Cybersecurity Risk in Smart Automobiles

Update for the Board of Directors

TABLE OF CONTENTS


BOOMBA
Go the distance

OUR MEMBERS

John Marcelia
CIO

Duy Pham
CIO

Neha Priyadarshini
CIO

Praveen Kesapragada
CIO

Chandnee K Iyer
CIO

Sandra Li
CIO

Our Product

Our cars are made specifically to go the distance -- so you can road trip in comfort, both physically and mentally.

Our Product

Than the leading EV driving range

Our lowest models staring at only $20k

More details to come


CURRENT
EVENTS

SECURITY RESEARCHERS BREAK INTO TESLA USING A DRONE FLYING OVER THE CAR

Security researchers were successfully able to hack TESLA Model 3 and all other Tesla Models, S, X, and Y by flying a drone over the car carrying a Wifi dongle.

‘SEVERE’ SECURITY ISSUES EXPOSE POPULAR FORD AND VOLKSWAGEN CARS TO HACKERS

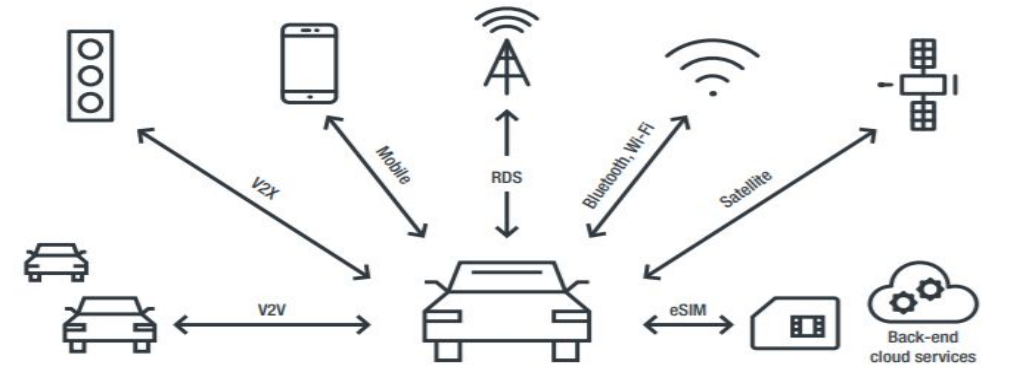
Top-selling Ford and Volkswagen cars have serious security issues that can put users personal data and safety at risk. The vulnerability was found in the car's traction control - a feature to help the driver control the vehicle movement.

FROM A SINGLE TCU TO FULL CONTROL

Security researchers from Pen Test Partners used the telematics connection to compromise the corporate network to obtain full charge of the backend servers using admin credentials.

CYBER-SECURITY RISKS

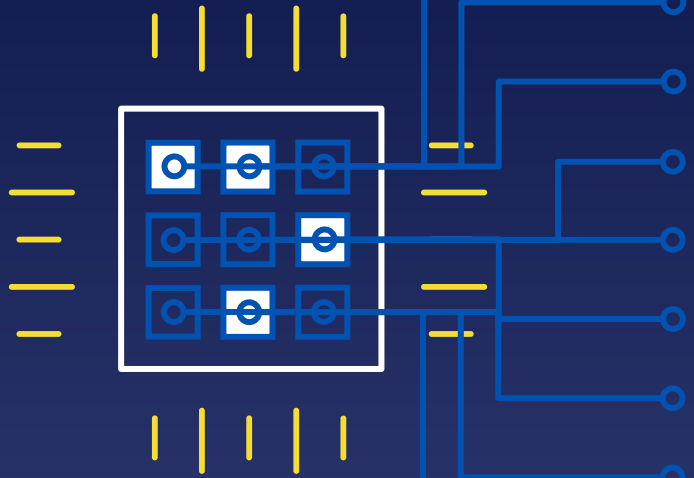
The Smart Automobile



Vehicle internal network

Powertrain	Communications	Body control	Power management	Chassis	Safety
Engine control unit	Head unit	Door locks	Hybrid powertrain	Adaptive suspension	Camera system
Traction control	Mobile connection	Climate control	Battery management	Electronic stability control	Radar/Lidar
Power steering	Telematics	Power window	Energy recovery	Active steering	Airbags
ACC, etc.	GPS, etc.	Sunroof, etc.	Actuators, etc.	Active body control, etc.	Tire pressure monitoring system, etc.

Attack Vectors



- Malicious CAN messages transmitted
- MitM wireless data transmissions
- Electronically jamming radio transmissions
- Exploitation of operating systems' vulnerabilities to compromise systems
- Extract firmware from hardware modules
- Upload of modified/malicious firmware and reflash ECUs
- Exploitation of mobile apps and their back-end servers
- Exploitation of third-party apps installed in the head unit
- Use of cloud APIs to compromise car

THREATS

Engineered Accidents

Auto Theft

Theft of User Data

Hijacking Shipments

System Infiltration

Fleet Fraud

National Threats

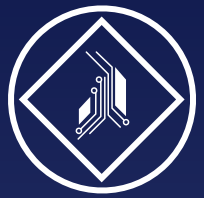
Roadway and Traffic Chaos

Terrorism

Bad Actors

Nation States

Criminal hacking groups



Insiders

Unscrupulous Operators

GAPS & CHALLENGES

Insecure Development

Insecure Design

Lack of security/ privacy-by-design

Insecure Development

Lack of comm protection, authentication / authorization for ECUs

Security Standard

Different actor domains means that there is a lack of security standard

Liability

Multiple Actors

Multiple different actors of the ecosystem: car manufacturers, developers, app stores

No Isolation

Hard to enforce perfect isolation between driving, debug and infotainment

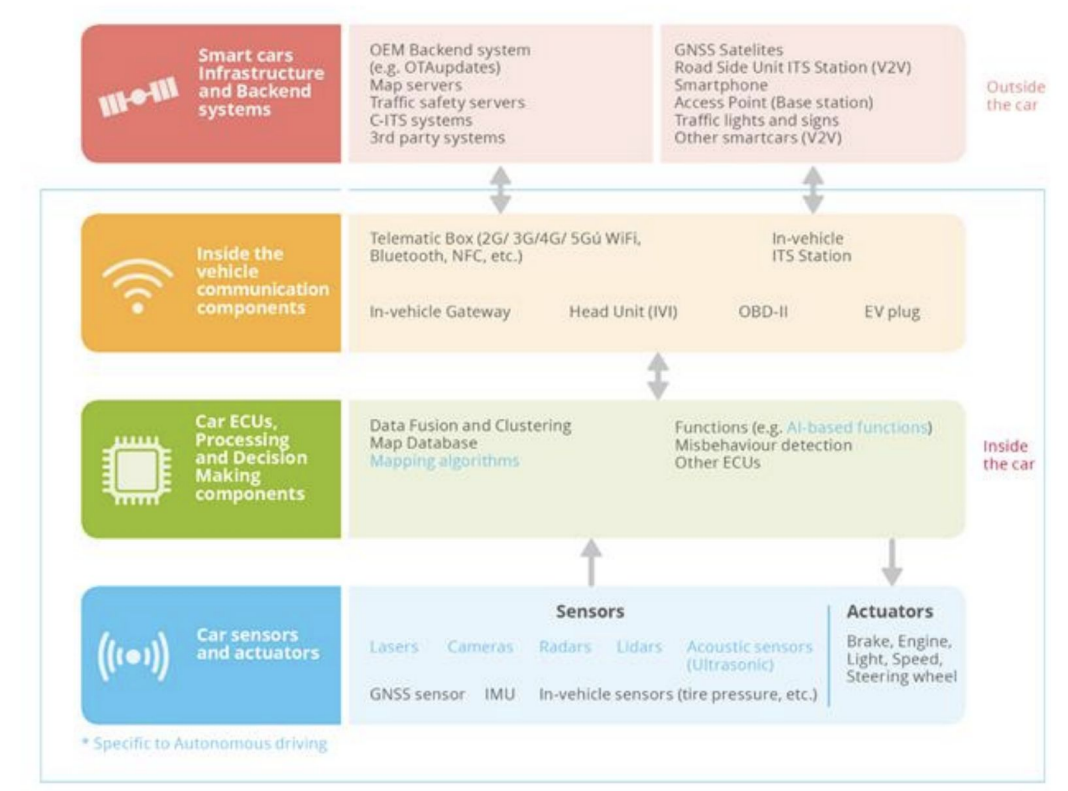
Multiple Entries for Vulnerabilities

Vulnerabilities from any actor can compromise car safety

Mitigations

NIST Framework

Identify



Common Practices

- Identify critical processes
- Continually document information flow
- Keep our software and physical assets up to date

Protect

Physical Assets

Ensure that physical sensors are always performing optimally

Private / Sensitive Data

Always backup data, encrypt it when sending and destroy safely and effectively

Customers & Employees

Train customers and employees to use apps and technologies safely and effectively

Detect

Intrusion Detection Systems

These can help identify threats both at vehicle level and back-end

Perform Inspection Logs

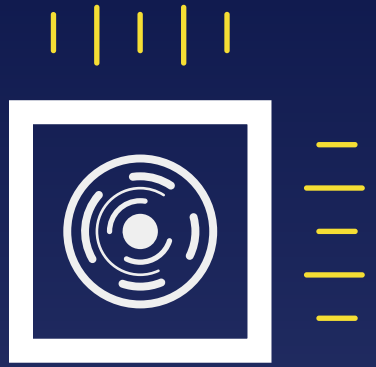
Can prevent disclosures to unknown entities and alert of unauthorized access

Establish Forensic Procedures

Can help with event reconstruction and retrace specific scenarios

Respond

Response Plan



Have to continually test and improve to ensure that:

- Response to incidents happen in a timely manner
- Ensure the safety of passengers and users
- Identify how much & what data was lost if any & isolate the incident
- This type of incident does not happen again

Recover

Communicate

Talk to stakeholders and customers to ensure that the situation is handled and won't happen again

Update

Update recovery plans and current systems to ensure breach does not happen again. Work on being preventive than reactive

Manage

Manage public , customer & supplier relations to ensure that company reputation is upheld

Future Plan

91%

New U.S Car Sales are Connected

Connected smart cars are on the rise in the US, accounting for 13 million purchases last year. Growth in connected cars is expected to only increase

46 Billion

IoT Devices in 2021

This is a 200% increase from 2016 and there will only be more connected devices developed, including those that can connect to smart cars

100%

Increase in IoT Device Hacks

Since last year, Kaspersky research shows a 100% increase in IoT cyberattacks and over 1.5 Billion attacks in just the first 6 months of 2021.

“I think one of the biggest risks for autonomous vehicles is somebody achieving a fleet-wide hack. In principle, if somebody was able to hack, say, all of the autonomous Teslas, they could, say ‘send them all to Rhode Island’ from across the United States. And that would be like, well OK, that would be the end of Tesla. And there would be a lot of angry people in Rhode Island, that’s for sure.”

—Elon Musk

Risk Matrix Chart

Consequence		Likelihood 1 Rare: The event may occur in exceptional circumstances	2 Unlikely: The event could occur sometimes	3 Moderate: The event should occur sometimes	4 Likely: The event will probably occur in most circumstances	5 Almost Certain: The event is expected to occur most circumstances
1	**Insignificant** No injuries or health issues	LOW	LOW	LOW	LOW	MODERATE
2	**Minor** First aid treatment	LOW	LOW	MODERATE	MODERATE	HIGH
3	**Moderate** Medical treatment, potential LTI	LOW	MODERATE	HIGH	HIGH	CRITICAL
4	**Major** Permanent disability or disease	LOW	MODERATE	HIGH	CRITICAL	CATASTROPHIC
5	**Extreme** Death	MODERATE	HIGH	CRITICAL	CATASTROPHIC	CATASTROPHIC

Risk rating:

Low risk: Acceptable risk and no further action required as long as the risk has been minimised as far as possible. Risk needs to be reviewed periodically.

Moderate risk: Tolerable with further action required to minimise risk. Risk needs to be reviewed periodically.

High risk: Tolerable with further action required to minimise risk. Risk needs to be reviewed continuously.

Critical risk: Unacceptable risk and further action required immediately to minimise risk.

Catastrophic: Unacceptable risk and urgent action required to minimise risk.

Risk Rating for this incident

□ LOW RISK	□ MODERATE RISK	□ HIGH RISK	□ CRITICAL RISK	□ CATASTROPHIC
Acceptable with periodic review	Tolerable with periodic review	Tolerable with continuous review	Intolerable	Intolerable

Future Plan Roadmap

Implement Mitigations

Begin implementing controls

Maintain System Updates

Ensure old systems are patched and up to date

2

4

1

3

Fleet Testing

Understand where vulnerabilities exist

Develop Breach Response Team

Put team in place to respond when incidents occur

THANKS!

Questions?