arbor, Michigan, Maryland, Berlin, Germany and an R&D center in Tel-Aviv, Israel

© TOWERSEC

- On July, 2015, two researchers (Miller/Valasek) have demonstrated a remote attack on a Jeep Cherokee taking control on critical functions of the car while the Wired journalist was driving it

# What is a Critical Infrastructure?

- “There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.” (www.dhs.gov)
- “**Critical infrastructure** is a term used by governments to describe assets that are essential for the functioning of a society and economy.” (Wikipedia)

Transportation Systems Sector

The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

# Attacks on Transportation Systems

© TOWERSEC

# Raptors Ahead! – Hacking into digital signage

Indiana, 2013 - Temporary road signs were hacking in 2013 with “Zombies Ahead”. Password for the signs was available online, posted by the vendor


June 2014 - overhead highway signs in multiple states simultaneously displayed “Hack by Sun Hacker”

# Hacking Traffic Control Lights

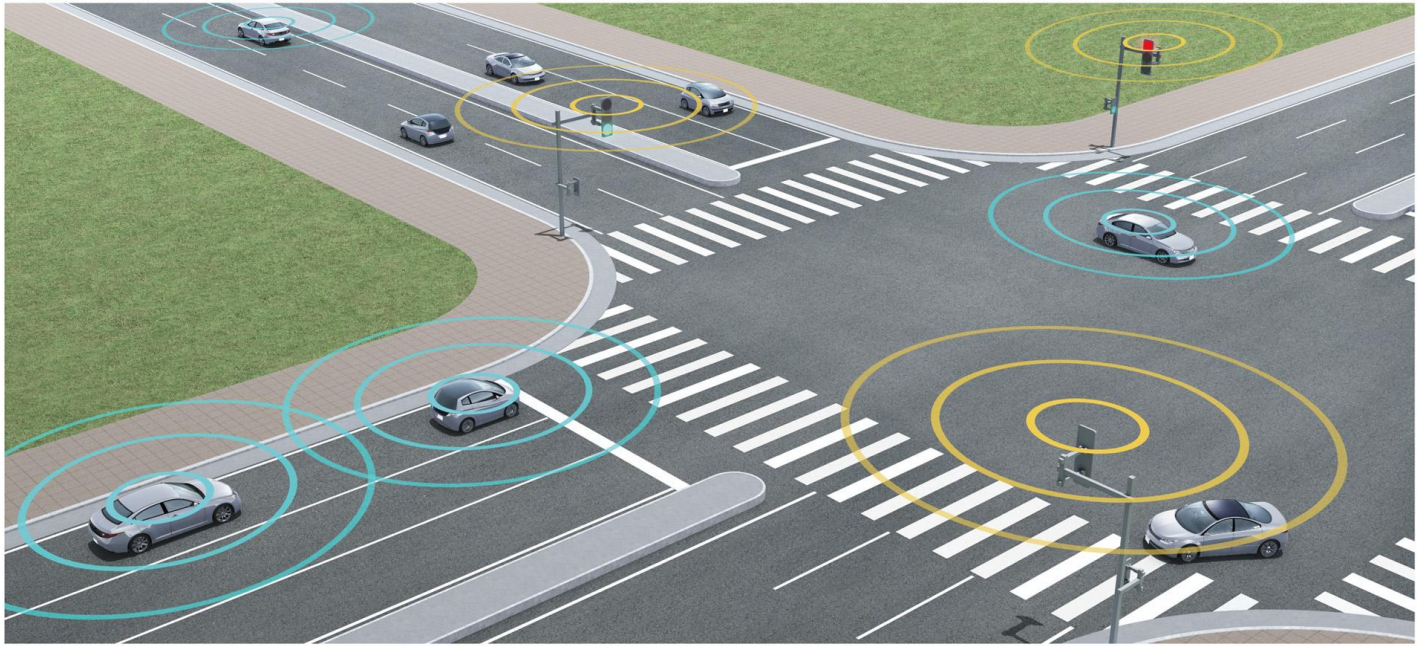
- 2014 / IO Active;  2015 / UMICH – escar europe
- The access point and receivers contain “no encryption at all
- firmware updates are neither encrypted nor signed
- no authentication of the signals.
- no encryption ; default username/passwords; password can’t be changed
- SSID is broadcast

- Attacker can do DOS, congestion (change

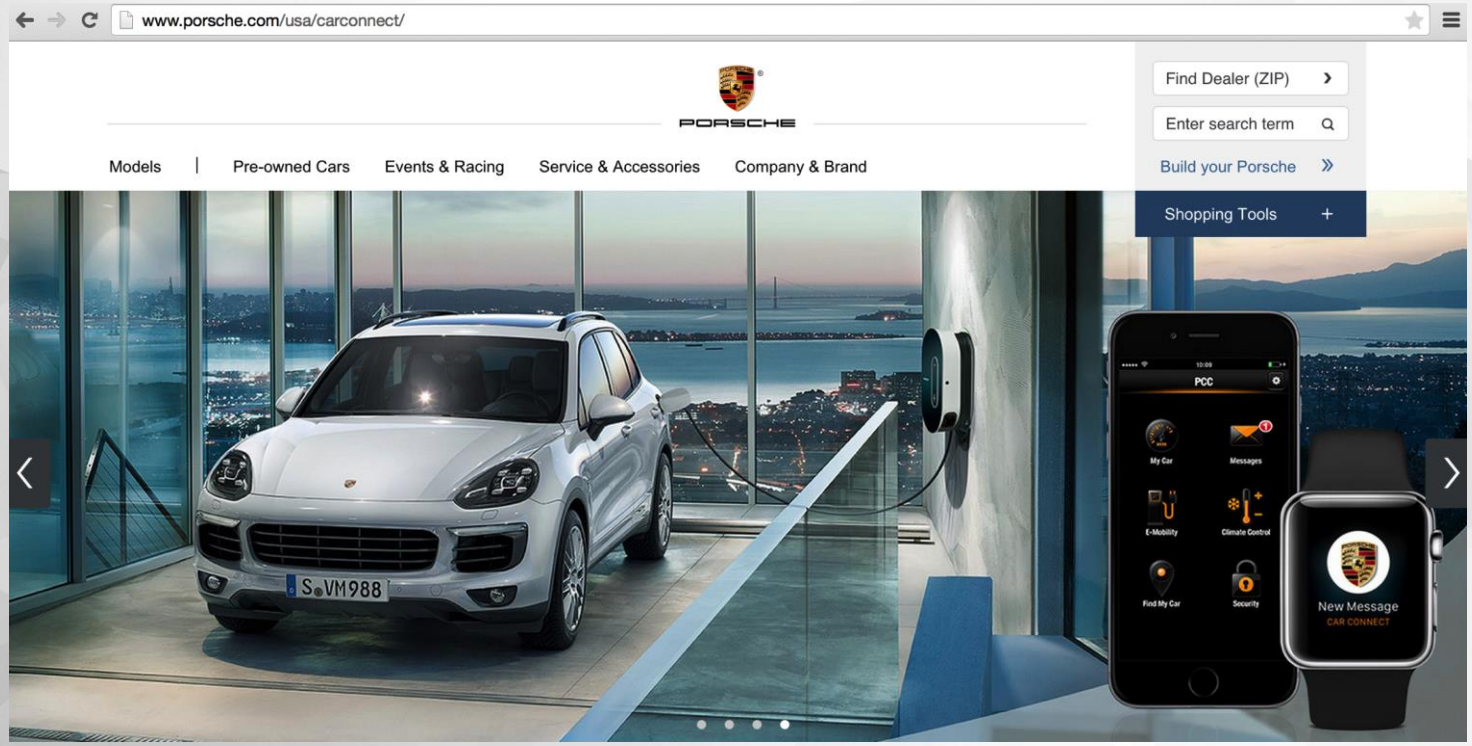
# Indirect attacks on ITS


Waze Attacked: Technion Students Create Traffic Jam Cyber Attack On GPS App

# V2x Misbehavior



# The vehicle is becoming Inter-connected



# The vehicle as a Trojan car

- For connected cars trojan car = especially interesting
- Ecosystem modern car connects to is ever growing

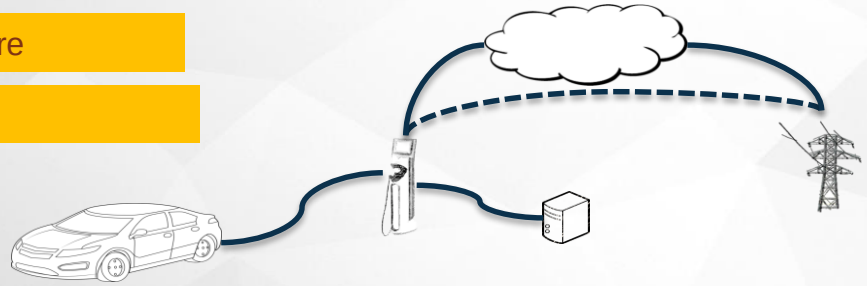
Transportation Infrastructure

Cellular Comm networks

Home Area Networks

Urban living services

EVs: Electric grids & payment systems



Telematics based Insurance

Smart Phones & watches

Payment gateways

Location based services

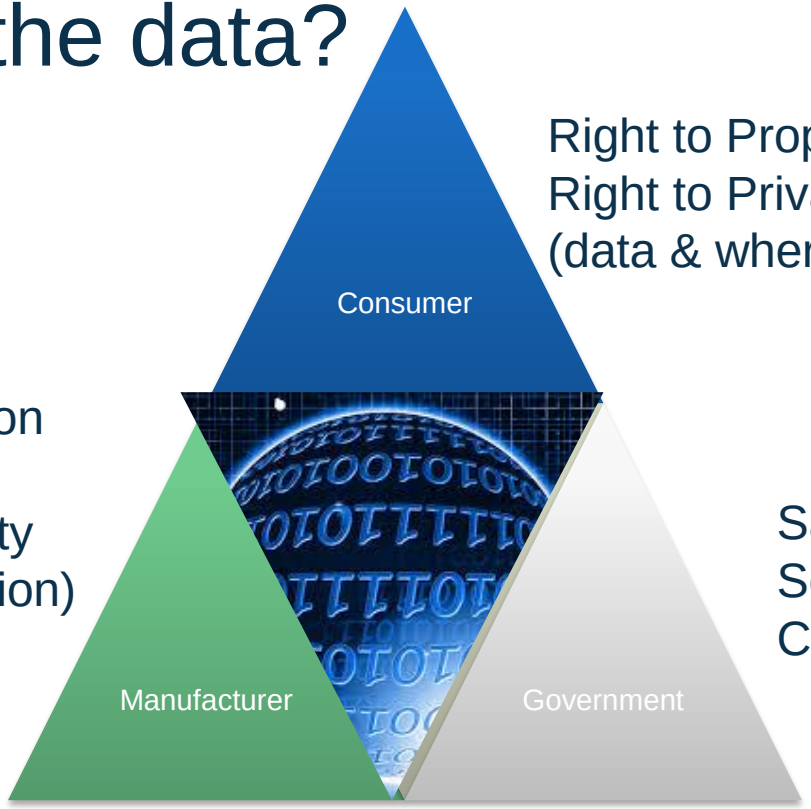
Other vehicles

# Data and Information Sharing

- Data plays a vital role in enabling future telematics services, as well as in monitoring and managing threats.
- Information sharing centers are common practice in some CI areas (e.g. Oil & Gas).
- Recently the Alliance of Automobile Manufacturers has granted BAH to build an automotive ISAC center to share incident data between different industry players.
- In the future, it is likely that ISACs of different CIs will be inter-connected s a way to address “mega-incidents”.

# Who owns the data?

Right to Property
Right to Privacy
(data & whereabouts)




Copyright Protection
(software & data)
Intellectual Property
(vis-à-vis competition)
Safety
Security

Safety
Security of
Critical Infrastructure

GM Says That While You May Own Your Car, It Owns The Software In It, Thanks To Copyright

Farmers can't legally fix their own John Deere tractors due to copyright laws

Automakers just lost the battle to stop you from hacking your car

*The vice grip on car software gets forcibly loosened*

Volkswagen hid a car hacking flaw for two years

# Conclusions

- ITS sub-systems should receive more focus on identifying and fixing security flaws.
- An holistic approach of threats and vulnerabilities assessment is desirable
- The vehicle presents a threat to ITS and other Cis
  - Through indirect attack (e.g. GPS spoofing`)
  - As a Trojan horse
- Data transparency and the “right to research” are critical for a greater security of vehicles and CI

TOWERSEC AUTOMOTIVE CYBER SECURITY

www.tower-sec.com | info@tower-sec.com