By Anna Stylianou

Automotive Cybersecurity Specialist

BSides Cyprus 2019

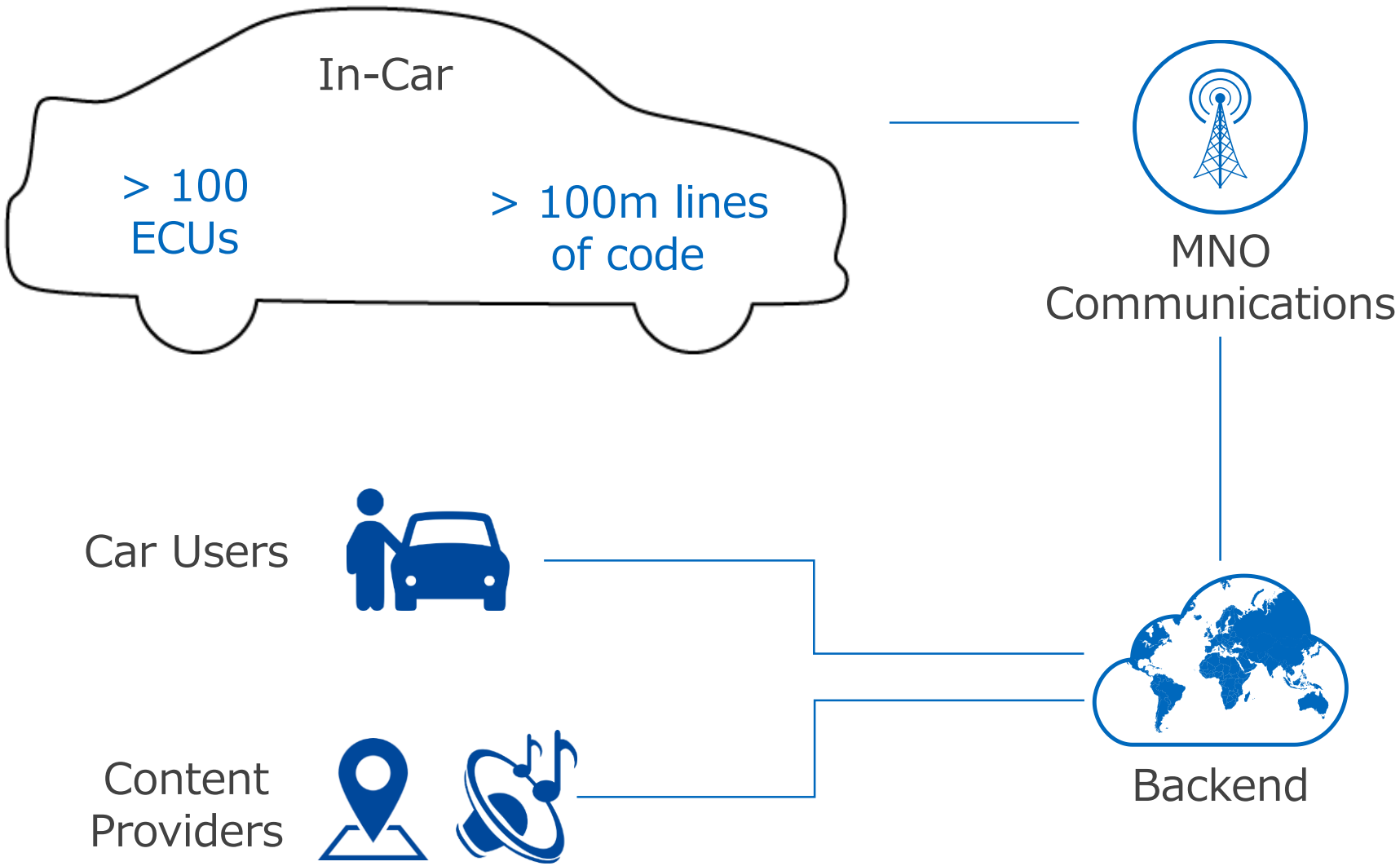
The Ever-Increasing Cyber Threat Landscape of Modern Cars and Smart Cities

05/10/2019

Agenda

1. Overview of the cyber threat landscape
2. Attack demonstration examples on how to hack a car
3. Reaction from the automotive industry to the current threats
4. Security recommendations for the way forward

Cars Are Becoming Computers on Wheels



50+ Generic Attack Points

SBD has identified 50+ generic attack points that hackers can exploit in order to hack a car.

In-Car Attack Points

TCU	
Tethered Modem	Embedded SIM

OBD	Powertrain
Port	EV Cable

Headunit				
Software Stack		**Comms Modules**		
Native Apps	Downloaded Apps	Bluetooth	USB	Wi-Fi
Middleware	OS	SD Card	HDMI	Aux-in
Processor	Energy Management	Satt. Radio	Toll Tags	CD/DVD
		NFC	DSRC/V2X	Wireless HD
		GPS		

MNO Attack Points

Data		Voice
CGSN	SMSC	MSC

Home Location Register	M2M Platform
Authentication Centre	SIM Management Portal

Radio Network	
Base Station	Radio Access Control

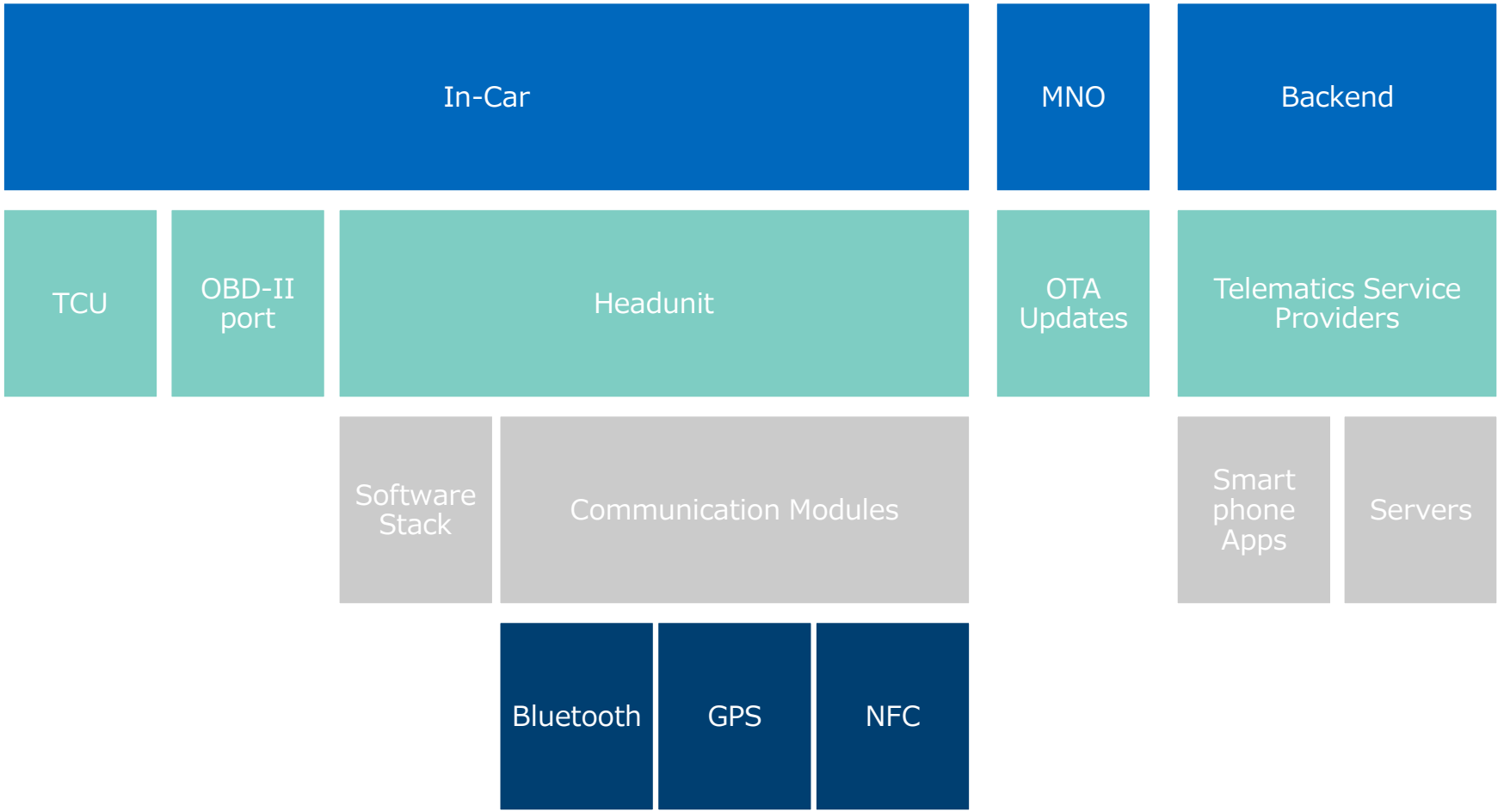
Backend Attack Points

Data Users	
3rd Party Data Users	OE SATA Users (dealer etc.)

Call Centers	Content Providers	
CGSN	Content Providers	App Providers

TSP				
Dispatcher	App Store	Billing Engine	CRM/VRM	Driver Portal

Most Hackable Attack Points



Hacking Tools For Vehicles

- Open Source
- CAN Network Analysis
- Reverse Engineering
- Packet Injection
- Black-box Testing

CANToolz

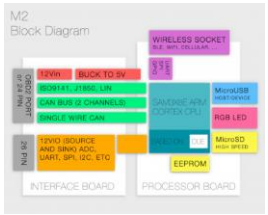
CANBadger

CANBadger hardware

CANSPY

Metasploit for Cars

M2 hardware design



M2 by Macchina

CANtac

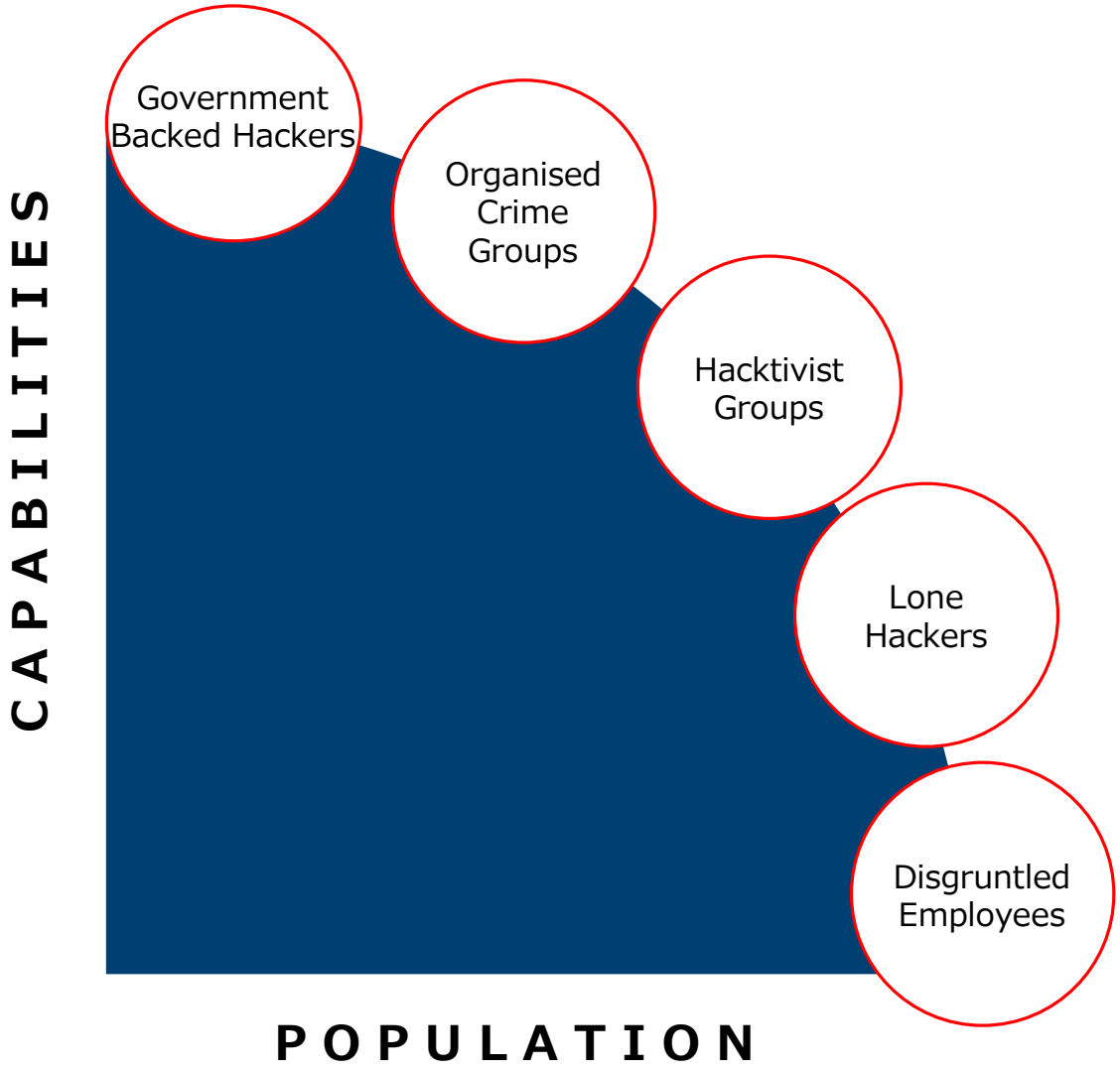
CANtac hardware

Universal Radio Hacker

PASTA

By Toyota InfoTechnology Center & Yokohama National University

Who Wants to Attack Cars?

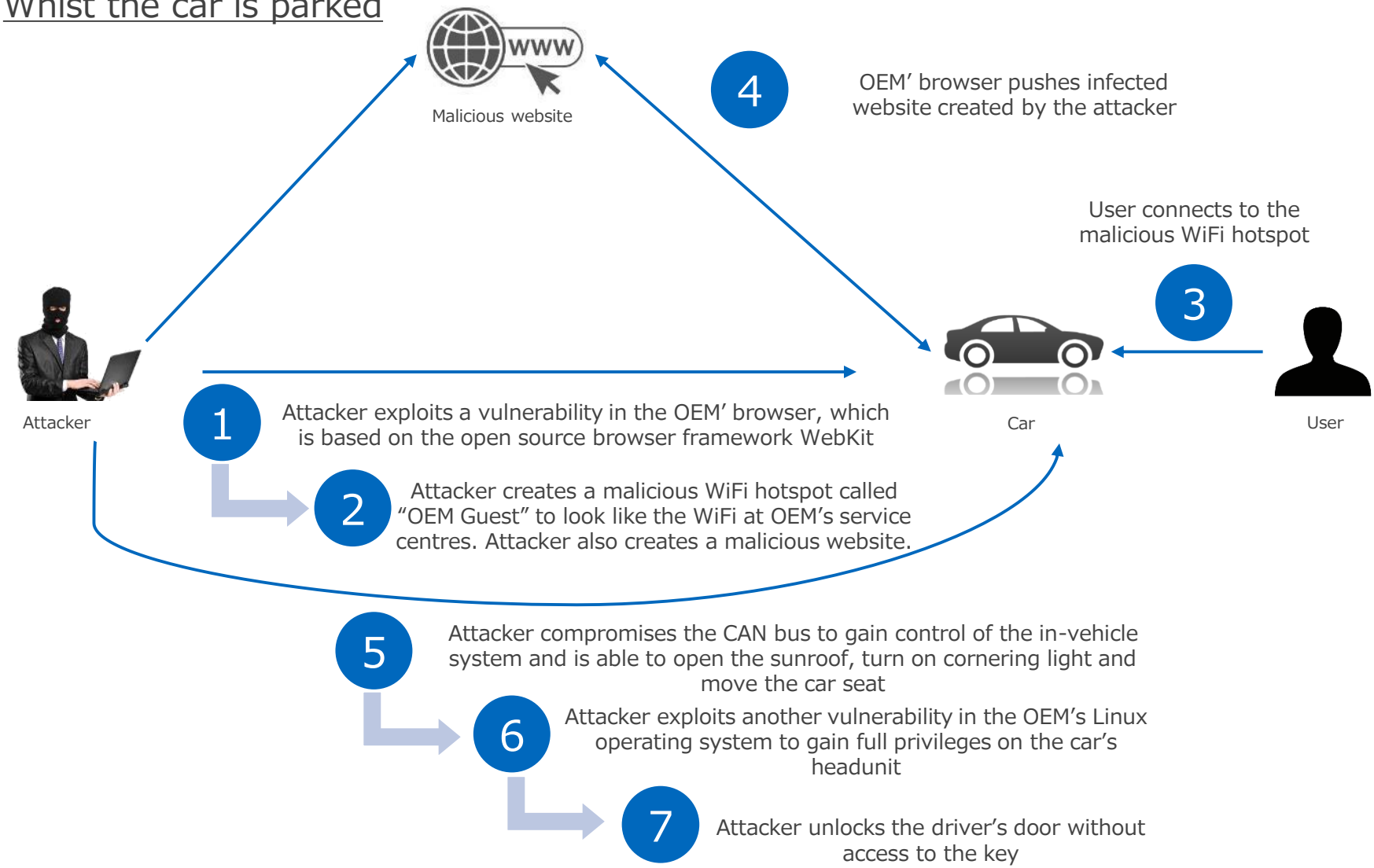


MOTIVATION

- Control
- Financial
- Data
- Destruction
- Disruption
- Fame

Remote Attack Demonstration

Whist the car is parked



Remote Attack Demonstration in Driving Mode

Remote Control in Driving Mode

Attacker

Car

1

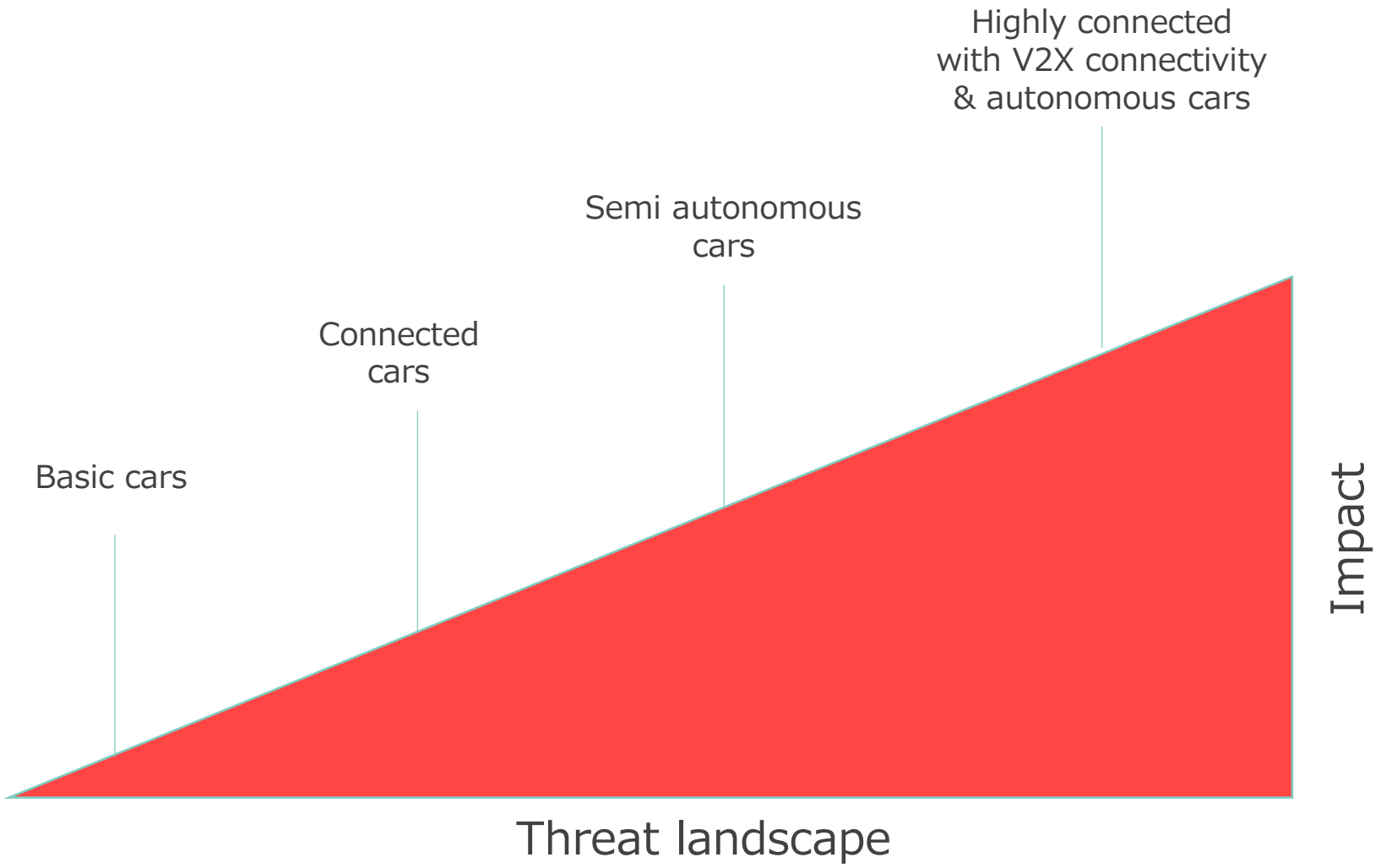
Attacker gains control of the car while is moving and:

1. Operate windshield wipers
2. Fold side-view mirror while vehicle is moving
3. Open the trunk

2

Attacker operates the brake system (12 miles away) and forces the car to stop.

Impact of Hacking



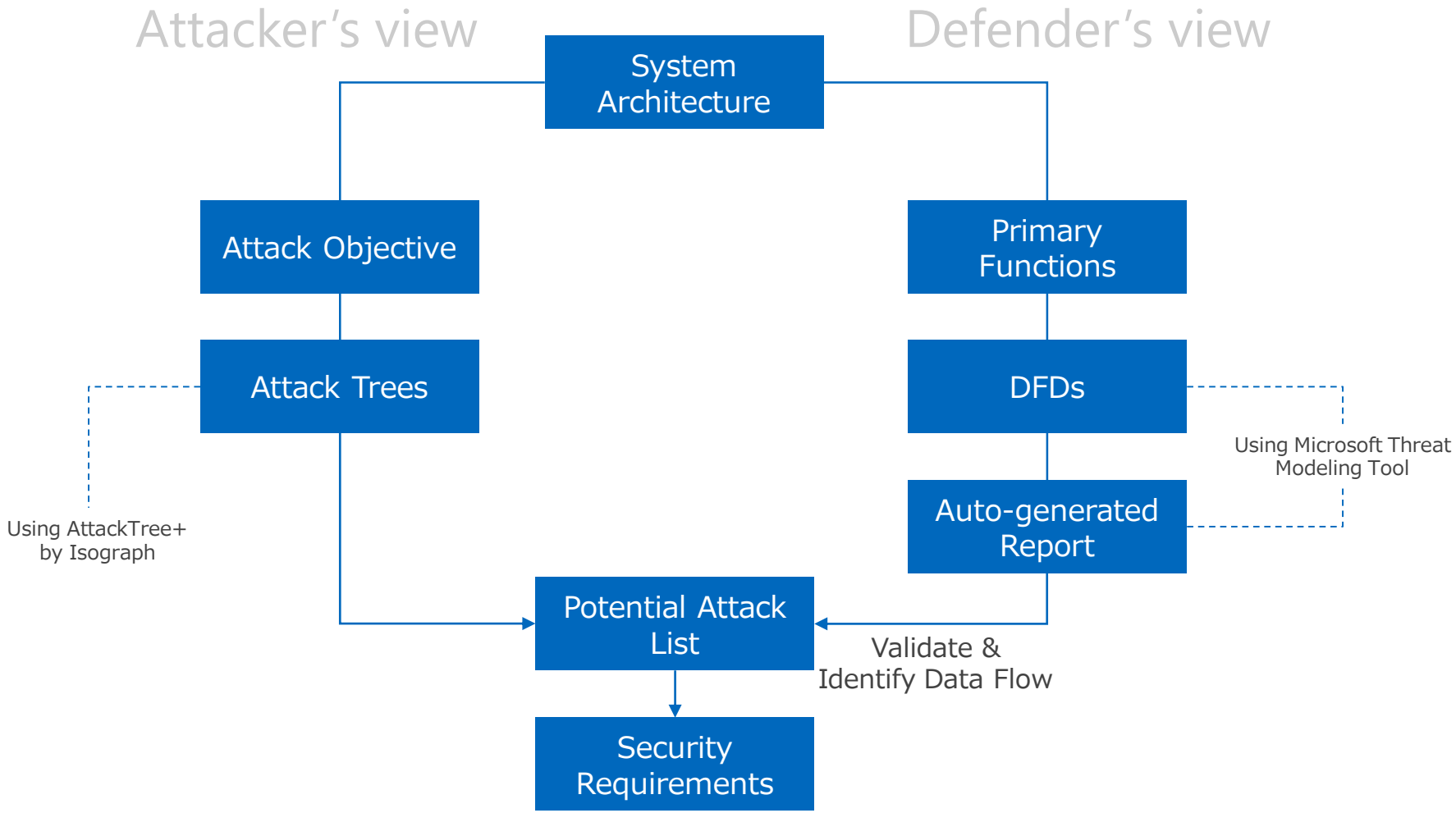
Automotive Secure Development Lifecycle

Inclusive Framework
- International Standards
- Industry Best Practice
- Company Guidelines

Agnostic
- Standards
- Methodologies
- Global Applicability

SBD Unique Value
- Global Knowledge-base
- In-house Expertise

Threat Modelling & Risk Assessment

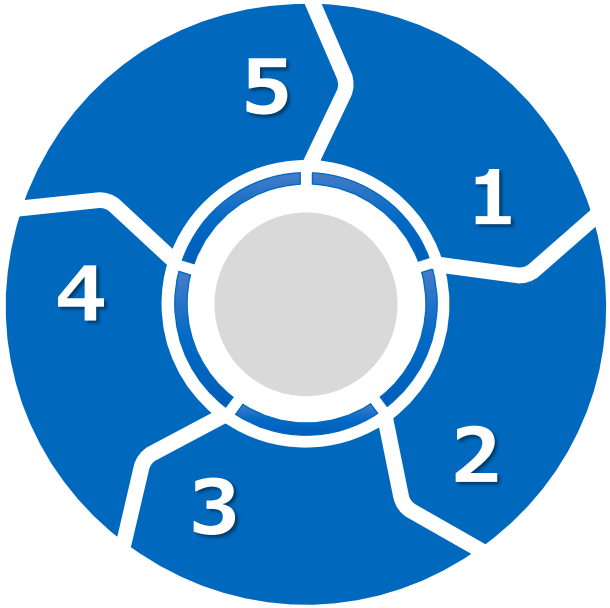


Countermeasure Lifecycle

- Countermeasure Lifecycle utilises the NIST Cybersecurity Framework that presents 5 key cybersecurity functions to help managing cybersecurity risk.

5. Recover

- Software OTA Updates
- Continuity of Operations
- Recovery Planning
- Communications (within organisation, with suppliers and with vehicle users)



1. Identify

- Threat Modelling
- Vulnerability Assessment
- Penetration Testing
- Design – Code Review
- Risk Management
- Governance

4. Respond

- Incident (In-Vehicle) Response
- Security OTA Updates
- Security Operation Centers
- Malware Analysis
- Forensic Remediation

2. Protect

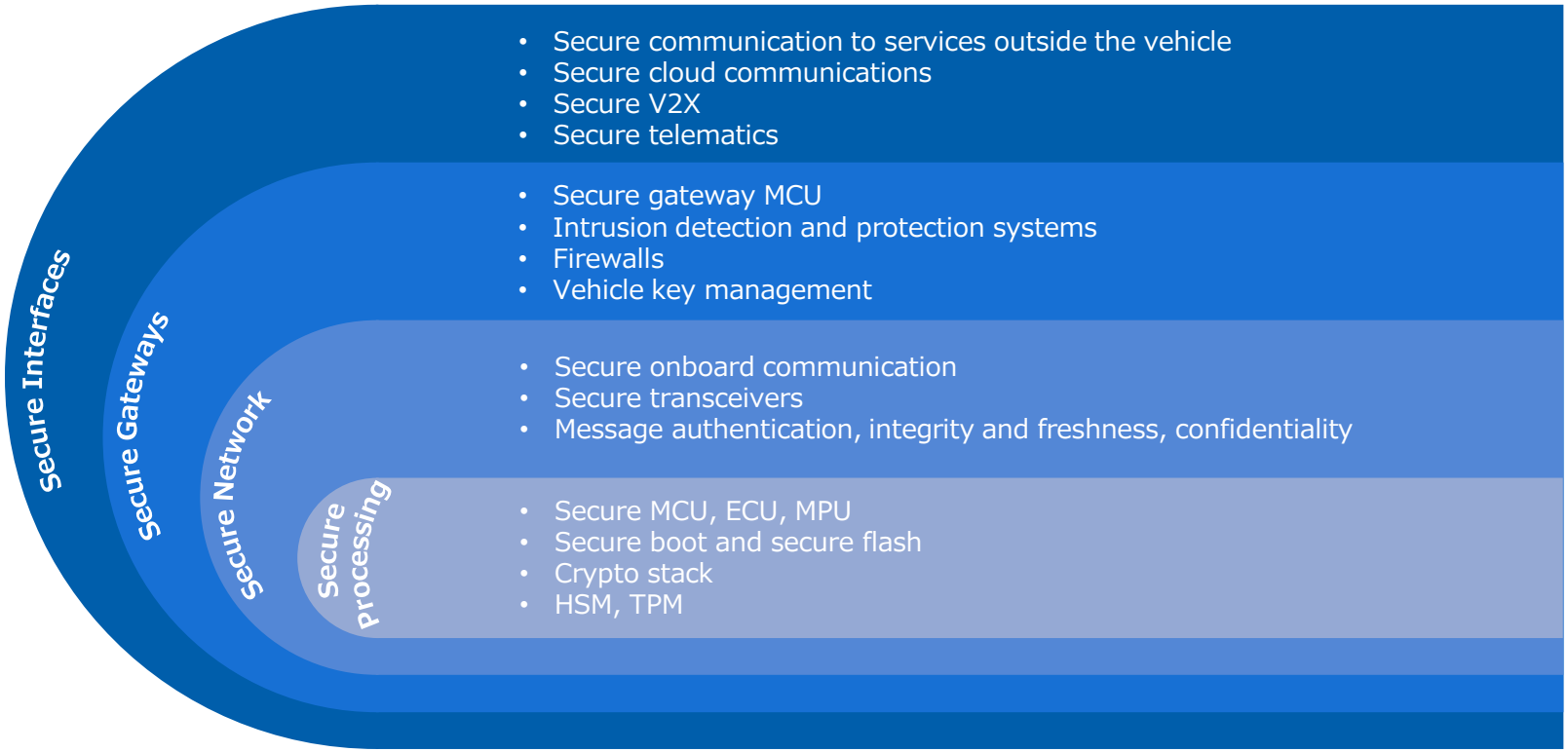
- Secure Processing, Networks, Gateways, Interfaces
- Threat Prevention, Firewalls, IPS
- Data Security
- Protective Technology
- Training and Procedures

3. Detect

- In-vehicle Network Continues Monitoring
- Anomaly Detection – IDS
- Alerts - Warnings

Layered Security Approach

- Layered security is vital because a device is only as secure as its weakest link.
- A single vulnerability could compromise the whole vehicle. This can be avoided in the case of multi-layered built in security.



Reaction from OEMs & Suppliers

- Development of cybersecurity teams within OEMs
- Partnerships between OEMs and suppliers
- Acquisitions of cybersecurity companies
- Automotive cybersecurity workshops and conferences
- Information Sharing & Analysis (Auto-ISAC)
- Vulnerability Disclosure Programs (FCA, General Motors, Tesla)
- Participation in the development of industry standards and best practices

Industry Standards & Best Practices

- Main active key players globally

Europe

UNECE

bsi.

ACEA European Automobile Manufacturers Association

enisa

ETSI

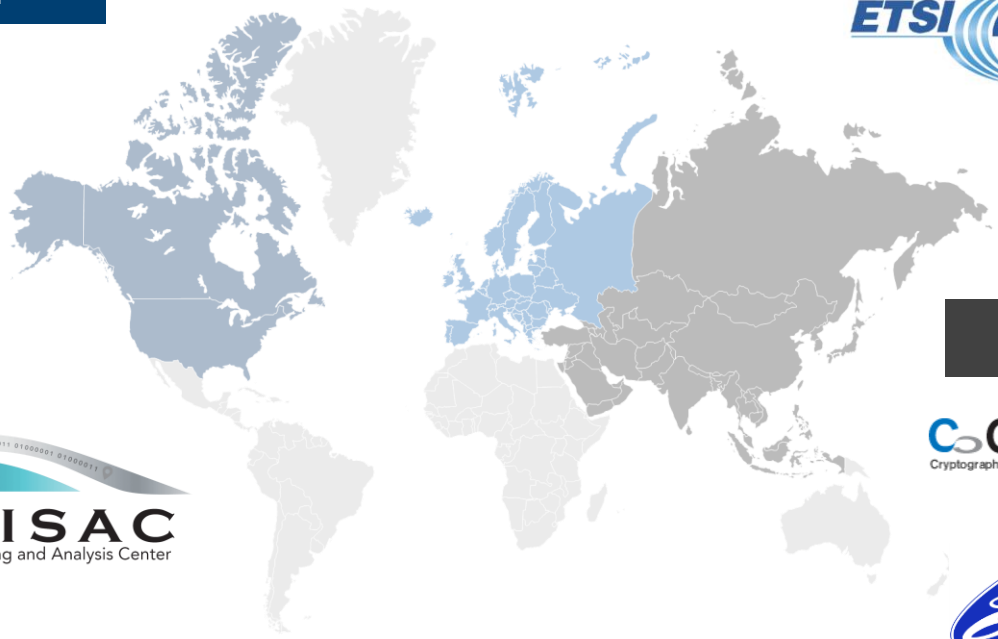
North America

ISO

SAE INTERNATIONAL

NIST

AUTO-ISAC
Automotive Information Sharing and Analysis Center



Asia

CRYPTREC
Cryptography Research and Evaluation Committees

JasPar

SAE OF JAPAN

Key Takeaways

1. Cyber Attacks Increasing
2. Increasing Connectivity → Attack Surface Increasing
3. Increasing Autonomy → Attack Impact Level Increasing

Increasing the need for:

4. Countermeasures – Standards – Methodologies