Address cybersecurity challenges for connected cars with penetration testing services

Sergey Razmakhnin,
Head of Cybersecurity, NavInfo Europe

Agenda

- Cyberattacks in Automotive industry
- Cybersecurity challenges for connected cars
- Real-life hacking scenarios for connected cars
- New attack vectors for ADAS/Autopilot and car's sensors
- New cybersecurity regulation (WP.29, ISO 21434)
- Pen-testing for connected autonomous cars

Global Footprint

NavInfo Europe

History

- Founded in **2011**, started **AI Computer Vision** research in 2015
- Started development of automotive **cybersecurity** solutions in **2018**
- Close cooperation with Technical University of Eindhoven (TU/e)

Team

- **180+** employees
- **130+** researchers and engineers
- Based in **Eindhoven**, Netherlands

Core Activities

- Cybersecurity
- NDS Compilation
- Advanced AI engineering and research
- Global Customer Support

Advanced Research

Our expertise lays in

- Artificial Intelligence Computer Vision
- Cyber Security
- SD/HD Map Data Services and processing

NavInfo Europe
Securing the automotive pipeline through various domains

Cloud Cybersecurity

- Foundation of the cybersecurity research lab in the Netherlands
- Completed the first penetration tests of the internal cloud infrastructure
- Started development of internal penetration testing tools

AI Security in Automotive

- Penetration testing for whole cars
- Penetration testing for standalone module (Infotainment, Gateway, T-Box, V2X, ADAS, Autopilot, Engine)
- Extended **security assessments** to in car mobile and Cloud applications
- **Robust and Reliable AI**: Adversarial attacks, Model & Training optimization, Regulatory compliance

Automotive Cybersecurity

- **Penetration Testing**: performed a large-scale penetration test of a connected vehicle with a top OEM
- Started development of cybersecurity products to leverage **AI** in Security for cars

2018 Cybersecurity Lab established in Eindhoven

2020 Extended cybersecurity expertise into the AI domain to create innovative AI security products

2022 Start of development of security solutions for connected cars

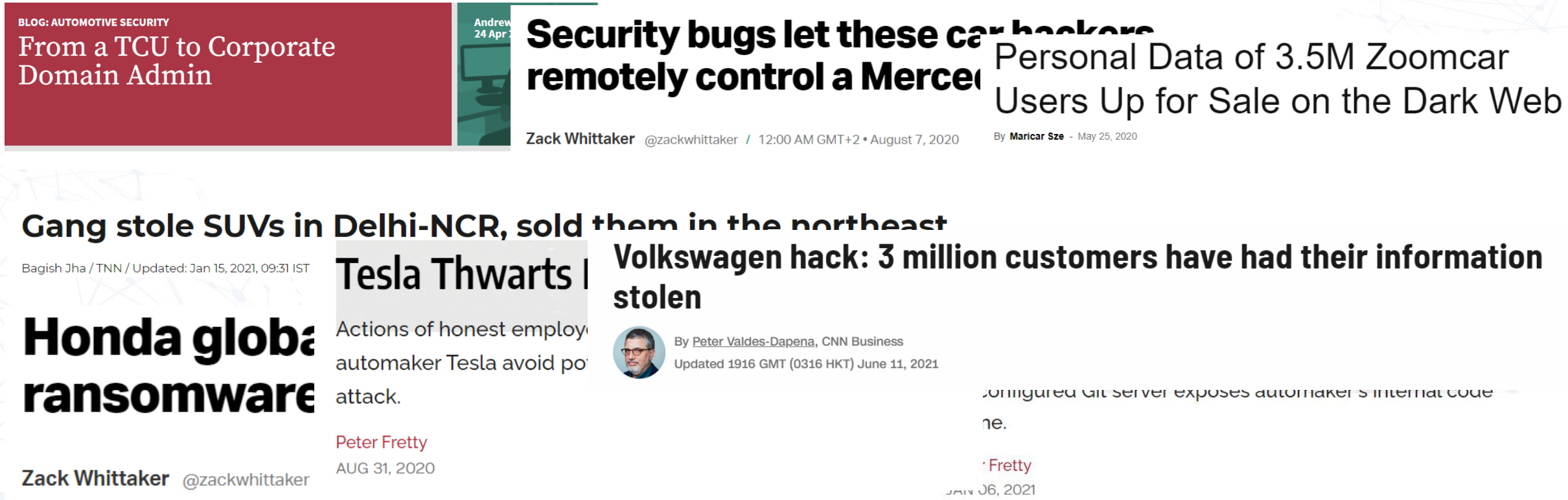
Future

Cyberattacks in automotive industry

A connected car in 2021 provides a massive attack surface and several entry-points to the most sensitive data. Hackers leverage these vulnerabilities to extort money and personally identifiable client data.

By 2025, **connected vehicles** will make up **86% of the international automotive market**

More than **300 vulnerabilities** were found in over **40 ECUs** developed by 10 Tier-1 companies and OEMs [1]



*Source: Upstream 2021 report

1 Source – Upstream 2021 Report

Real-life attacking scenarios for connected cars

Hacking, obtaining root access:
In-Vehicle Infotainment
& Gateway

Hacking, obtaining root access:
T-Box, Emergency call module,
Adaptive cruise control unit, ABS control unit,
Engine/Motor control unit

Track car's geo-location remotely

Extract & steal car location history remotely

Record passenger information through the microphone

Record information from the car's cameras and send the data to a remote server

Control car charging remotely

Control acceleration, steering and brakes remotely

Embed malicious code & stream in ADAS, auto-pilot systems

Control car's entry system (open doors, windows, start engine) remotely

Cybersecurity challenges in the automotive industry and for connected cars

Software Complexity growing
- Millions lines of codes
- More than 50 different ECU with proprietary firmware
- The modern connected car provides a multitude of interfaces that are increasingly more software-based
- The Attack Surface of the Vehicle is growing with the amount of software
- Attacks on Autonomous driving AI models

Connectivity growing
- The vehicles are becoming more connected and dependent on the back-end systems
- Amount of data exchange is increasing, meaning a larger privacy concern
- Car2X/V2X connectivity
- Wi-Fi, Bluetooth, NFC, Custom RF protocols
- 2G/3G/4G/5G connectivity

Supply Chain & Processes risks
- Compromission of TIER 1/2/3 suppliers
- Complexity of supply chains
- Considering the lifetime of a vehicle can be around 10-20 years, OEMs need to install frameworks and processes in order to secure the vehicle from the design to the aftermarket stages

New attacks on car's sensors
- Camera-based computer vision attacks
- Adversarial attacks on AI models
- Lidar attacks
- Radar attacks
- GPS spoofing
- Attacks on V2X interfaces

New attack vectors on car's Back-End and Cloud services
- Stealing user accounts
- Data breaches of user's data
- Data breaches of source codes
- Remote control of the car
- Mass-fleet infection

New cybersecurity regulation:
- UNECE WP.29
- ISO 21434
- Regulation on Security Management of Automotive Data in China
- Connected vehicle Security requirements of data in China

Rewards in public bug bounty programs for connected cars

- Only a few automotive companies provide public prices for rewarding bug-bounty program for Web, Cloud, Back-End services
- Only one of the biggest automotive companies provides public price for hacking own connected car

Target		Prize Amount	Additional Prize Options
Initial Vector	Final Stage		
Tuner, Wi-Fi, Bluetooth, or Modem	Infotainment	**$250,000 USD**	Vehicle Prize
			Infotainment Root Persistence Add-on
			Autopilot Root Persistence Add-on
			CAN Bus Add-on
Infotainment	VCSEC, Gateway, or Autopilot	**$300,000 USD**	Vehicle Prize
			Infotainment Root Persistence Add-on
			Autopilot Root Persistence Add-on
			CAN Bus Add-on
Tuner, WiFi, Bluetooth, or Modem	VCSEC, Gateway, or Autopilot	**$400,000 USD**	Vehicle Prize
			Infotainment Root Persistence Add-on
			Autopilot Root Persistence Add-on
			CAN Bus Add-on

- Such programs allow car OEMs to receive the “second” opinion, multiple critical vulnerabilities have been identified and solved and the security of cars has been protected

https://bugcrowd.com/tesla
https://hackerone.com/bmwgroup?type=team
https://www.zerodayinitiative.com/blog/2022/1/12/pwn2own-vancouver-2022-luanch#auto

New attacks vectors on ADAS/Autopilot

Scenario

Attacks on Autopilot, ADAS algorithms for forcing the cars to make wrong decisions about other cars on the roads, pedestrians, road signs

Consequences

Incorrect input from computer vision systems can create critical incidents on the road

Risk Level

Critical
Life-Threatening

Example

Adversarial crafted picture and shapes are applied to the object, making it **invisible** for Autopilot, ADAS systems

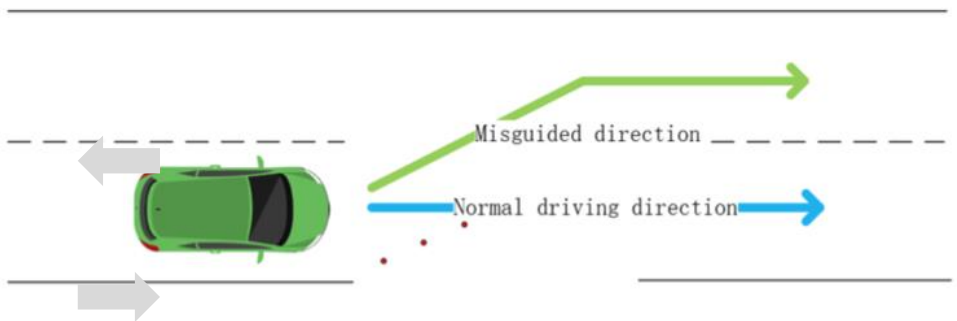
Autopilot, ADAS algorithm

score: 0.999 **score: 0.003**

Example

Adversarial created marks on the road are correctly supplied to ADAS and **forces** it to **change the lane** on the road

Autopilot, ADAS algorithm



New Cybersecurity regulations in Automotive industry

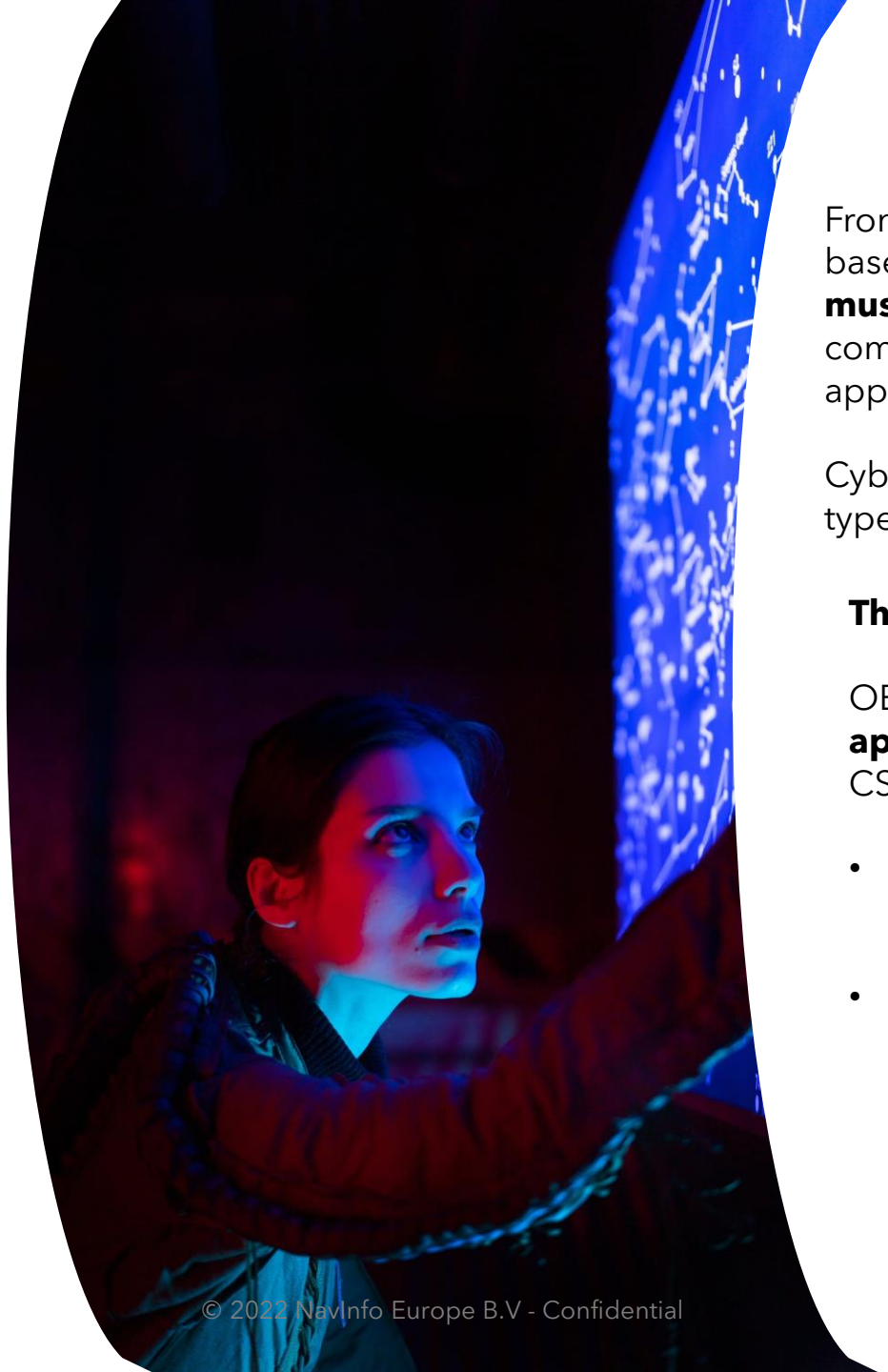
- United Nations Economic Commission for Europe UNECE WP.29
- ISO/SAE 21434 Standard
- Regulation on Security Management of Automotive Data in China
- Connected vehicle Security requirements of data in China

United Nations Economic Commission for Europe / UNECE WP.29

2 main Regulations:

- **CSMS** (Cybersecurity Management System)
- **SUMS** (Software Updates Management Systems)

54 countries - all EU countries and other OECD nations like Japan, Turkey, Russia, Australia, and South Africa



From **July 2022** newly produced vehicle lines based on **existing electronic architectures must receive type approval** as a sub-component of the process of vehicle type approval (WVTA)

Cybersecurity is **mandatory** for **all** first vehicle type registrations **after July 2024**

The process in a nutshell:

OEMs submit applications for **vehicle type approval** to demonstrate compliance with CS regulations:

- **Certificate** of Compliance for CSMS & SUMS
- **Description** of the vehicle type (Annex 1) should include prove **what tests** have been used to verify the cyber security of the vehicle type and its systems and the outcome of those tests

Relation between ISO/SAE 21434 and UNECE WP.29

The standard and the regulation are complimentary and non-contradicting, meaning that the implementation of both will result in better compliance

ISO/SAE 21434

UNECE WP.29

A **standard** that will be adopted in the industry and widely used

Thoroughly describes **how** to do TARA, cybersecurity management in the organization, and the supply chain

Regulates vehicles and its systems, firmware, hardware and software components & any connection to external servers/devices

Shared Requirements

Cybersecurity by Design
Both require the OEMs to secure the vehicle lifecycle – from development to production and post-production service.

Cybersecurity Management System
- Risk Mitigation strategies
- Threat Analysis and Risk Assessment
- Supply Chain Management

Legally binding **regulation** with consequences within 54 countries (contracting parties)

Defines **what** to do - Provides a list of 69 threats & 23 mitigations that serve as baseline for cybersecurity assessment

Regulates the vehicle, OTA updates and establishes CSMS at every stage of the vehicle lifecycle

Create and Sustain Cybersecurity for Strategic Success

Prevent cybersecurity, financial, reputational and legal risks

Penetration testing **during the development cycle** ensures your business is protected from costly data breaches and their aftermath

Improve Compliance

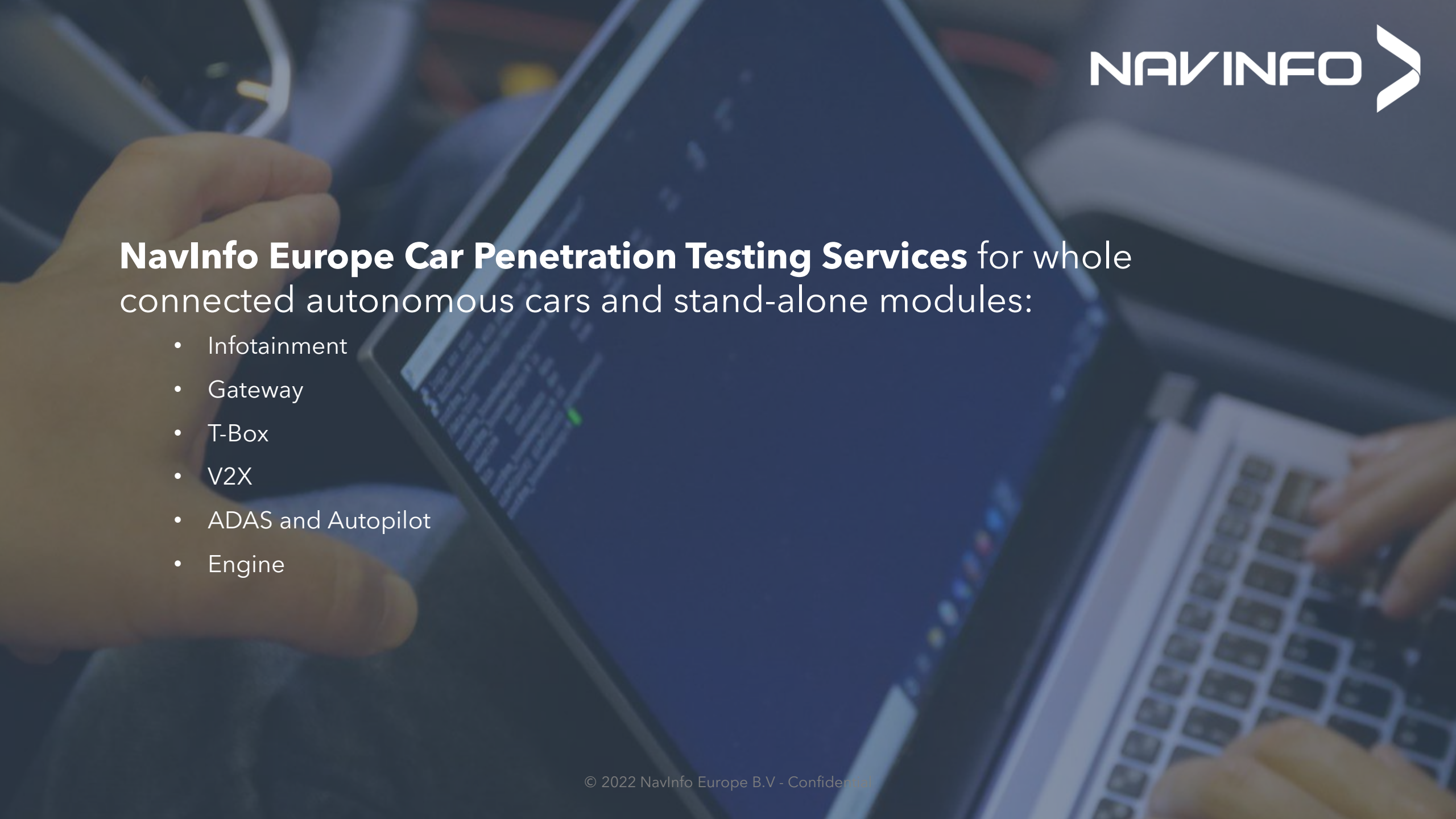
Stay ahead of cybersecurity regulation in the European Union

Ensure insight quality

Every car module that is tested is paid outstanding attention, with research and deep-down analysis at every stage

Save costs on finding cybersecurity talent & the right tools

Our cybersecurity experts with world-class certification complete penetration tests **on time using the right tools**



NavInfo Europe Car Penetration Testing Services for whole connected autonomous cars and stand-alone modules:

- Infotainment
- Gateway
- T-Box
- V2X
- ADAS and Autopilot
- Engine

NavInfo Cybersecurity Expertise

- Penetration Testing & Reverse Engineering of connected cars
- Data privacy in Automotive, Autonomous Driving & Big data Security
- Cloud and Enterprise Security
- Telecom security, 3G/4G/5G security
- Security Operation Centers

OSCP · OSWP · OSCE · CISSP · GPEN · OSWE · CEH Certified Ethical Hacker · AWS certified Security Specialty · Certified Red Team Professional

Discover our penetration testing services

Wide Range of Interfaces

Build a package to ensure the large-scale testing and discovery of all hacking scenarios

- Connected cars
- IoT Devices
- External and Internal Networks
- Cloud Platforms
- Web Applications
- Mobile Applications

Full Scope of Security Testing Activities

Uncover the full potential of penetration tests through our extended list of services that cover the entire vehicle lifecycle

Our approaches:

- **External Penetration Testing**

We'll simulate attacks with real-life hacking scenarios

- **Internal Penetration Testing**

Simulate the threats faced from connected third parties, employees, or contractors who have direct internal network access.

Activities:

- Vulnerability Analysis
- Smart Fuzzing of wireless interfaces
- Reverse Engineering of SW and HW
- Statical and Dynamic Binary Code Analysis
- ECU Firmware Dumping & Disassembling
- Default Credential and Configuration manipulation

Deliverables of Security Testing

Thorough and detailed testing reports ensure contribution to the success of the overall cybersecurity management system

The full **cybersecurity evaluation report** includes:

- Overview of findings and vulnerabilities
- Proof-of-Concept code and exploits
- Penetration Testing Strategy and Concept
- Results of Fuzzing Tests on wireless interfaces
- Recommendations on Code Review
- Guidelines for fixing discovered vulnerabilities

Car Security Assessment

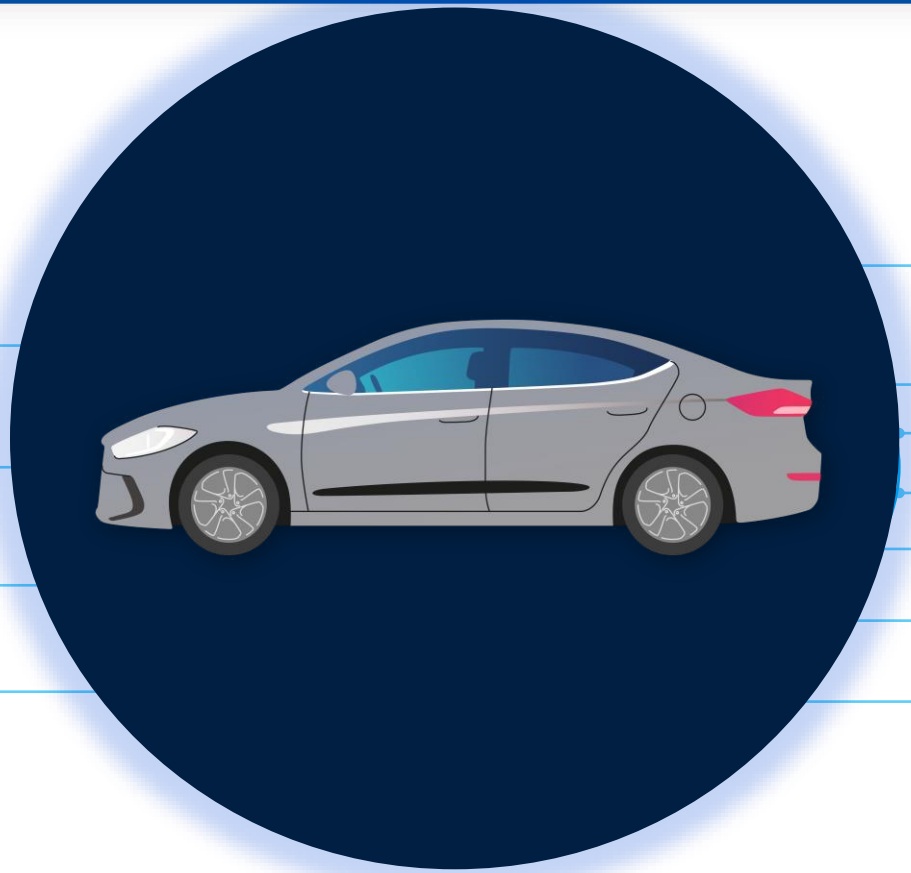
The average connected car in 2021 contains more than 50 ECUs and million lines of code

The attack surface is immense – the Internet, Wi-Fi, Bluetooth, custom RF protocols, CAN, OBD2 interfaces, media files imported over USB, Automotive ethernet, remote diagnostics, telematics, mobile apps

Our team simulates the cyber threats faced against connected cars

Manual Pen-Testing

- Identify vulnerable interfaces, ports and services
- Analyse externally and internally exposed services and enterprise traffic
- Man-in-the-Middle attacks for Cellular, Wi-Fi, Bluetooth, NFC traffic interception
- Fuzzing of wireless interfaces and software, firmware



Reverse engineering

- Software, hardware components reverse engineering for vulnerability assessment
- ECU firmware dumps and disassembling for security testing
- Statical and dynamical binary code analysis for vulnerability analysis
- Default configuration and credential manipulation
- Mobile application reverse engineering
- CAN bus, OBD2 interfaces communication security analyses
- Car's sensors and AI model robustness testing

Car Security Assessment

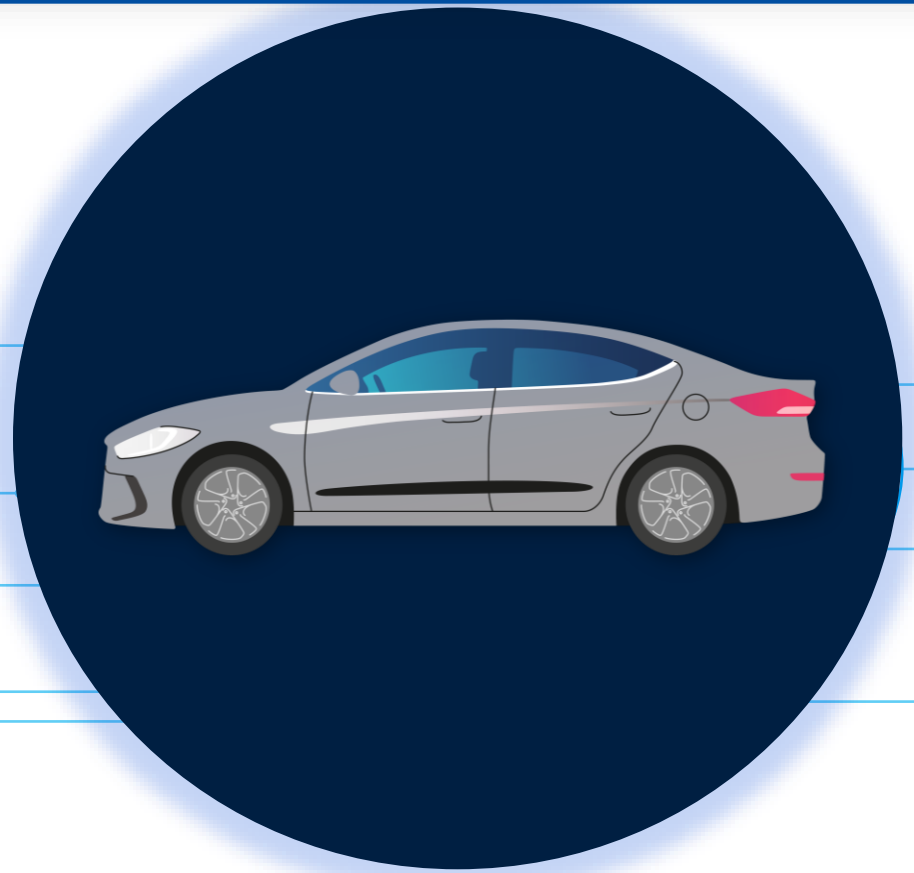
The average connected car in 2021 contains over 150 ECUs and 100 million lines of code

The attack surface is immense – the Internet, Wi-Fi, Bluetooth, custom RF protocols, CAN, OBD2 interfaces, media files imported over USB, Automotive ethernet, remote diagnostics, telematics, mobile apps

Our team simulates the cyber threats faced against connected cars

Attack Demonstration

- Remote control of the adaptive cruise control and autopilot functions
- Access to steering and brakes functions
- Remote keyless entry
- Remote access to car's microphone, camera
- Malware persistence in car's software and firmware



Access to Crown Jewels

- Sensitive driver's data exfiltration
- Drivers and Vehicle makers account compromise
- Malicious firmware updates, Access to the vehicle's source code
- Data breaches

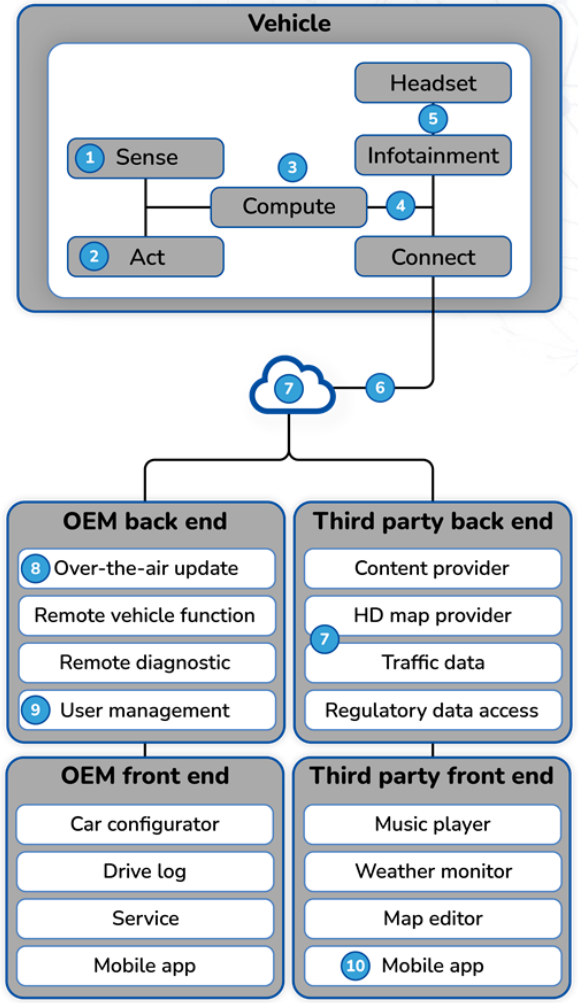
Pen-testing wireless interfaces in Connected Cards

- We research vulnerabilities in wireless interfaces in connected cars:
  - Bluetooth
  - Wi-Fi
  - Cellular (2G/3G/4G/5G)
  - V2X
  - Custom RF protocols
- We use our in-house fuzzing tools for guided security testing all wireless stacks, drivers, chips in connected cars
- We use smart fuzzing and guided fuzzing patenting technologies for wireless interfaces
- We organize real-life demonstration of hacking cars via wireless interfaces

Pen-testing the back-end services of Connected Cars

- We do pen-testing for OEM and Third party Back End services:
  - Over-the-air updates
  - Remote diagnostic
  - User management
  - Content providers

- We provide pen-testing for all type of Back End services:
  - Cloud and Enterprise services
  - API gateways
  - Web services
  - Mobile Applications
  - External and Internal networks



Vulnerability Analysis

Criticality of Software Update

- Complexity of vulnerability exploitation and skill needed
- Impact scope on connected vehicle fleet & back-end platform of OEM and 3rd parties

Impact on the Vehicle/Drivers

- Effect on Passenger Safety and other vehicles on the road
- Vehicle Performance and User Experience Affected
- Implications of the Hacking Scenarios in real-world situations

Remediation Complexity

- Complexity of fixing vulnerabilities and related processes
- Dependencies with 3rd party suppliers
- Secure Development Lifecycle

Regulatory Compliance

- Criticality of exposed client data (passenger, owner, driver) & OEM data
- Risk Assessment of possible non-compliance with WP.29, ISO/SAE 21434, GDPR, etc..

Cooperation

Cooperation Model

- Penetration testing for whole car
- Penetration testing for standalone module, ECU:
  - Infotainment
  - Gateway
  - T-Box
  - V2X
  - ADAS
  - Engine, etc.

Goals & KPIs

- Penetration testing report with identified vulnerabilities
- Demo of hacking scenarios
- Recommendations and guidelines for fixing discovered vulnerabilities
- Verification of fixing vulnerabilities

Prioritization

- Priority of modules/system, car models, platform/car lines, car's back-end services
- Focus on real-life hacking scenarios
- Focus on compliance

Disclosure Policies

- Definition of the engagement process for resolution of vulnerabilities with Suppliers
- Participation and Disclosure of findings at industry events
- Cybersecurity consultancy for proper vulnerabilities disclosure

Thank you!

Contact us
info@navinfo.eu

www.navinfo.eu

Follow us