DEKRA Testing and Certification

Cyber Security for the Automotive

Embedded Software Engineering Kongress

The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard

Posted on: August 16, 2017 at 5:00 am **Posted in:** Exploits, Internet of Things
Author: Federico Maggi (Senior Threat Researcher)

2

In many instances, researchers and engineers have found ways to hack into modern, internet-capable cars, as has been documented and reported several times. One famous example is the Chrysler Jeep hack that researchers Charlie Miller and Chris Valasek discovered. This hack and those that have come before it have r
makes a
vulnerab
security
only suc
performa
vendor r

Team of hackers take remote control of Tesla Model S from 12 miles away

Chinese researchers were able to interfere with the car's brakes, door locks and other electronic features, demonstrating an attack that could cause havoc

ANDY GREENBERG SECURITY 07.21.15 08:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

WIRED TECH

HACKERS NOW ABLE TO TAKE CONTROL OF CARS TO CAUSE DELIBERATE ACCIDENTS, SCIENTISTS WARN

Challenges in automotive cyber security evaluation

Regulations are in early stages of consideration.

Each car manufacturer and supplier is used to define its own internal performance standards, and homologation processes do not cover cyber security yet.

BUT the need to have **assurance on the security of the devices embedded in the car** is here, and will be key to market success.

5 Myths in Automotive Cybersecurity

1

The Myth:

Hacking is not a real world problem, its only researchers creating publicity

5 Myths in Automotive Cyber security

1

WRONG

Organized Car crime Groups are already using reverse engineering methods

Hardware Based	Software Based	Network based
Clone cards	Firmware Analysis	Diagnostic Manipulation
PCB By-pass	Input & Output Monitoring	Bus Injection (Fuzzing)

Secrecy is not Security

5 Myths in Automotive Cyber security

DEKRA

2

The Myth:

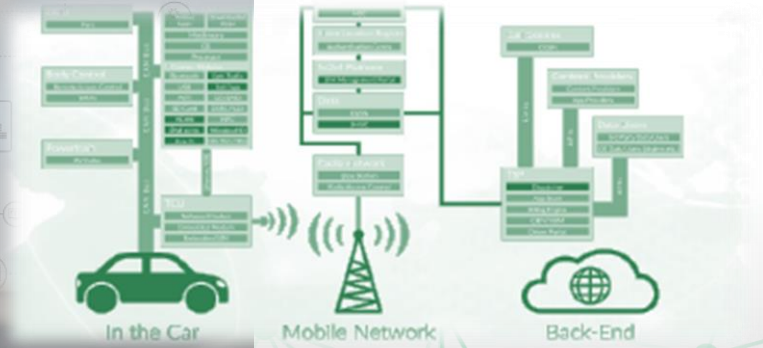
Hacking only affects to some components of “cars”

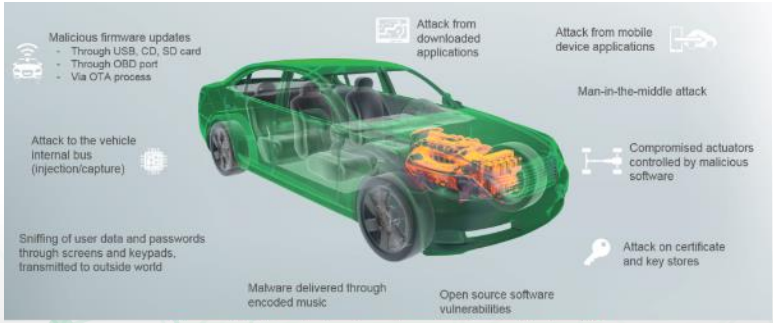
5 Myths in Automotive Cyber security

2

Wrong:

There are over 50 attacks points in the eco system of a connected vehicle





Any part of the electronic system can be an attack point

5 Myths in Automotive Cyber security

3

The Myth:

The OEMs are only responsible for their cars, they cannot be responsible for all their suppliers and partners

5 Myths in Automotive Cyber security

3

Wrong:

The customer only ever sees the vehicle brand

Chrysler Jeep Example (August 2015)

Good argument to say Harman (HeadUnit) and Sprint (TSP) were liable…

But only FIAT-Chrysler made the headlines

The quality of your (supplier) code is now the quality of your Brand !

5 Myths in Automotive Cyber security

4

The Myth:

OEMs can not justify the costs to support a cyber security program without specific legislation, regulations or detailed market requirements

5 Myths in Automotive Cyber security

4

Wrong:

"Do nothing" is not a viable alternative

The cost doing nothing:

To be out of the business

The Institute of the Motor Industry (IMI) security risks of today's 'connected' vehicles. https://www.theimi.org.uk/

5 Myths in Automotive Cyber security

5

The Myth:

Hacking is a technical problem, so it needs a technical solution

5 Myths in Automotive Cyber security

5

Wrong:

It is also a business problem that needs a business solution

- Security requirements in development life cycle for all OEMS
- Security standards for process and products in all stakeholders facilities
- Regulatory security requirements
- Security testing in homologation process
- Pen-testing as part of product development
- Data privacy regulation
- Etc.

Do no think what you vehicle can do for you…
Think about what you can do for the Security of your vehicle

What we do

We offer product cyber security evaluations for the whole product lifecycle

Product development

Final product

Product maintenance

Product development and prototypes

- Vulnerability assessment
- Penetration testing

Final product

- Certification
  - ISO 15408/Common Criteria
  - FIPS 140-2/ISO 19790
  - IEC 62443

Product maintenance

- Security evaluation and certification other product release
- Early Warning Alert System

Cyber Security Services

Penetration Test I

Due to the number and variety of interfaces avaliable to the ECUs, there is the possibility of unauthorized access by malicious attackers, on these kind of devices, with the purpose to compromise the entire vehicle via specific vectors of attack.

Therefore penetration tests needs to take place, this testing plan should be along a risk assessment procedure in order to test their potential risk and the importance of the protected data. This means that the tests with the highest priority are usually done at the beginning of the evaluation. We can define the priority, as follows:

- Interfaces with the highest probability of attack
- Highest potential of damage to device or vehicle
- Sensitive data to be protected

Cyber Security Services

Penetration Test II

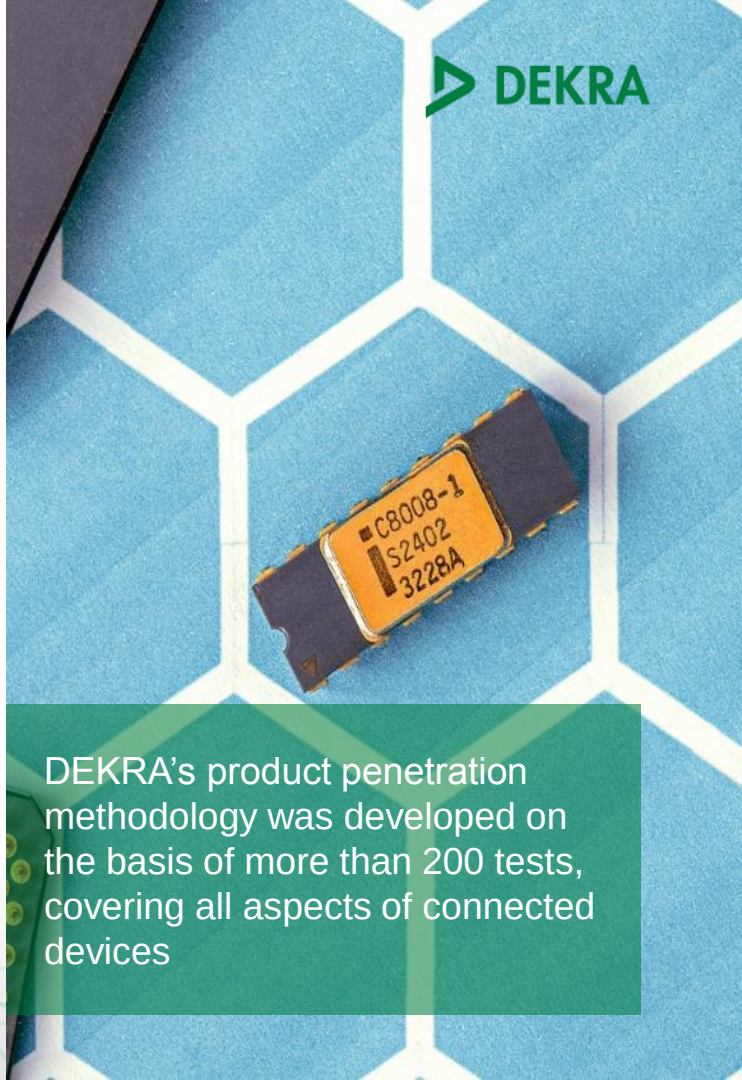
The following tests are usually performed for ECUs:

- Test of radio based interfaces:
  - WIFI
  - GSM
  - BLE/BLUETOOTH
  - Others
- Test of locally avaliable interfaces:
  - JTAG/UART
  - CAN
  - USB
  - Others
- Test with shell access:
  - Known software vulnerabilities
- Test without shell access:
  - Booting process
  - FOTA (update procedure)
  - Hardening

Cyber Security Services

Penetration Test III

- Tests with wired interfaces:
  - Test reponses via USB, CAN, UART…etc.
  - Test if device sensitive information regarding device is readable
  - Test if any read/write access is possible
- Test with software
  - Test if SW of device can be read out (debugging) and executed on external devices
  - Test if SW can be manipulated
  - Test if SW update packages can be manipulated
  - Test if SW update packages are signed or correctly verified
  - Test if SW components/libraries are outdated
- Test private data
  - Test if sensitive data can be extracted from ECU
    - Public certificates, keys…etc.
  - Test if sensitive data can be manipulated



DEKRA's product penetration methodology was developed on the basis of more than 200 tests, covering all aspects of connected devices

Cyber Security Services

Penetration Test IV

- Tests boot process
  - Test if any boot mode can be manipulated
  - Test if boot can be interrupted to cause unexpected behaviour
  - Test if is possible to modify internal memory partitions
  - Test if security mechanisms can be bypassed successfully
- Test backend
  - Test possible MiTM attacks
- Test possible apps
  - Test possible vulnerabilities in mobile app if exist

In conclusion, automotive assessment is inherently more complicated than the traditional one because more hardware, software and communication protocols are involved. This means that a larger attack surface and wider array of attack vectors during the evaluation may be considered. One of the key differences between traditional and Automotive penetration tests is related to the diversity in the Automotive world (different architectures, operating systems, communication protocols, etc.) that require new expertise and tools to test them.

Cyber Security Evaluation and Certification

Common Criteria, ISO/IEC 15408

- Products are evaluated by competent and independent licensed laboratories to determine the fulfillment of particular security properties:
  - 7 evaluation assurance levels and specific protection profiles for different types of products

NIST FIPS 140-2, ISO/IEC 19790

- Security requirements for cryptographic modules
- Conformity assessment of cryptographic algorithm implementations.

IECEE CB Cyber Security Certification

- DEKRA tests and assesses against the IEC 62443 series of standards

Achilles

- DEKRA provides you with the industry-leading benchmark for communication robustness

3GPP Accredited for MME devices

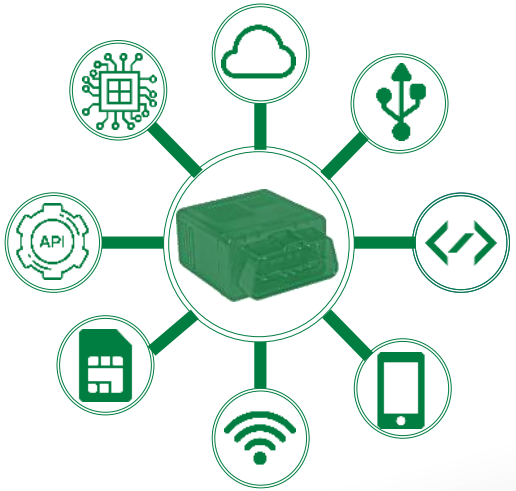
- Conformance test and functional security evaluation for MME devices: 3GPP TR33.916, TR33.116, TR33.117


Examples

Objective of the project

Example Request

- Customer is developing a new **integrated dongle** device with the following features:
  - Supports CANbus / LINbus , Bluetooth LE 4.0, GSM/GPRS& GPS
  - Data exchange between dongle, vehicle, mobile device and Cloud
  - Android and iOS applications
- Customer requested us to perform **a Black Box Security Evaluation** of the dongle device



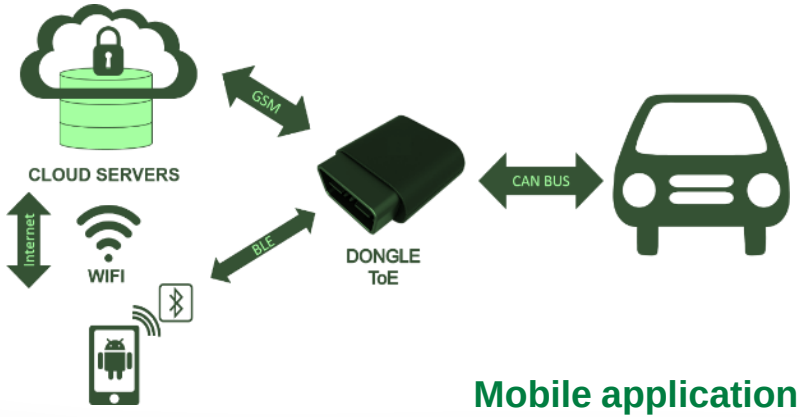
Project objective

- Evaluate the product and services developed by supplier to identify potential vulnerabilities or security risks in devices and the data managed in services.
- The evaluation covers:
  - The embedded hardware and software
  - The communication protocols between the vehicle, device, cloud and the mobile device
  - The Android mobile application (front-end)
  - The cloud services (backend)

Example Ecosystem - Definition

Cloud services: This component implements an interface for the dongle and mobile application to send and receive information.

Dongle: This component communicates the car with cloud services and with the mobile application. Its purpose is to monitor the car in order to give useful information to users.



Mobile application: This component manages the interaction between the user and the hardware components and cloud services.

Example Penetration Test Evaluation Areas

Firmware Analysis

- File system analysis
- Identification well-known vulnerabilities
- Malware analysis
- Reverse engineering
- Firmware extraction
- Command Line Interface
- Finding and exploiting logic flaws
- Extracting and running binaries
- Bypassing stack protections
- Firmware modification/persistance

Software Analysis

- Static code analysis
- Dynamic code analysis.
- Finding code security Vulnerabilities

Mobile App Assessment

- Obfuscation
- Secure communications
- Insecure data storage
- Information disclosure
- Malware code
- Unnecessary permissions

Communication Protocol assessment

- Wired-based Network
  - Ethernet
  - USB, etc.
- Wireless-based Network
  - Wi-Fi
  - Bluetooth
  - ZigBee
  - Proprietary and custom protocols

Updating Mechanics

- Encrypted channel
- Missing update mechanism
- Early end-of-life
- Update must be signed
- Non-official updates in the wild

Hardware Analysis

- Attack hardware Interfaces
- Identify vulnerabilities
- Debug ports
- Reset to insecure state
- Tamper resistance

Vulnerability template

Description

The following slides shows main findings and vulnerabilities identified in the evaluation

Each Vulnerability is composed by:

- Risk Description
- Severity Level according to CVSS v3.0 and Vulnerability Classification
- Evaluation Area

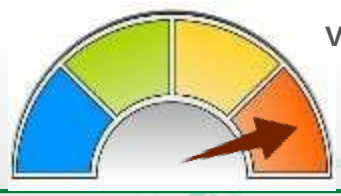
Risk Description

Threat Description: Brief explanation of the vulnerability or threat identified and the potential exploitation

Potential Impact: Brief explanation of the attack scope of the potential impact for the customer

Security Level

- Critical
- High
- Medium
- Low



Vulnerability Classification

- Confirmed
- Potential
- Informative

Affected component

- Evaluation area where vulnerability has been identified

FINDING: Sniffing Bluetooth communications

RISK DESCRIPTION

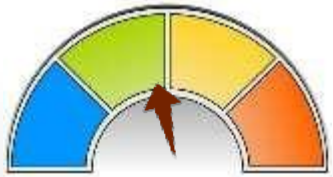
Threat Description: Unencrypted Bluetooth communication protocol is used for communication between dongle and the mobile application. The information could be accessible and readable in clear text performing a Man in the Middle (MitM) attack.

Potential Impact: An attacker could obtain information of the car from the dongle using a MitM attack and potentially perform replay attacks.

AFFECTED COMPONENT

- HW

SEVERITY LEVEL



- Confirmed Vulnerability

EVIDENCES

This example shows a network capture for Bluetooth where VIN number is read from an external attacker:

```
▸ Bluetooth Low Energy Link Layer
▸ Bluetooth L2CAP Protocol
▾ Bluetooth Attribute Protocol
  ▸ Opcode: Read Response (0x0b)
  ▸ [Handle: 0x0026 (Unknown: Unknown)]
    Value: 4d48424a3243483246414141414141000000
    [Request in Frame: 68242]
0000  98 06 2c 01 f5 4f 06 0a  01 0d 2c 34 02 96 00 00   ..,..O.. ..,4....
0010  00 e9 a2 9a af 0a 19 15  00 04 00 0b 4d 48 42 4a   ........ ....MHBJ
0020  32 43 48 32 46 41 41 4a  41 41 41 41 41 00 00 00   2CH2FAAJ AAAAA...
0030  81 f9 40                                          ..@
```

FINDING: Lightning Control Module

RISK DESCRIPTION

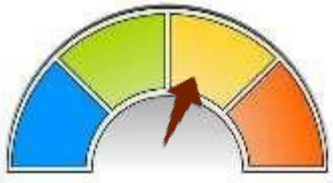
Threat Description: The Electronic Control Unit (ECU) related with light system is accessible from the OBD-II port.

Potential Impact: An malicious attacker could perform an attack to the lightning system potentially damaging it, causing problems to the driver turning-off or turning-on random lights in the vehicle and generating safety problems.

AFFECTED COMPONENT

- Customer Cross

SEVERITY LEVEL



- Confirmed Vulnerability

EVIDENCES

Though a fuzzing attack to the Customer Cross performed in Customer facilities, the evaluator discover the system that manages the lights in the car.

FINDING - Malicious file upload

RISK DESCRIPTION

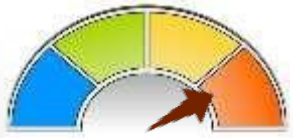
Threat Description: The server allows file uploading for all authenticated users without any kind of filter for the uploading. These files uploaded are stored in the server and can be retrieved with the url /v1/files/get/<number> (for authenticatd users) or /v1/file/test/<number> (public)

Potential Impact: A malicious attacker with a valid account could upload files with malicious content in the server. The attacker could perform attacks to other sites using the malicious files uploaded in the Customer servers, including malware distribution or other kind of illegal content.

EVALUATION AREA

- Cloud Services

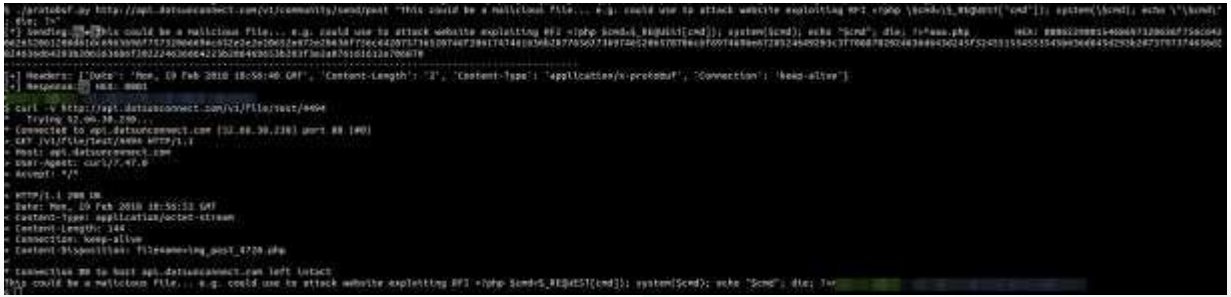
SEVERITY LEVEL



- Confirmed Vulnerability

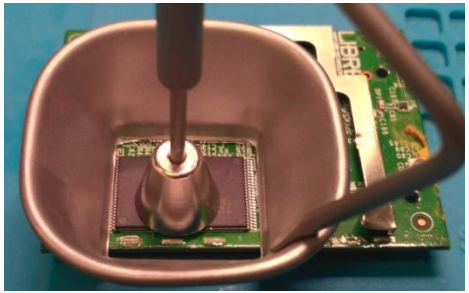
EVIDENCES

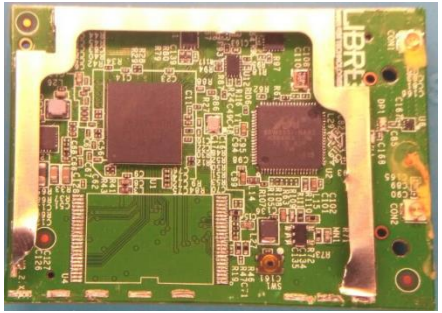
The following figure shows how a file has been uploaded and how it can retrieve from the server:

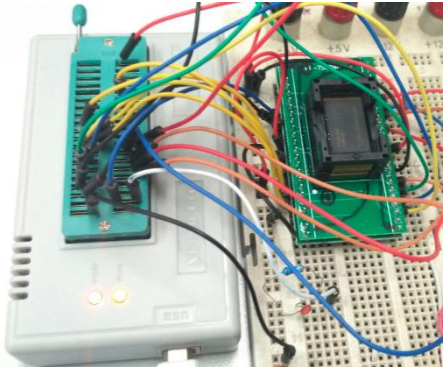


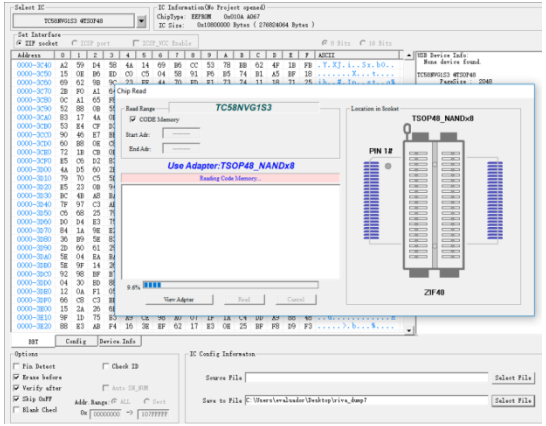
FINDING 1. Firmware Extraction (I)

EVIDENCES



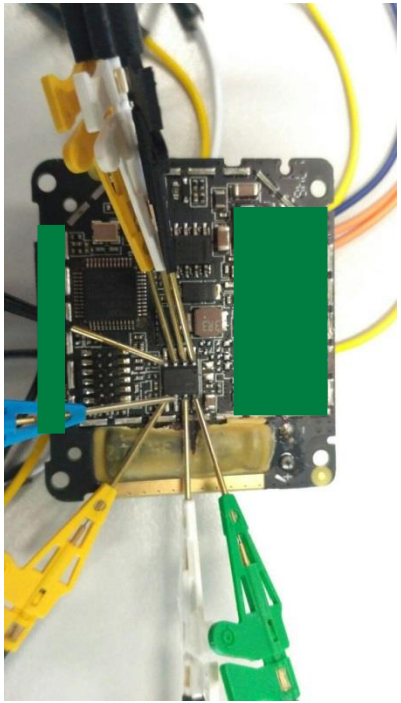


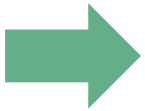




FINDING 1. Firmware Extraction (II)

EVIDENCES





```
          @ws1:~/Escritorio/      winbond$ sudo python spiflash.py -i
FT232H Future Technology Devices International, Ltd initialized at 15000000 hert
z
EF 40 14
          @ws1:~/Escritorio/      winbond$ sudo python spiflash.py --read=dump.bin
 --size=1048576
FT232H Future Technology Devices International, Ltd initialized at 15000000 hert
z
Reading 1048576 bytes starting at address 0x0...saved to dump.bin.
              :~/Escritorio/      winbond$ /home/          /Escritorio/spiflash.py
```

Our cyber security experts

One of the largest cyber security evaluation & certification labs:

- Dedicated and experienced team of 35 security evaluation engineers
- >10 years of experience with Common Criteria, FIPS-140 certification, penetration testing, and R&D in new vulnerability attack methods
- Experienced in product security evaluation

The cyber security team works with reputable technical security certifications:

- OSCP: Offensive Security Certified Professional
- CEH: Certified Ethical Hacker
- Lead Auditor ISO 27001: Information security Management
- Assembly Language and Shellcoding on Linux (SLAE)

DEKRA's cyber security team consists of security experts with expertise in a.o.:

- Ethical hacking
- Penetration testing
- Reverse engineering
- Embedded device security
- Code analysis
- Run time analysis
- Vulnerability assessment

Some of our customers

- Apple
- Microsoft
- Huawei
- Hewlett Packard Enterprise Development L.P.
- Dell Technologies, Inc.
- Check Point Software Technologies Ltd.
- Autek Ingeniería, SL
- Sistemas Informáticos Abiertos, SA
- B-Solutions Advanced Technologies S.L.
- Realia Technologies
- NetApp, Inc
- Safelayer Secure Communications
- INIXA S.L
- ASELSAN Inc
- Authenware Corporation
- Big Switch Networks
- Bittium
- Authenware Corporation
- INCIBE
- Cyberoam Technologies Pvt
- SOMA- Sociedade de Montagem de Automóveis, S.A.
- ATOS Consulting
- INDENOVA SL
- EADS-CASA
- HV Sistemas
- Nimble Storage, Inc.
- PR
- SOMA- Sociedade de Montagem de Automóveis, S.A.
- OYTECSA SECURITY S.L.
- Karpersky

Thank you!
More information?
www.DEKRA-product-safety.com

Contacts

Juan Sánchez
Cyber security Manager
Mobile: +34 655 42 15 15
juan.sanchez@dekra.com

Jorge Wallace
Cyber security Lab Manager
Mobile: +34 605 122 756
jorge.wallace@dekra.com