AUTHORS: Jose Ángel Gumiel Jon Mabe Jaime Jiménez Jon Barruetabeña

A Holistic Approach on Automotive Cybersecurity for Suppliers

Presenter: Jose Ángel Gumiel
Affiliation: Fundación Tekniker
E-mail: jagumiel@tekniker.es

Tekniker
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE

eman ta zabal zazu
Universidad del País Vasco Euskal Herriko Unibertsitatea

BATZ

IARIA

Curriculum Vitae

Jose Ángel Gumiel

HW Engineer & Ph.D. Student at Tekniker

I have a **B.Sc. in Informatics Engineering**, majoring in Computer Engineering, and a **M.Sc. in Advanced Electronic Systems**. I am currently **pursuing my Ph.D.** in Electronics and Communications, focusing on **automotive electronics** and its integration into mechanical systems.

I have been **working at Tekniker**, R&D center, since 2018. There I did my master's thesis, which was the development of a three-phase controller for a power converter on FPGA. During my stay, I also participated in projects that required **analysis and application of cybersecurity** techniques for encryption of communication protocols and sensitive data.

I started my Ph.D. at the end of 2019. Since then, I have been in **constant cooperation with BATZ**, a TIER 1 automotive supplier. Part of their business is pedals and active aerodynamics. Since 2022, the relationship has grown closer as **I partially work there** and I have learned first hand the problems that TIER 1 and OEMs face.

A Holistic Approach on Automotive Cybersecurity for Suppliers

Introduction

Brief analysis of the automotive sector, its disruptions and challenges.

Safety & Security

Differences between safety and security, with particular emphasis on the role of ISO standards in improving both aspects.

Focus on Cybersecurity

Where must be cybersecurity ensured?
There are a several areas where must be present: Office environment, product development, testing department, production line…

The Aging of the Connected Vehicle: Cybersecurity Concerns

The vehicle should be cybersecure throughout its lifetime. What will be the future of the connected vehicle?

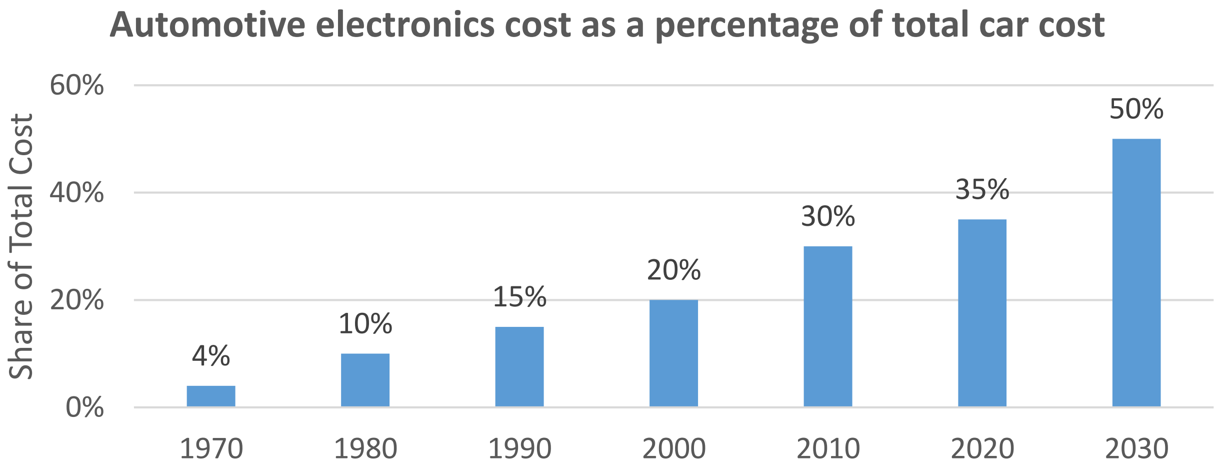
Conclusions and Future Work

Summary of key findings and suggestions for future practice.

INTRODUCTION

Electronization

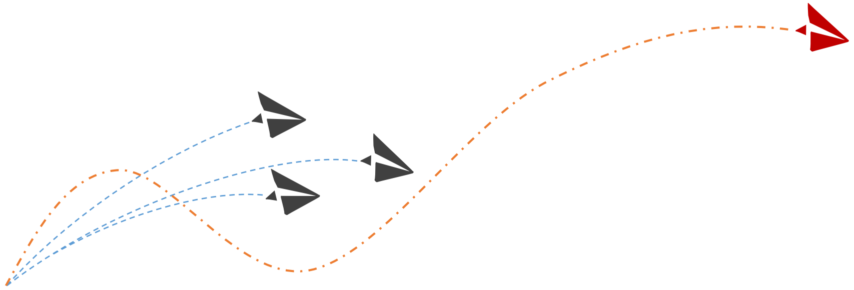
- Automobiles have become computers on wheels.
- 90% of the technological innovation in vehicles is electronic .
- 30% of the total vehicle cost is electronics.



Automotive electronics cost as a percentage of total car cost

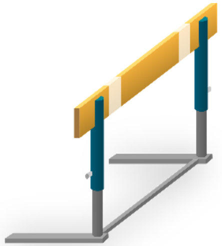
Disruption

- Electronics is a big challenge for traditional suppliers.
- New competitors enter the market.
- Electronics is an opportunity to create high value-added products and differentiate from commodities.
- Traditional suppliers benefit from being trusted by OEMs and having a large mechanical footprint.
- TIER 1s need to start designing mechatronic parts.

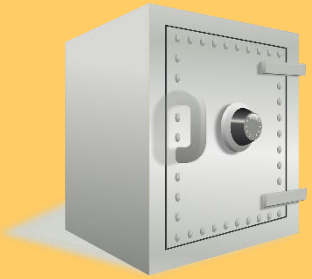


Challenges

- Mechatronic parts present new challenges.
- Smart components need to communicate:
  - *In-vehicle protocols must be secure.*
  - *Data must not be compromised.*
- But… How to design cybersecure products? What will be the impact on the organization? And what happens as the vehicle ages?



SAFETY & SECURITY



SAFETY (ISO 26262)

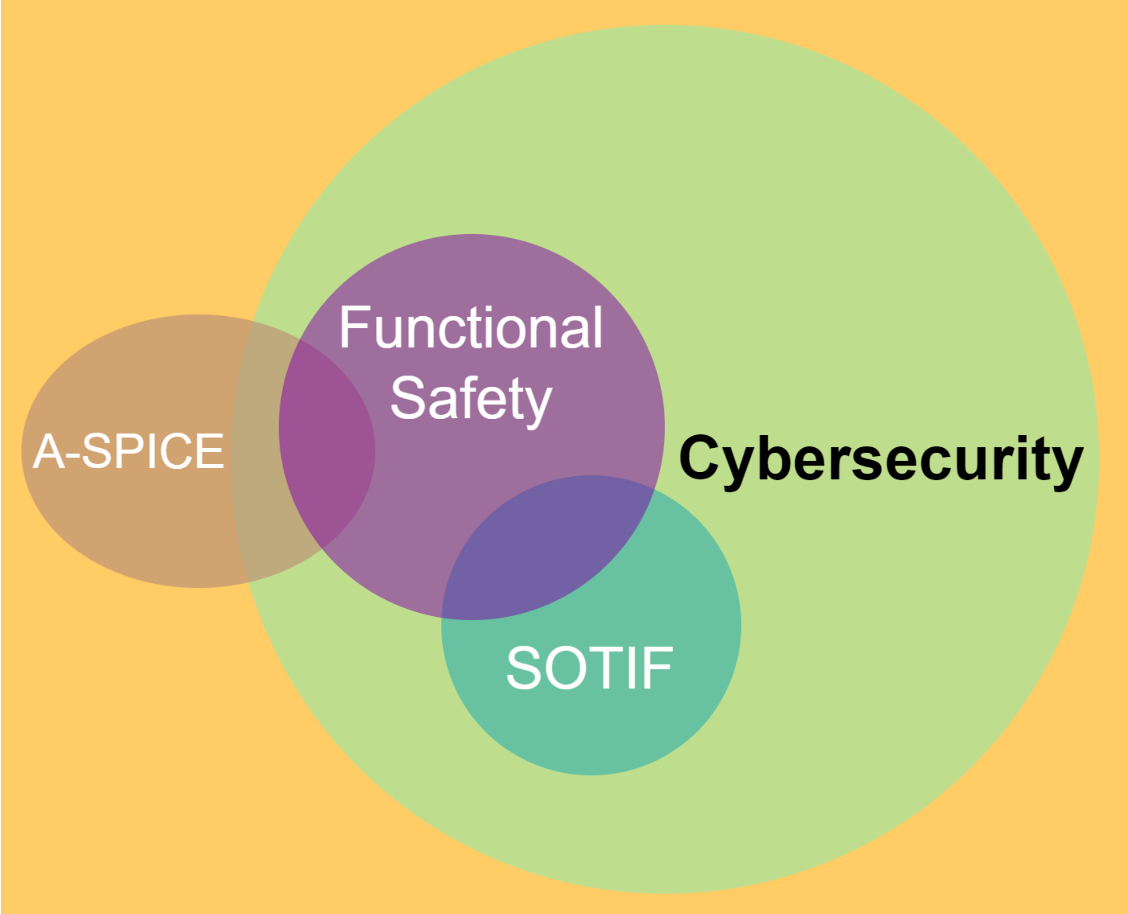
- Focuses on identifying hazards and controlling associated risks.
- Concerned with preventing accidents, injuries or fatalities.
- Addresses FuSa requirements for E/E systems in vehicles.
- Emphasizes robust safety processes throughout the development lifecycle.
- Requires a safety management system in the organization.

SECURITY (ISO/SAE 21434)

- Focuses on identifying potential threats and vulnerabilities, implementing measures to mitigate them.
- Focused on protecting the vehicle and occupants from unauthorized access, theft or malicious attack.
- Emphasizes a systematic and risk-based approach to security.
- Addresses the entire lifecycle: From design to decommission.
- Requires a security management system in the organization.

Cybersecurity is all-encompassing

A vehicle cannot be safe if it is not secure.



Focus on Cybersecurity

CYBERSECURITY

MORE THAN YOU MIGHT THINK

Academia is already aware about security, but…

- TIER 1s are unaware of the implications and costs of adopting the concept of cybersecurity.
- OEMs don't seem to be convinced either, sometimes sharing specifications that are vague or too strict for the part's category.

CYBERSECURITY

MORE THAN YOU MIGHT THINK

Cybersecurity is a holistic concept and includes...

- Office Environment
- Project Development
- Testing Department
- Production Line
- Vehicle & Beyond

Cyb-Sec at the Office

The importance of protecting the working environment:

- OEMs & Suppliers share sensitive information.
- Business must continue.
- A cyberattack could affect company’s reputation.
- Projects timelines are tight.

Cyb-Sec at the Office

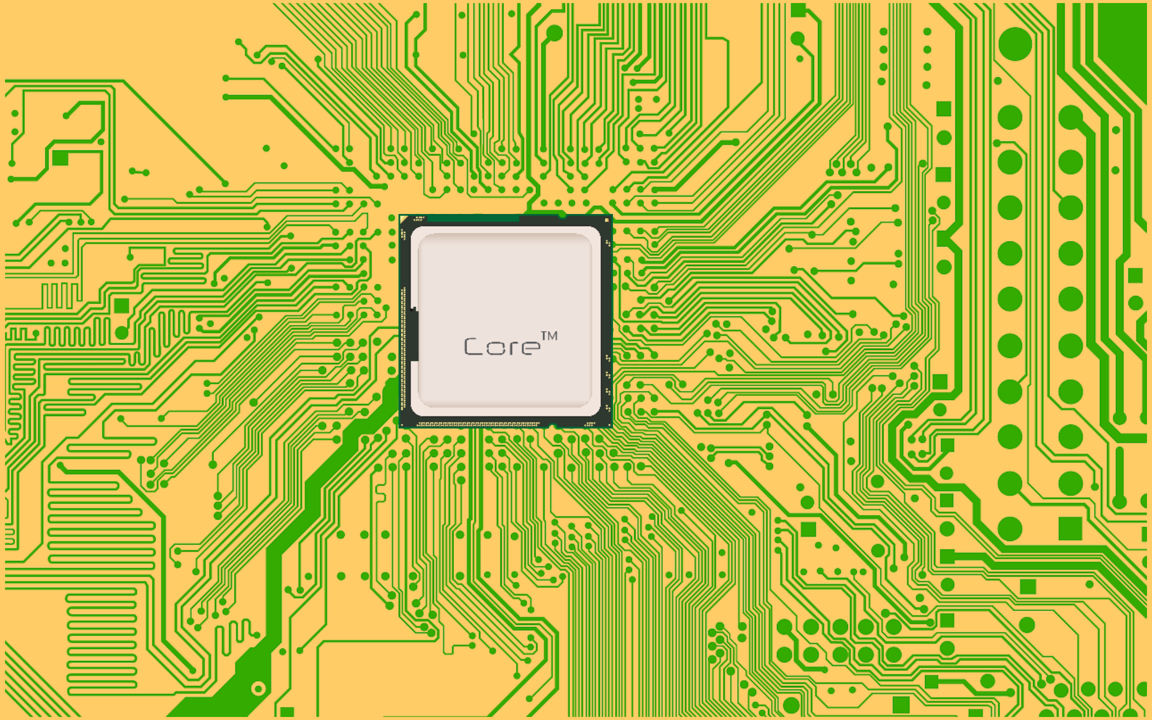
Some measures to implement:

- Access Control at the company entrance.
- Security as a culture. Education.

Cyb-Sec at the Office

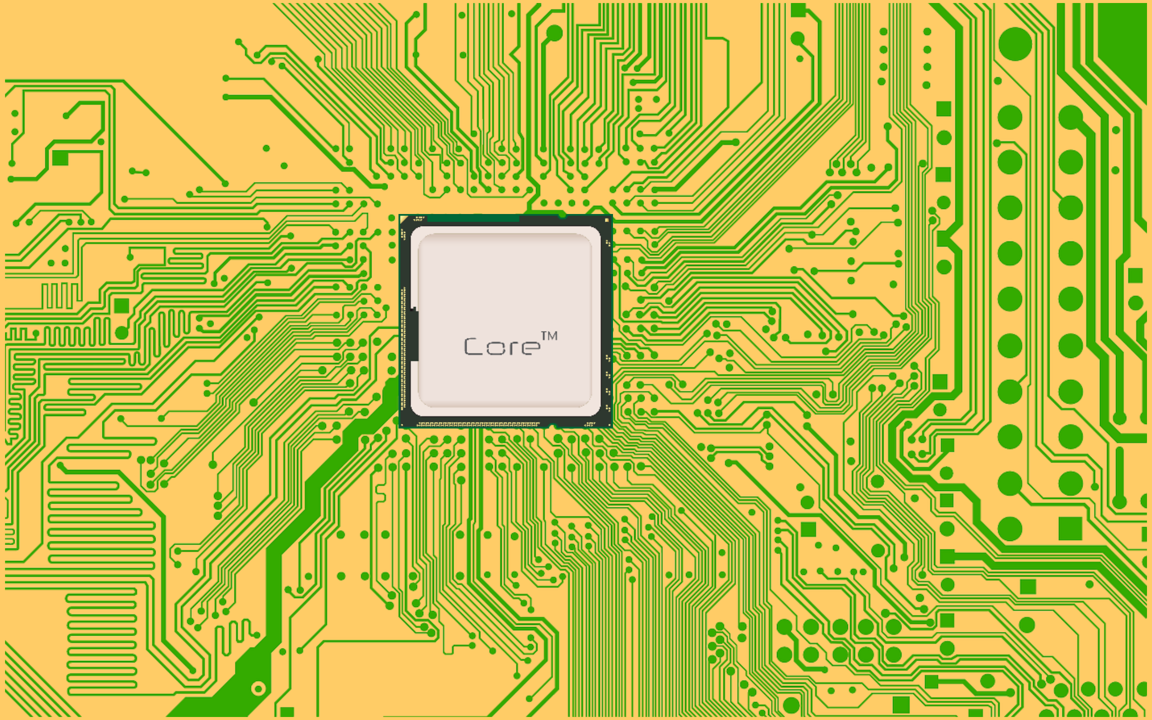
Some measures to implement:

- Network Segmentation.
- Firewall.
- Demilitarized Zone (DMZ).
- Virtual Private Network (VPN)
- Secure Information Access and Version Control.
- Updated Software.



Cyb-Sec at the Dev. Phase

- OEMs are asking for ISO 21434.
- TIER 1s are being responsible for security.
- Implementation similar to ISO 26262.
- Applies to the entire product lifecycle.
- Component understood as a system.

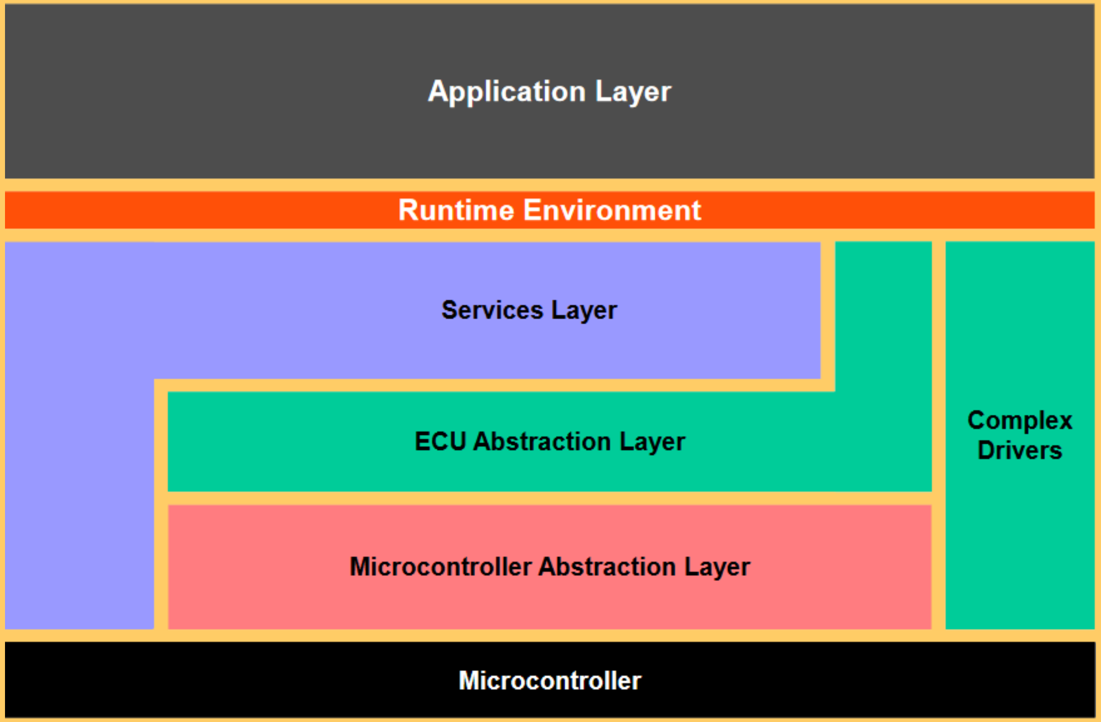


Cyb-Sec at the Dev. Phase

CONCEPT DEFINITION

Details the system requirements:

1. Define the item, operational environment, and its interaction with other items.
2. Specify cybersecurity goals and claims.
3. Specify cybersecurity requirements.



* **AUTOSAR Architecture.** Even if not developing an AUTOSAR-compliant project, this architecture can be taken into account for modular development.

Cyb-Sec at the Dev. Phase

PRODUCT DEVELOPMENT

Some considerations:

- Is the protocol secure for the application?
- Is a Trusted Platform Module (TPM) needed?
- SW Eng: Modularity, Abstraction, Layering, Process Isolation, Domain Separation…
- EEPROM must be lockable.

Cyb-Sec at the Dev. Phase

CYBERSECURITY VALIDATION

Some considerations:

- Penetration Tests.
- Vulnerability Scans.
- Security Scans.
- Communication Analysis:
  - Interruption, impersonation, repudiation, man-in-the-middle- eavesdropping, spoofing, data manipulation…

Ethical Hacking

To defeat hackers, you must become one.

In the fight against hackers, knowledge is power. By **understanding the techniques and tactics attackers use**, you can better defend against them.

Ethical hacking, also known as penetration testing, is an important part of the cybersecurity landscape. By **simulating attacks against your own systems**, you can identify and fix vulnerabilities before they can be exploited by real attackers.

With cyber threats constantly evolving, a proactive approach to cybersecurity is essential.

Cyb-Sec at the Dev. Phase

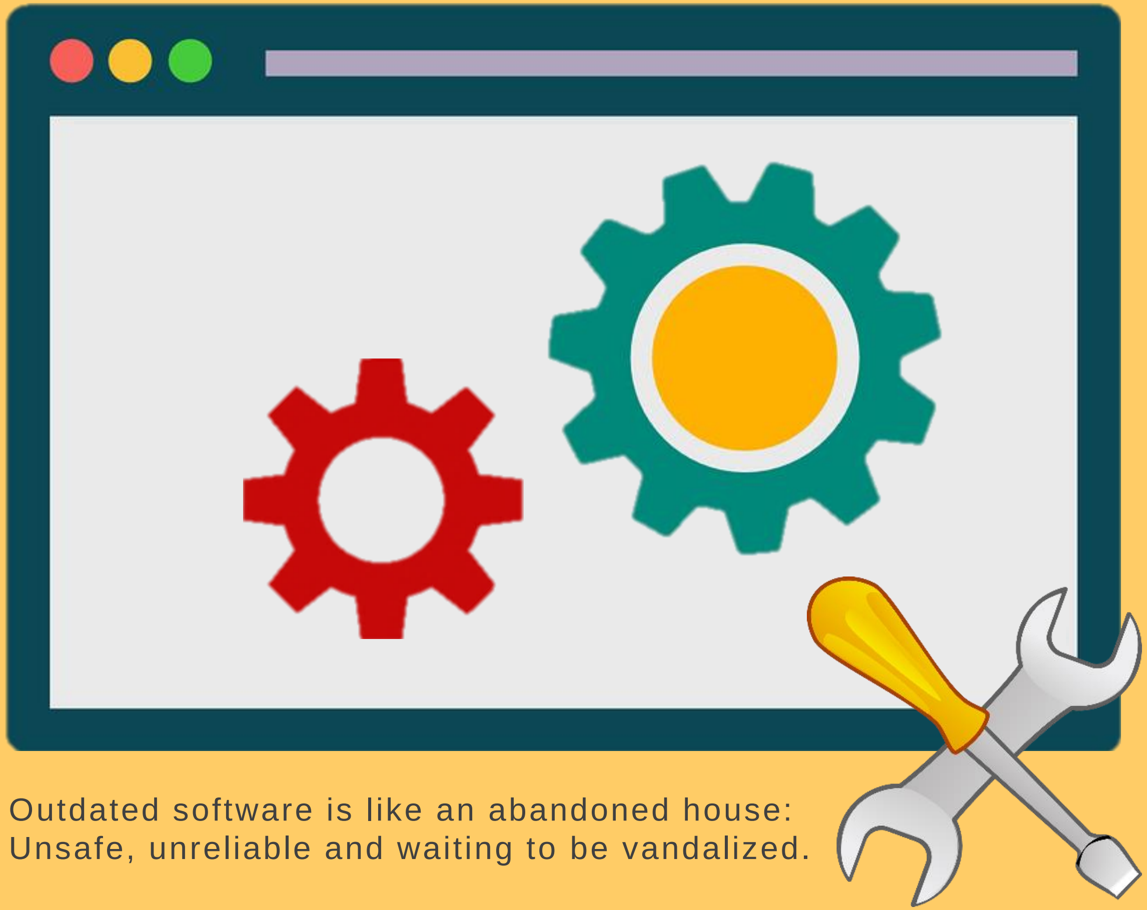
PRODUCT MAINTENANCE

Aging is a problem:

- Hackers acquire more knowledge.
- More vulnerabilities are discovered.

Updates prevent premature aging:

- Over-The-Air Updates.
- Bugs get fixed.
- Secure online SW updates.



Outdated software is like an abandoned house:
Unsafe, unreliable and waiting to be vandalized.

Cyb-Sec at the Testing Dept.

Prototypes and products are tested in the testing department. They manage sensitive information.

- The testing department must be protected with high walls and controlled access.
- Photographs are not allowed.
- Sensitive data must be protected.
- Network may be isolated.

Cyb-Sec at the Production Line

The production line is the last link in the supplier's chain before the part reaches the vehicle.

Nowadays, they are highly-automated and connected, so they must be secured.

Some measures to mitigate risks:

- Secure the access to the production line.
- Double verification. Check that the FW or calibration parameters have been recorded correctly.
- Lock the EEPROM and verify.

Cybersecurity in the Vehicle

The vehicle must be secure. These are some considerations to protect the electronic systems:

- Secure Boot.
- IDPS.
- Communication Encryption.
- NFT & Blockchain.

What can an attacker do on a connected vehicle?

Charlie Miller and Chris Valasek explained at the Black Hat Conference how they hacked a connected vehicle.

They showed a reporter from Wired magazine what actions they could perform on a moving vehicle remotely.

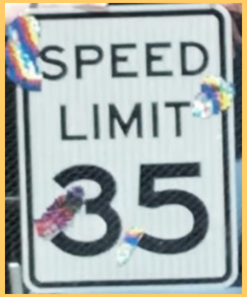
These are some of them

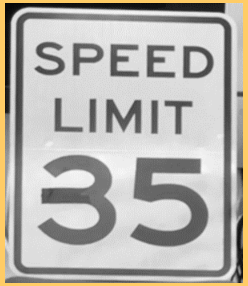
- Accessing to the infotainment (and annoying the driver).
- Operating the windshield wipers.
- Turning off the engine
- Manipulating the brakes.

Beyond the Vehicle

AND IF I TOLD YOU THAT THE ENVIRONMENT CAN ALSO BE HACKED?

Sabotaged Traffic Signal:

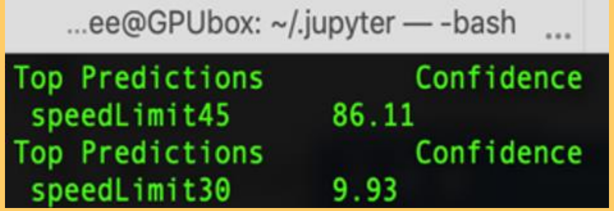




Vehicle Interpretation:

SPEED
LIMIT
45

SPEED
LIMIT
85



```
...ee@GPUbox: ~/.jupyter — -bash
Top Predictions            Confidence
 speedLimit45         86.11
Top Predictions            Confidence
 speedLimit30         9.93
```

- Traffic signals can be sabotaged using aluminum foil (left) or electrical tape.
- The worst case is shown on the left.
  - Even a small black tape can mislead the vehicle's signal recognition system.
  - A vehicle with Traffic Aware Cruise Control (TACC) will accelerate after identifying the signal.
  - Although the machine is wrong, the human eye would still see a 35 mph signal.

Beyond the Vehicle

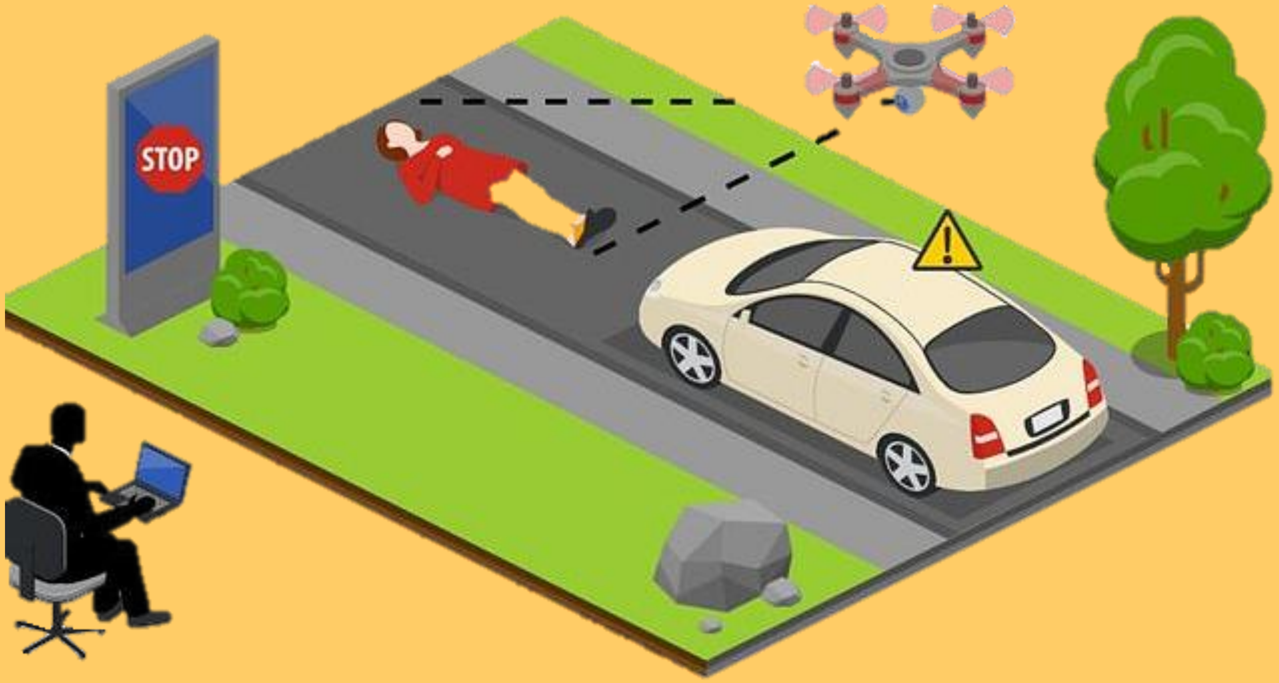
AND IF I TOLD YOU THAT THE ENVIRONMENT CAN ALSO BE HACKED?

This is the “Phantom Attack”.

An image is projected on the road. The vehicle could misinterpret this.

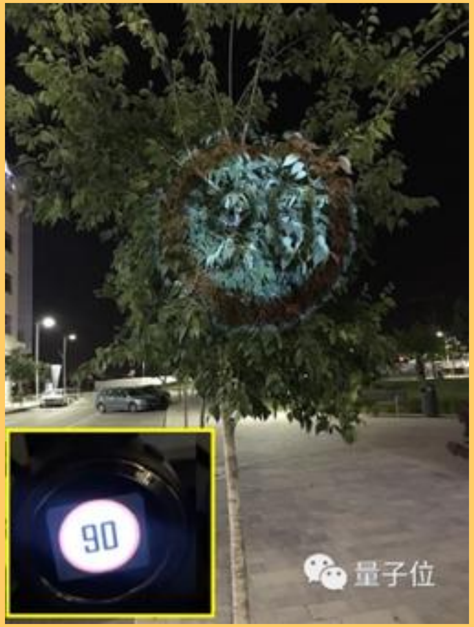
List of projections:

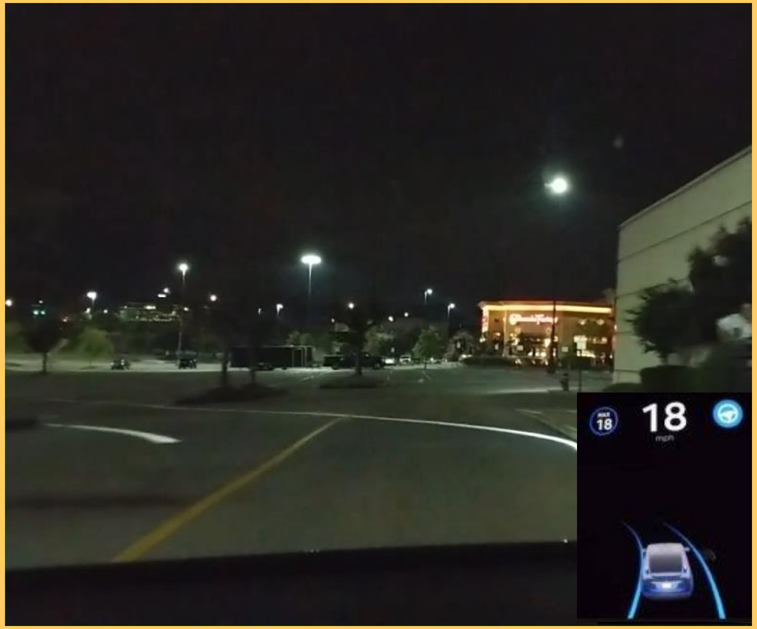
- Traffic signals.
- Fake road lines.
- Human images.

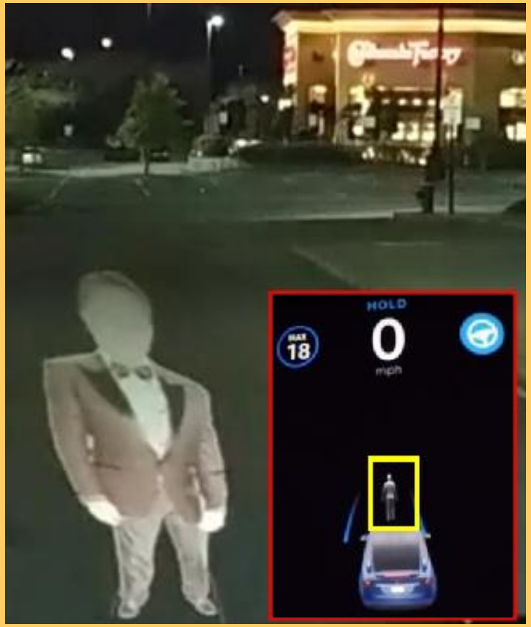


Beyond the Vehicle

AND IF I TOLD YOU THAT THE ENVIRONMENT CAN ALSO BE HACKED?







Signal Projection

A 90mph sign is projected onto a tree. The vehicle identifies it.

Lane Projection

A false lane is projected on the road. The vehicle recognizes a curve.

Human Projection

A human silhouette is projected on the road. The vehicle detects a pedestrian.

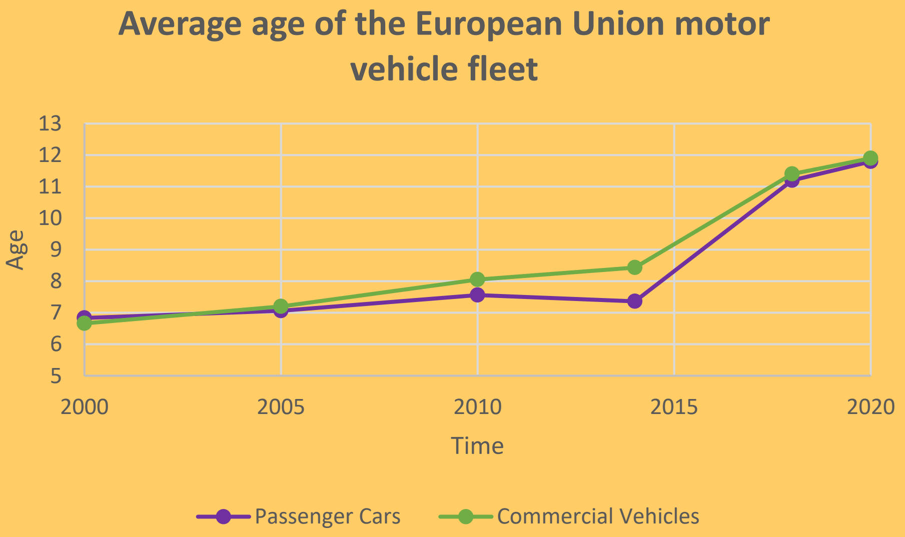
VEHICULAR 2023

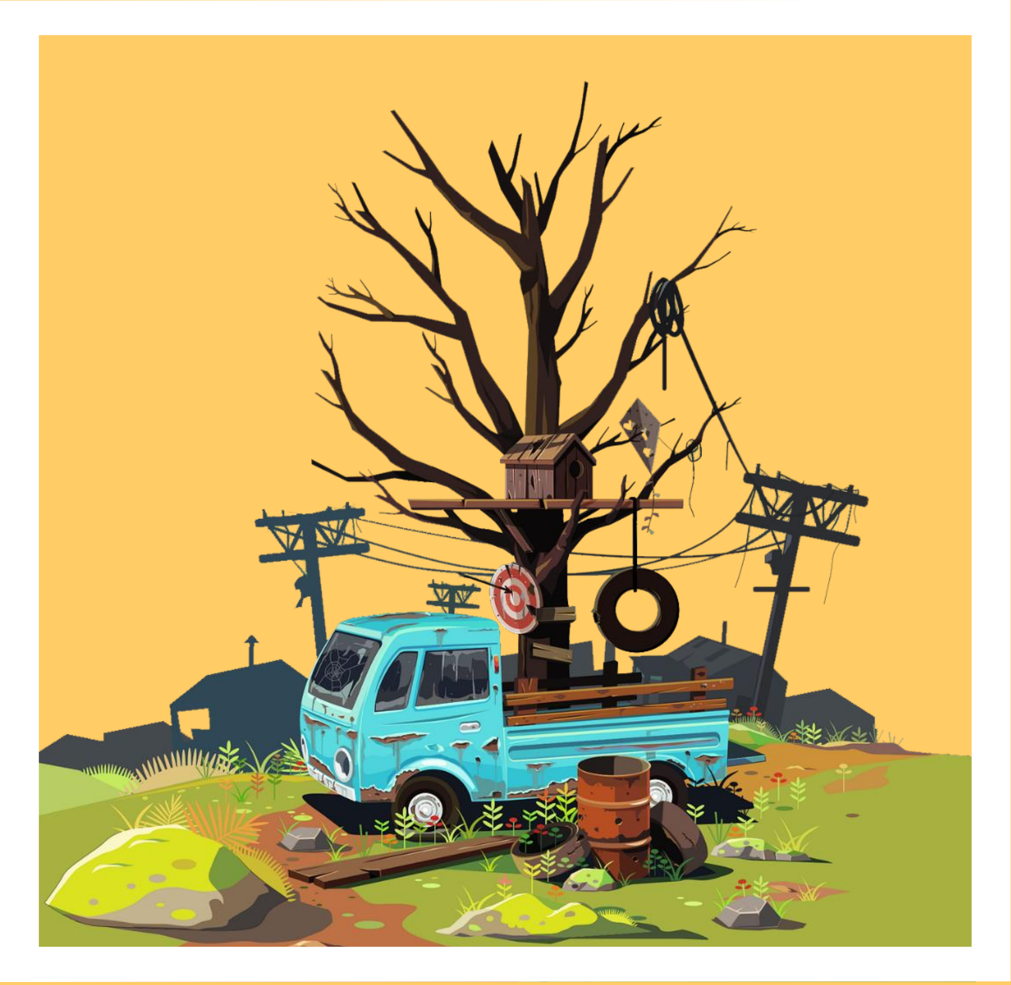
THE AGING OF THE CONNECTED VEHICLE:

CYBERSECURITY CONCERNS

Current Scenario

- The average age of the European fleet is 12 years.
- Older cars lack connectivity, which means fewer potential threats.
- We expect more than 400 million connected vehicles by 2025.
  What will happen as they age?





Connected Future

The future brings new challenges.

- Each vehicle will generate more than 25GB/h.
- Connectivity will provide services that must be secured.
  - i.e. OTA SW Updates, V2X, Shared Mobility, Smart Recharge or information about the vehicle status (battery, refueling, last parking, next service…).
- Electric Vehicle and Charging Station are also critical. Vulnerabilities have been identified that could affect the vehicle and the power grid.
- Over time, new vulnerabilities will emerge. If they are not fixed, the vehicle’s security will be compromised, and so will safety.
- Security updates will be needed to protect the vehicle and the personal information of its occupants.

Conclusions & Future Work

Conclusions

- Security is a hot topic in the automotive industry as we move closer to the connected vehicle.
- OEMs and TIER 1 have a certain lack of knowledge and sometimes misunderstand the requirements.
- Both must become aware and move forward together on this path of knowledge.

Future Work

- Although cybersecurity is a hot topic in academia, it has yet to be adopted by the automotive industry.
- The connected vehicle and its presence in the Smart Grid will bring a new set of challenges.
- Security must accompany the vehicle throughout its life.
  - What happens as the vehicle ages?
  - How long will OEM and TIER 1 support last?

AUTHORS: Jose Ángel Gumiel Jon Mabe Jaime Jiménez Jon Barruetabeña

A Holistic Approach on Automotive Cybersecurity for Suppliers

THANKS

Tekniker
MEMBER OF BASQUE RESEARCH
& TECHNOLOGY ALLIANCE

eman ta zabal zazu
Universidad
del País Vasco
Euskal Herriko
Unibertsitatea

BATZ

IARIA