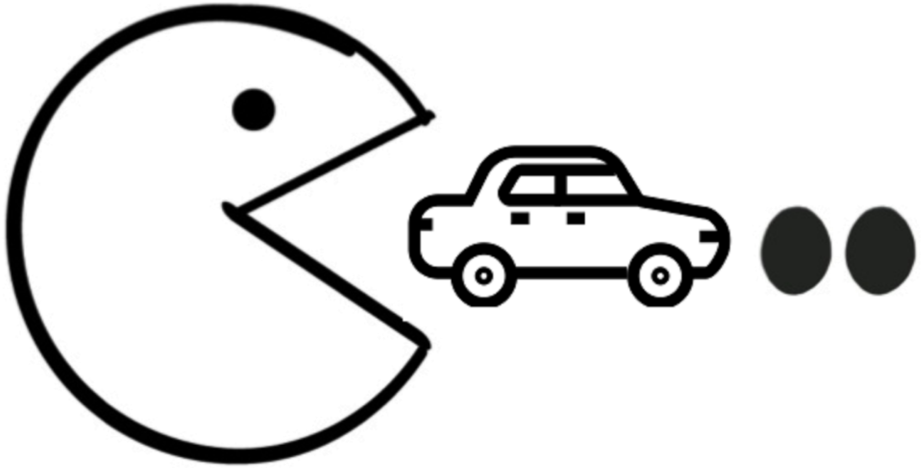


Agile Software Ate My Vehicle

The drive to a more modern and integrated vehicle ecosystem

4-Jun-2021

Why Is This Important?

Cybersecurity Management System

- OEMs and Suppliers are actively engaged in the design, creation, refinement and application of re-architecting the vehicle, connected vehicle ecosystem, autonomous-vehicles, and electrification technology for next-generation products
- These changes are driving the industry toward more software-defined vehicles
- Securing this ecosystem will challenge all of us

Software Update Management System

- Advances in vehicle over-the-air (OTA) updates are already addressing concerns relating to revenue, the ability to introduce new features and services, and upcoming regulatory compliance
- Not only will OTA significantly impact the ability to provide security fixes, but it enables the ability to add features and services
- This will quickly increase with the rollout of 5G network capability

Agenda

1. Reality Check

2. A Digital Vehicle Ecosystem Has Emerged

3. Software BOMs In The Automotive Ecosystem

4. APIs Are Eating Software

5. Time To Deliver On The OTA Promise

6. Securing the Vehicle Ecosystem

7. Time To Shift-Left On Security

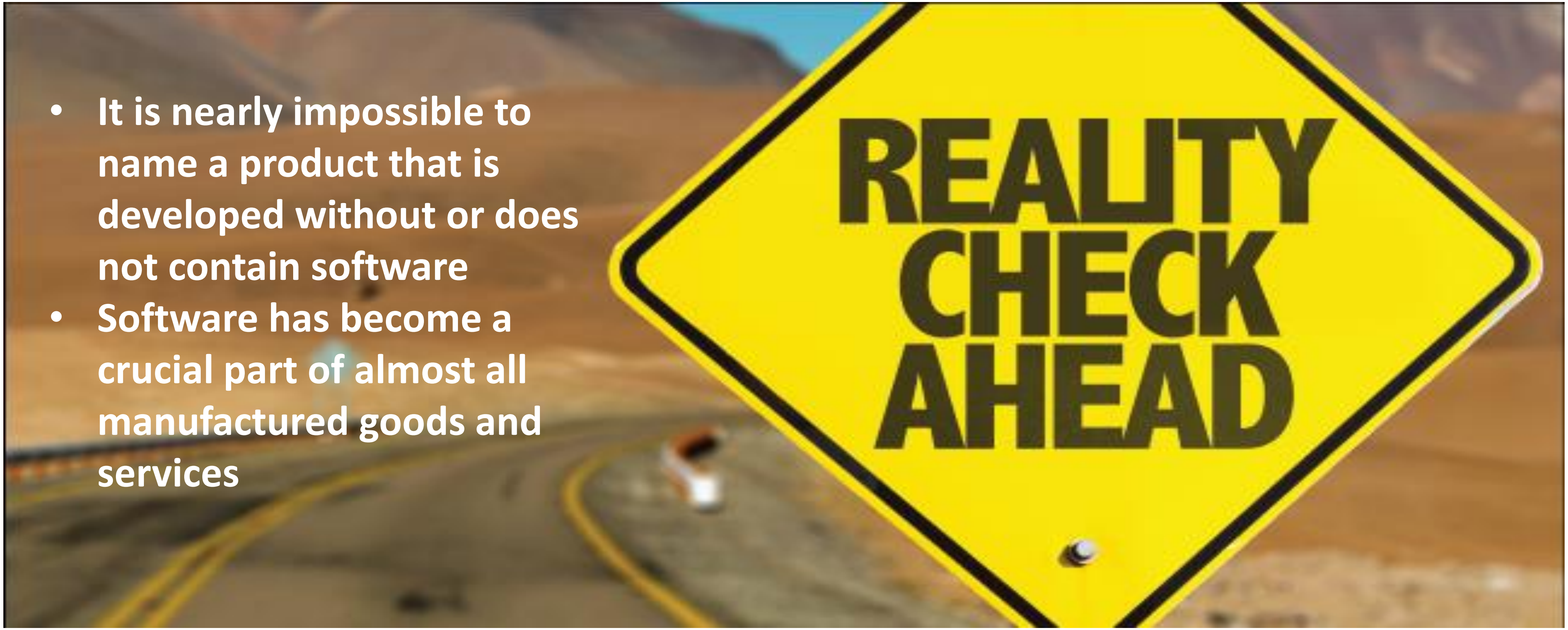
8. Cybersecurity Legislation Friend or Foe?

Presenters Tim Geiger Darren Shelcusky Mike Westra Lisa Boran

Reality Check

Tim Geiger

Software is Pervasive



- It is nearly impossible to name a product that is developed without or does not contain software
- Software has become a crucial part of almost all manufactured goods and services

The Growing Reliance On Software Exposes OEMs To A Multitude Of Threats

Some Important Automotive Metrics

152M
Connected Vehicles
In 2020

7x Growth In Vehicle
Cyber Incidents
2010-2020

$85.4B
Commercial
Telematics
Market In 2024

2.8B
5G
Connections
By 2025

75%
Cyber attacks
target APIs

$600B
Cybercrime is more
profitable than the
global illegal drug trade

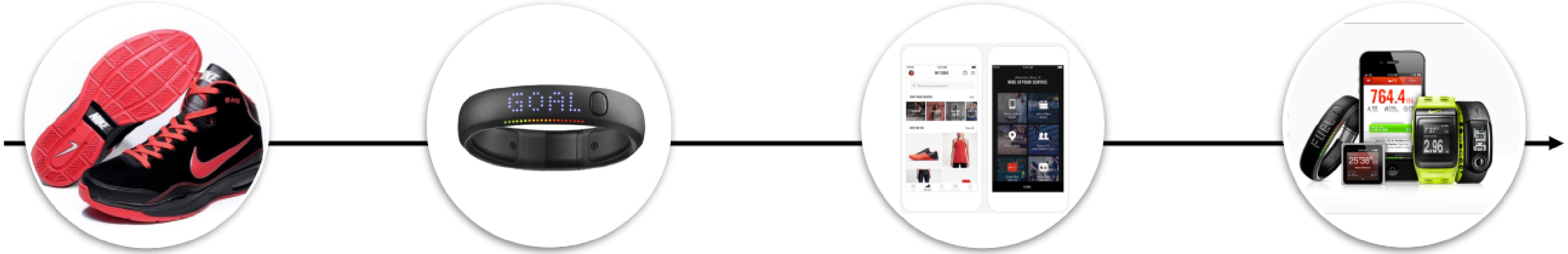
25,000
Charging Stations
In 2020

android

7
# OEMs Adopting
Android
Automotive OS

86% of all vehicles will be connected in the global automotive market in 2025

From Shoeware to Software….



In 2006, to expand their shoe ecosystem and become part of their customer's journey, Nike entered the digital gadget realm by introducing a small sole-insertable chip.

In 2012, Nike created the Fuelband that users wore on their wrists and worked in parallel with Apple's iPhone.

Nike recognized that Apple hardware was more sophisticated and the adoption rates of mobile phones were higher than fitness wearables, so **2014** was the end of the Fuelband. Leaving the hardware to Apple and developing its own software, Nike's mobile app platform, Nike+, came out as the winner.

Today, having built an in-house digital team, Nike has launched a myriad of Nike+ mobile application platforms that collects users' real-time data while integrating themselves into users' fitness lives.

Source: APIdays Paris 2019

Almost Every Major Industry Is Now Software Driven

The Agile Opportunity

The practice of continuous software delivery allows OEMs to provide a stream of innovations throughout the life of a vehicle

The Challenge: We Must Prevent This From Happening…

The Ultimate Question

What Is An Acceptable Level Of Risk?

Tim Geiger

A Digital Vehicle Ecosystem Has Emerged

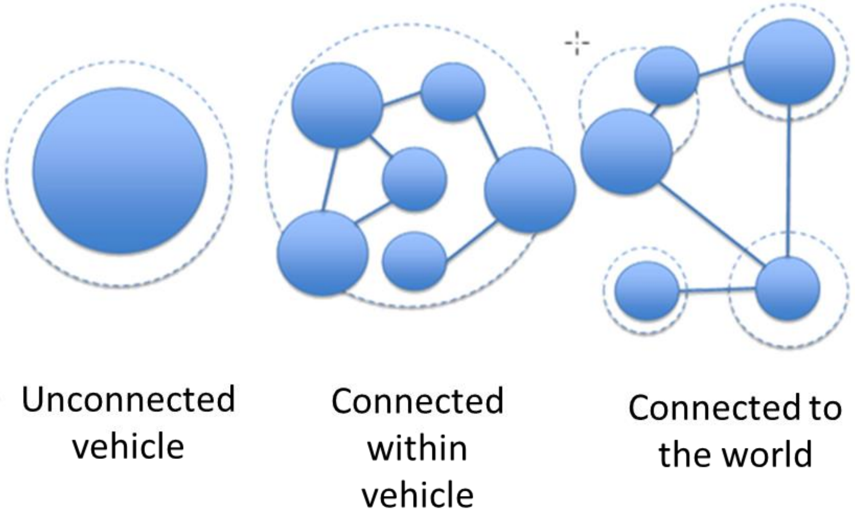
AUTOMOTIVE DIGITAL TRANSFORMATION IS YEARS AWAY. I DON'T SEE OUR COMPANY HAVING TO CHANGE ANY TIME SOON.
CYBERSECURITY
TOM FISH BURNE
© marketoonist.com

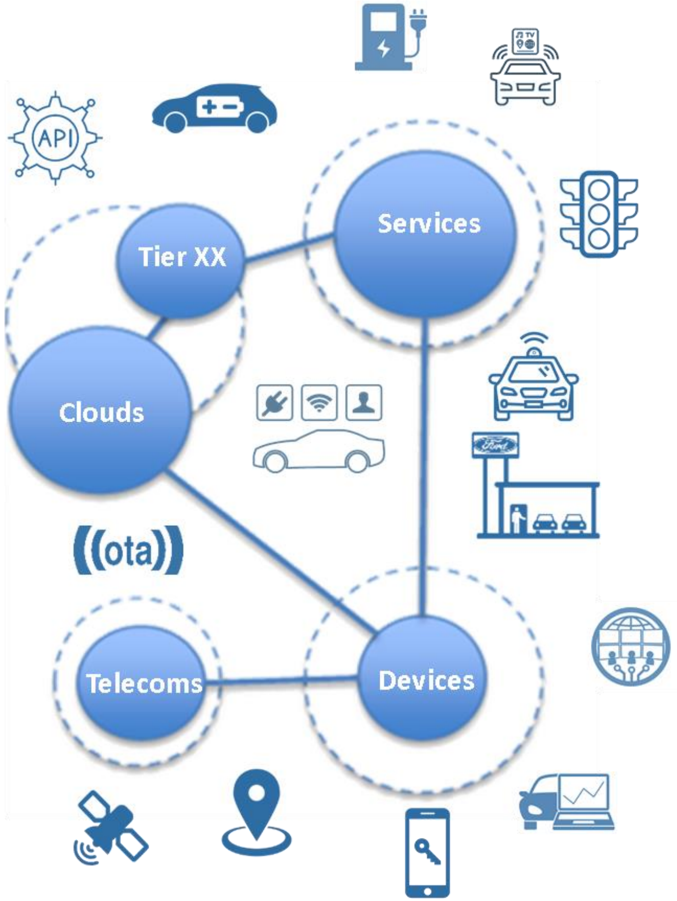
Cybersecurity Has Become A Critical Part of the Business

AGENDA
• WARRANTY
• CUSTOMER SAT
• RECALLS
• INVESTMENT
WHAT DID I TELL YOU? WE'VE BECOME A VITAL PART OF THE BUSINESS STRUCTURE!
Board of Directors
www.jklossner.com
©02 Klossner

CYBER SECURITY

Ecosystems Are Key To Digital Transformations

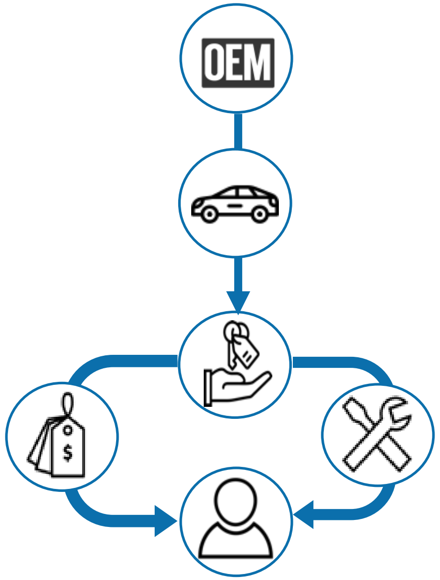




Digital Ecosystems Are A Key Enabler Of Digital Transformation And Are Driving Changes In Software Architectures

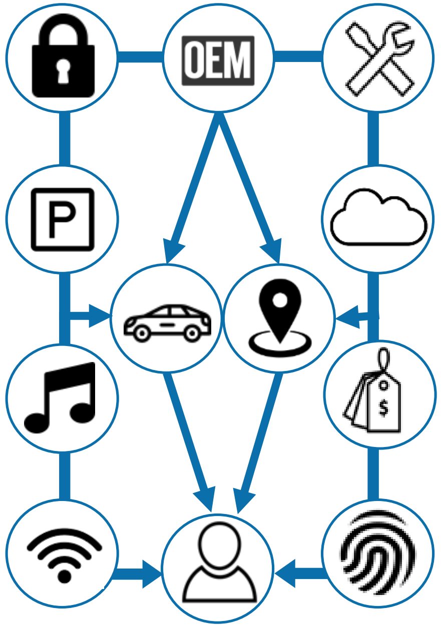
Vehicle's Are Morphing Into The Automotive Ecosystem

Vehicle as a Product



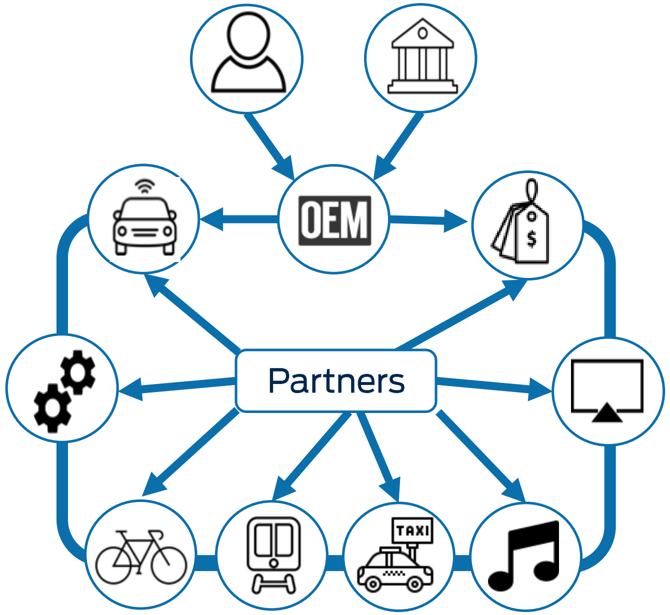
- Mixed levels of vehicle connectivity
- Product ownership is at the center

Vehicle as a Platform



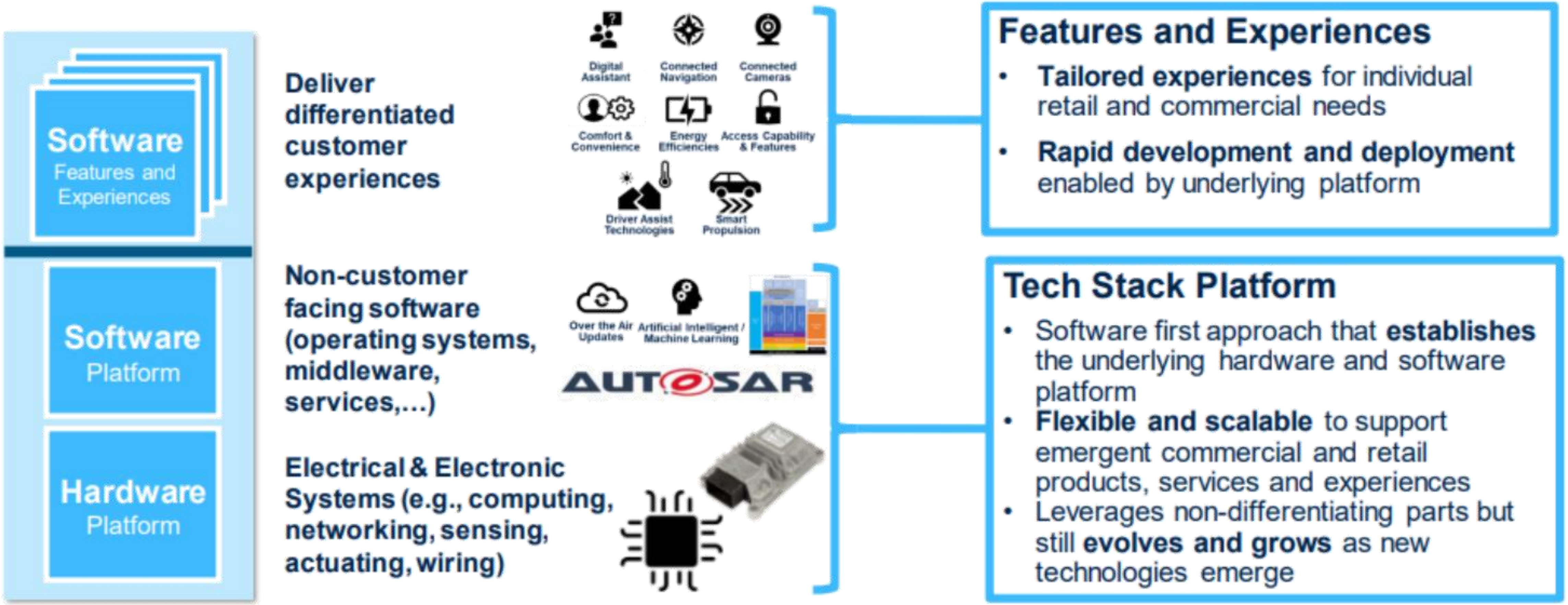
- Majority of vehicles connected
- Consumer interactions built on platforms

An Ecosystem



- Connectivity is ubiquitous
- Customer experiences via OEM's ecosystem of services

Software Is Abundant In A Vehicle Tech Stack



Deliver differentiated customer experiences

Non-customer facing software (operating systems, middleware, services,...)

Electrical & Electronic Systems (e.g., computing, networking, sensing, actuating, wiring)

Features and Experiences

- **Tailored experiences** for individual retail and commercial needs
- **Rapid development and deployment** enabled by underlying platform

Tech Stack Platform

- Software first approach that **establishes** the underlying hardware and software platform
- **Flexible and scalable** to support emergent commercial and retail products, services and experiences
- Leverages non-differentiating parts but still **evolves and grows** as new technologies emerge

A Tech Stack Establishes A Platform That Enables Software For Commercial And Retail Products, Services, And Experiences

Darren Shelcusky

Software BOMs
In The Automotive Ecosystem

The Invisible Man Problem

Software and cybersecurity are essentially invisible within most manufactured products

This visualization problem is a source of many potential and real failures

Software BOMs Are Key To Cybersecurity

- Today, software makes up **10%** of a vehicle's bill-of-materials
- Vehicle software is expected to grow at **11% CAGR** and will represent **30%** of a vehicle's BOM by 2030
- Software BOMs are being considered by regulatory agencies to streamline the process of identifying component vulnerabilities
- WP.29 regulations **requires** OEMs to demonstrate supplier-related cybersecurity risks

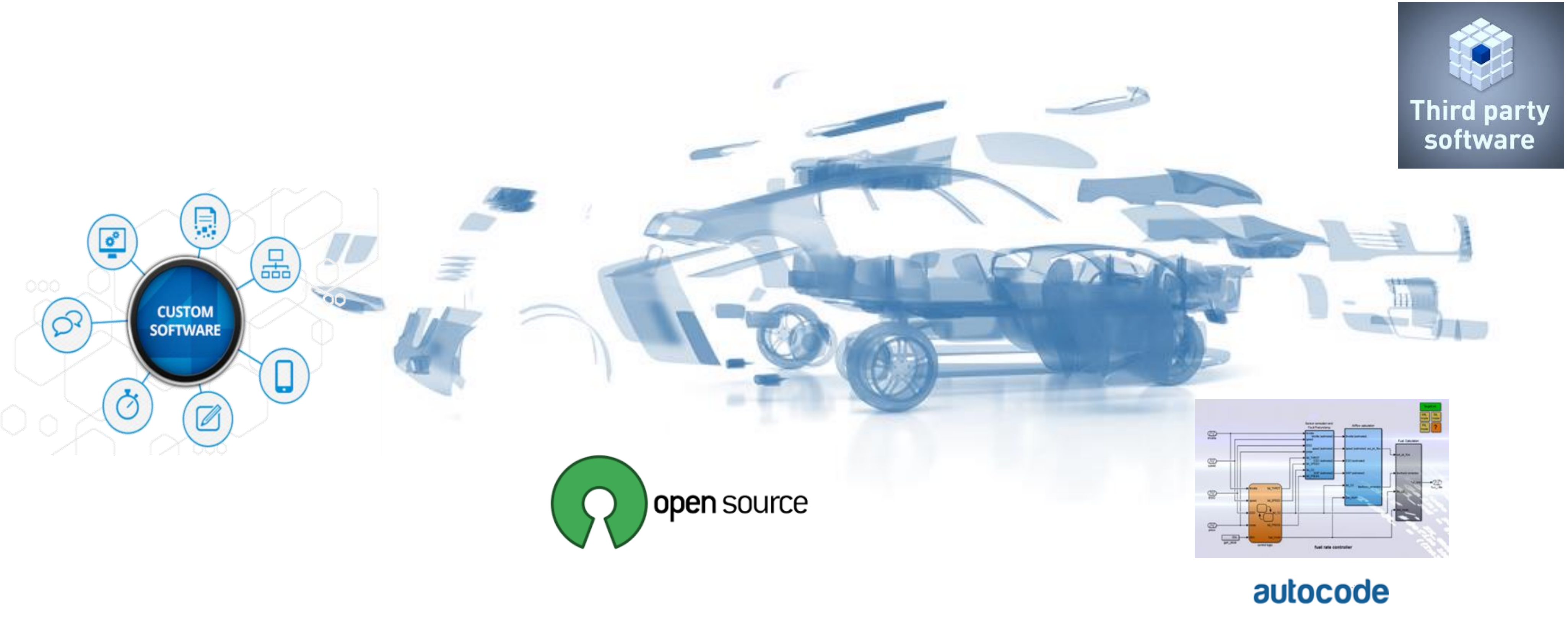
A Software Bill Of Materials Can Uncover Security Vulnerabilities And Build A Foundation For Better Cybersecurity

Cybersecurity And The Software Supply Chain

- OEMs will require suppliers (Tier 1/2/3) to demonstrate compliance with vehicle cybersecurity regulations
- This means that each supplier product that goes into a vehicle containing software must come with evidence that it complies with UNECE WP.29 cybersecurity regulations
- If a supplier cannot provide evidence, it will become increasingly difficult for OEMs to accept or integrate their products into UNECE WP.29 compliant vehicles

OEMs Must Attest And Take Responsibility For The Cybersecurity Implementation By Their Suppliers

Vehicle Software Sources

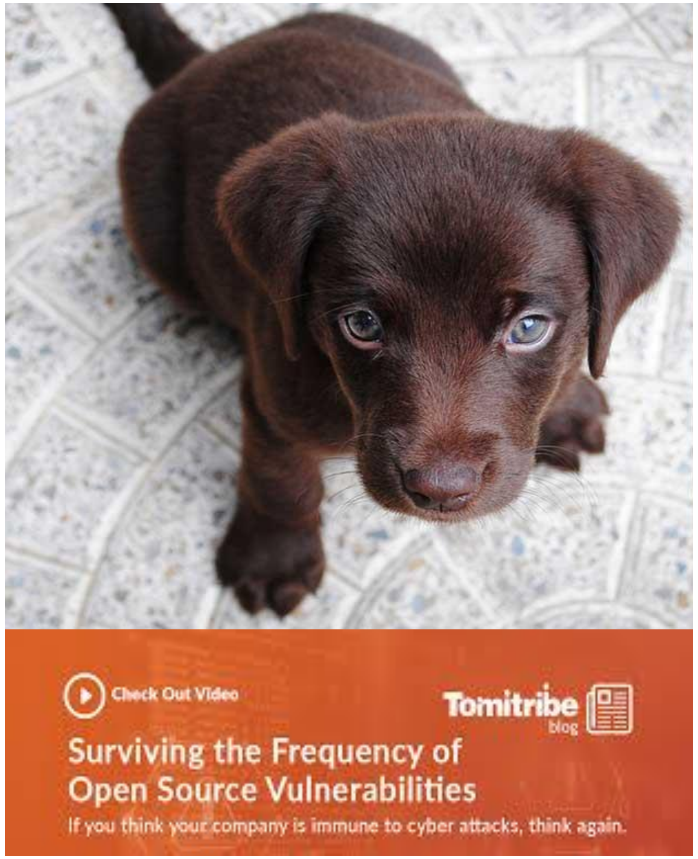


Onboard + Offboard

OEMs Must Maintain An Accurate Software BOM To Ensure Their Vehicle Ecosystem Is Compliant With Cyber Regulations

Open-Source Software ‘Is free like a puppy is free'

- The work and expense begin once you bring the puppy home, you also bring home the puppy’s problems
- Open-source software plays a key role in the development of the automotive ecosystem
- **49%** percent of the code bases contained high-risk vulnerabilities
- **91%** of code bases contained components that either were more than **4 years out of date** or had no development activity in the past 2 years
- **68%** of code bases contain some form of open source
- Software products require automated solutions to identify CVEs


Check Out Video
Tomitribe
blog
Surviving the Frequency of
Open Source Vulnerabilities
If you think your company is immune to cyber attacks, think again.

Open-Source Saves Time And Increases Delivery Speed, But It Potentially Comes With An Increase In The Volume Of Vulnerabilities

Approach: Software Composition Analysis (SCA)

- Virtually all products include 3rd party components, including open-source, commercial software, auto generated code, and internally developed software
- Open-source software represents a weak link in the supply chain that provides a point of entry for attackers
- SCA tools analyze 3rd party and open-source for vulnerabilities, licenses, and operational factors
- SCA tools can scan software binaries in the absence of source code

Modern software is a patchwork quilt of components

A Comprehensive Software Security Program Contains Both SAST And SCA

Darren Shelcusky

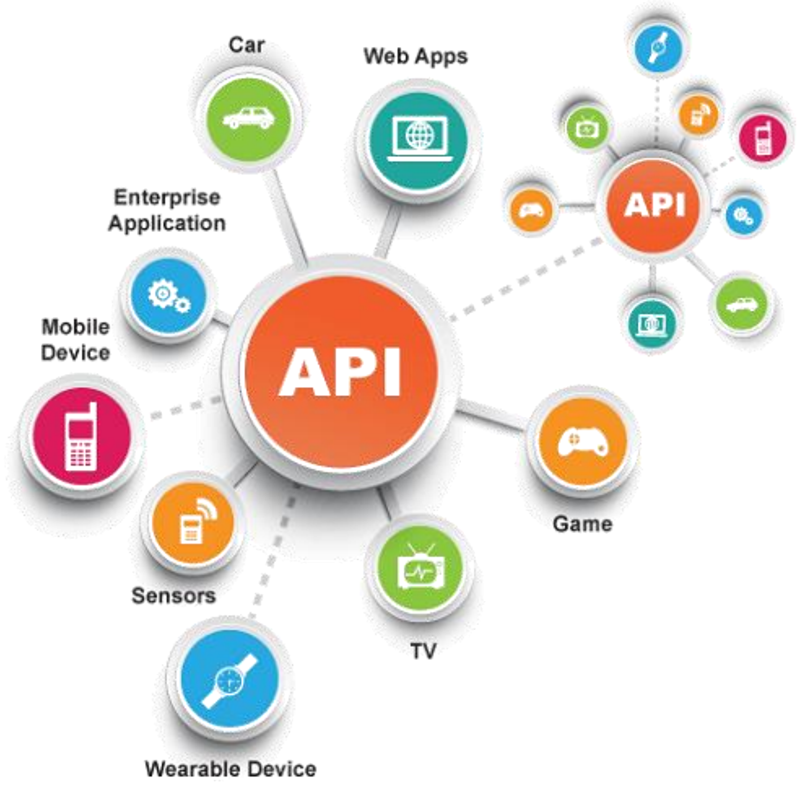
Ford

Vehicle & Connected Cybersecurity

APIs Are Eating Software

Apparently our open API is giving our customers unprecedented control over their own lives and allowing them to seize control of their destinies. So please shut it down.

What Is So Special About APIs?

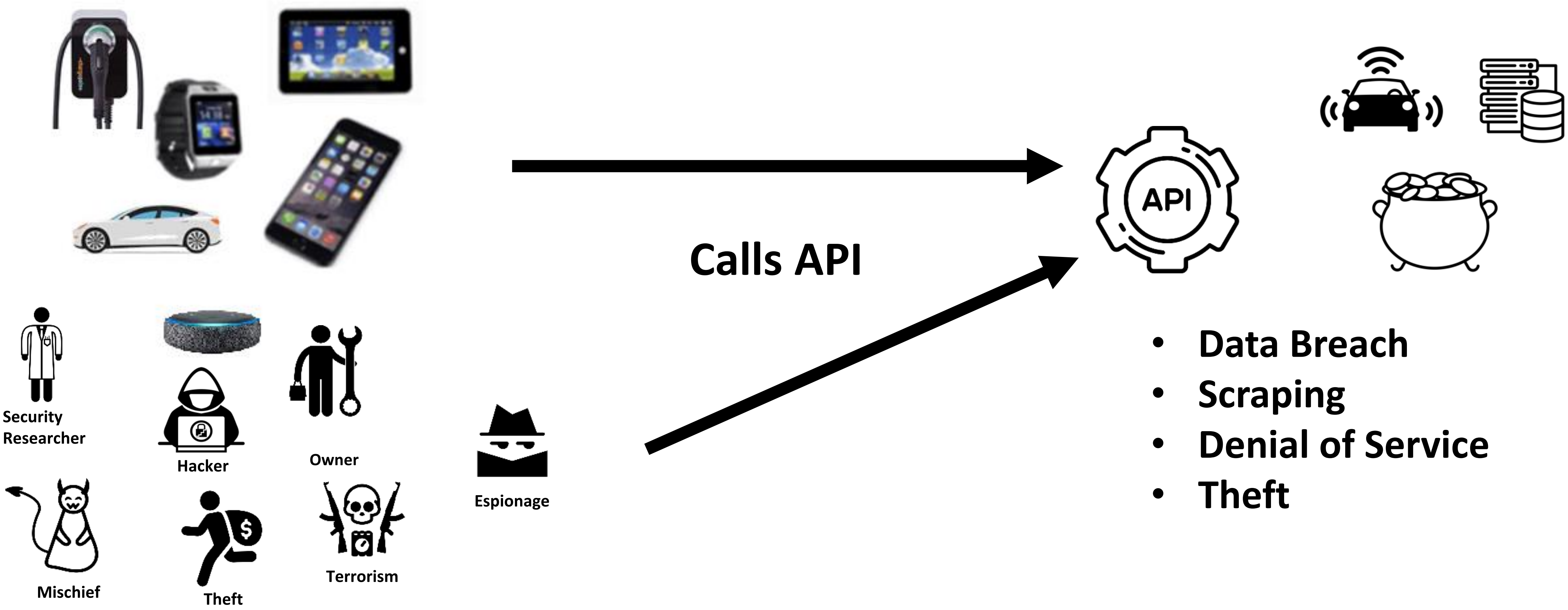


APIs are best thought of as contracts, they define exactly how two pieces of software will interact just like a well written legal document

APIs are the backbone of digital ecosystems

Today Entire Business Models Are Based On The Exchange Of Information Via APIs

Attackers Are Eating APIs



- Data Breach
- Scraping
- Denial of Service
- Theft

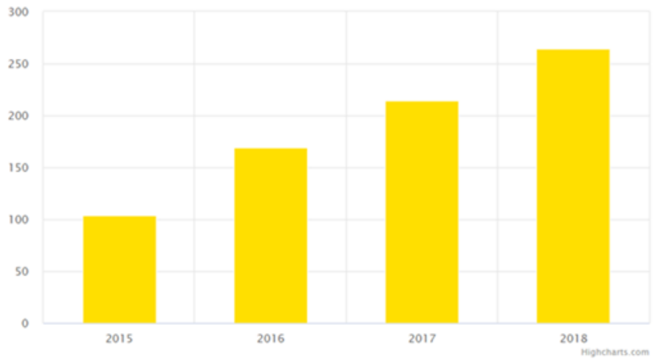
Attackers Go To Where The Data Is

Some Important API Metrics

BOTs represent up to **60%** of web traffic

Why is retail the most attacked target? Money…

83% of web traffic is API data

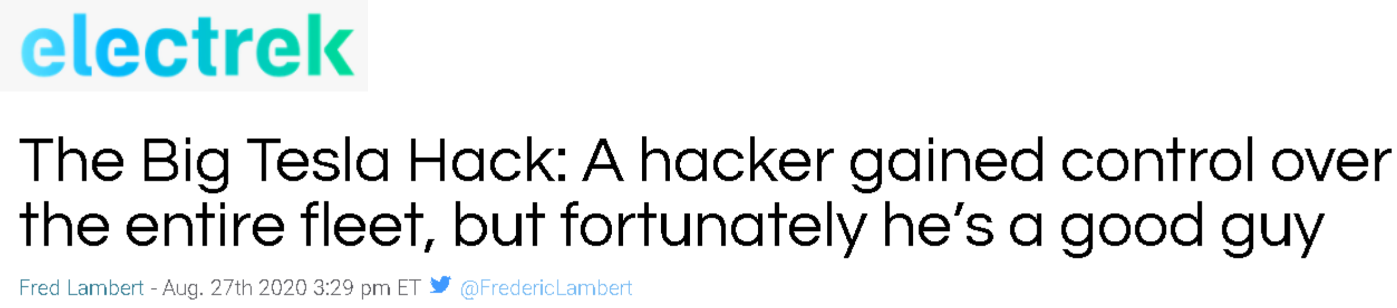


"APIs will be the **most frequently attacked vector** for enterprise web application data breaches by 2022" - Gartner

75% of attacks target APIs

Source: Akamai state of internet security

API Breaches Become Front Page News



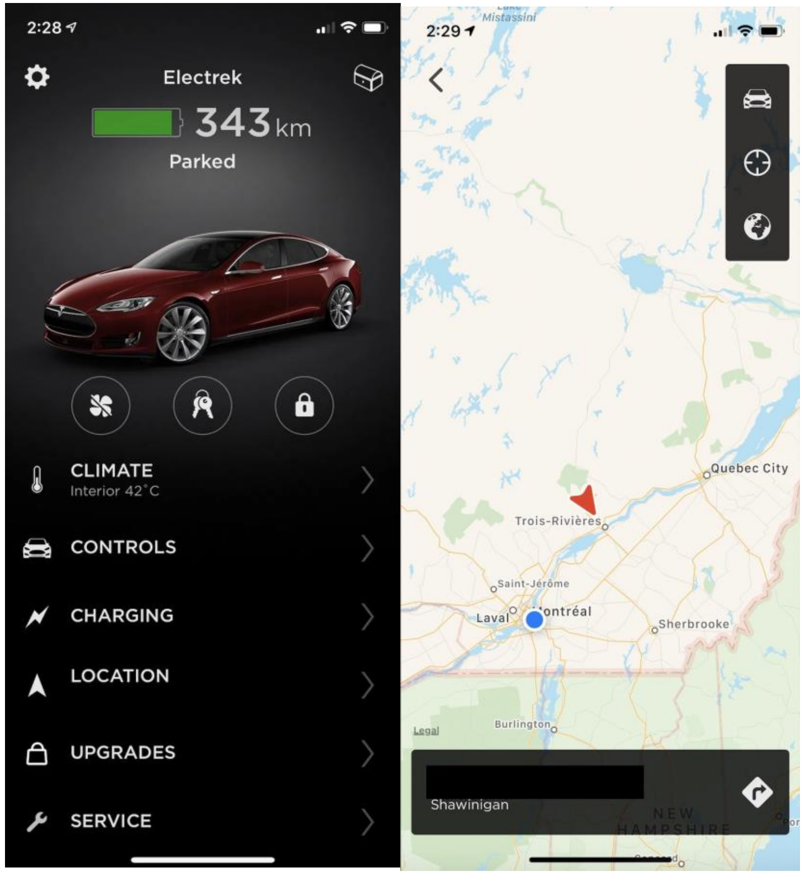
electrek

The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy

Fred Lambert - Aug. 27th 2020 3:29 pm ET @FredericLambert

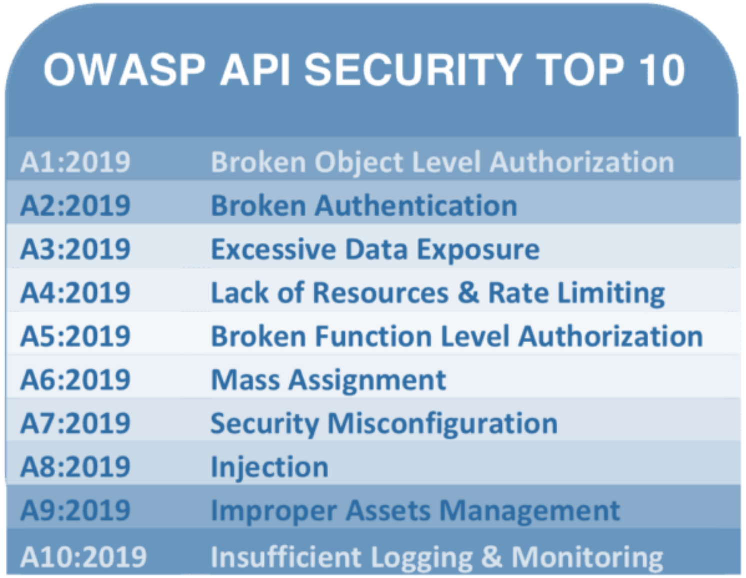
"I found a hole in the server-side of that mechanism that allowed me to basically get data for every Supercharger worldwide about once every few minutes."

All he needed was a vehicle's VIN number, and he had access to all of those through Tesla's "tesladex" database, and he could get information about any car in the fleet and even send commands to those cars.

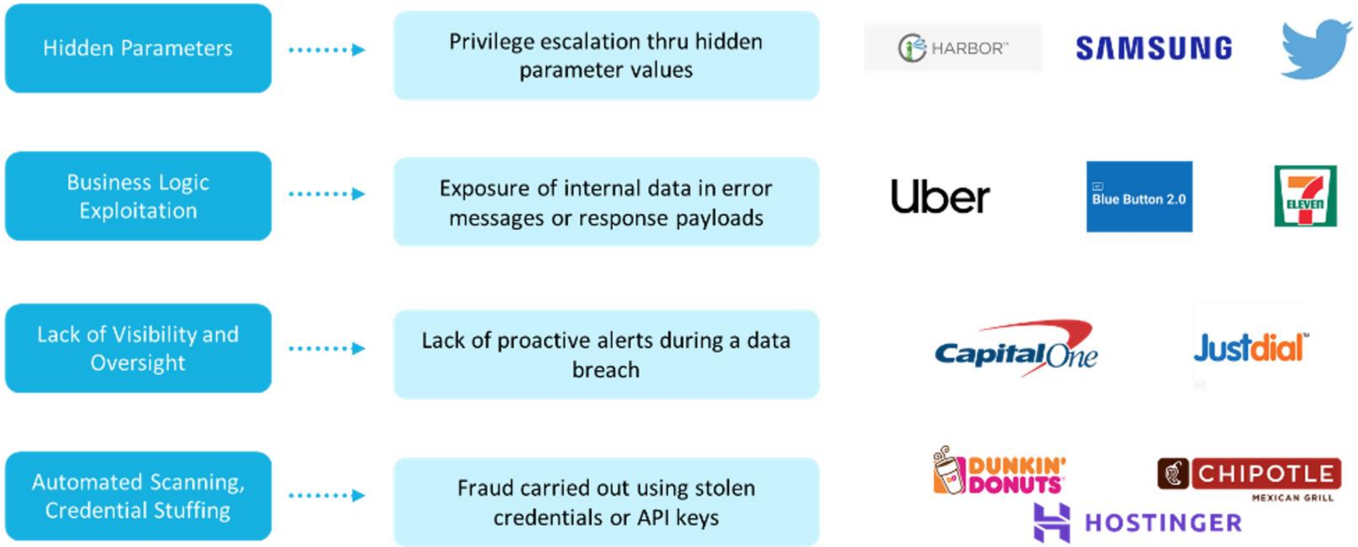


Source:https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/

APIs Have Their Own Unique Threats



OWASP API SECURITY TOP 10	
A1:2019	Broken Object Level Authorization
A2:2019	Broken Authentication
A3:2019	Excessive Data Exposure
A4:2019	Lack of Resources & Rate Limiting
A5:2019	Broken Function Level Authorization
A6:2019	Mass Assignment
A7:2019	Security Misconfiguration
A8:2019	Injection
A9:2019	Improper Assets Management
A10:2019	Insufficient Logging & Monitoring



Hidden Parameters → Privilege escalation thru hidden parameter values

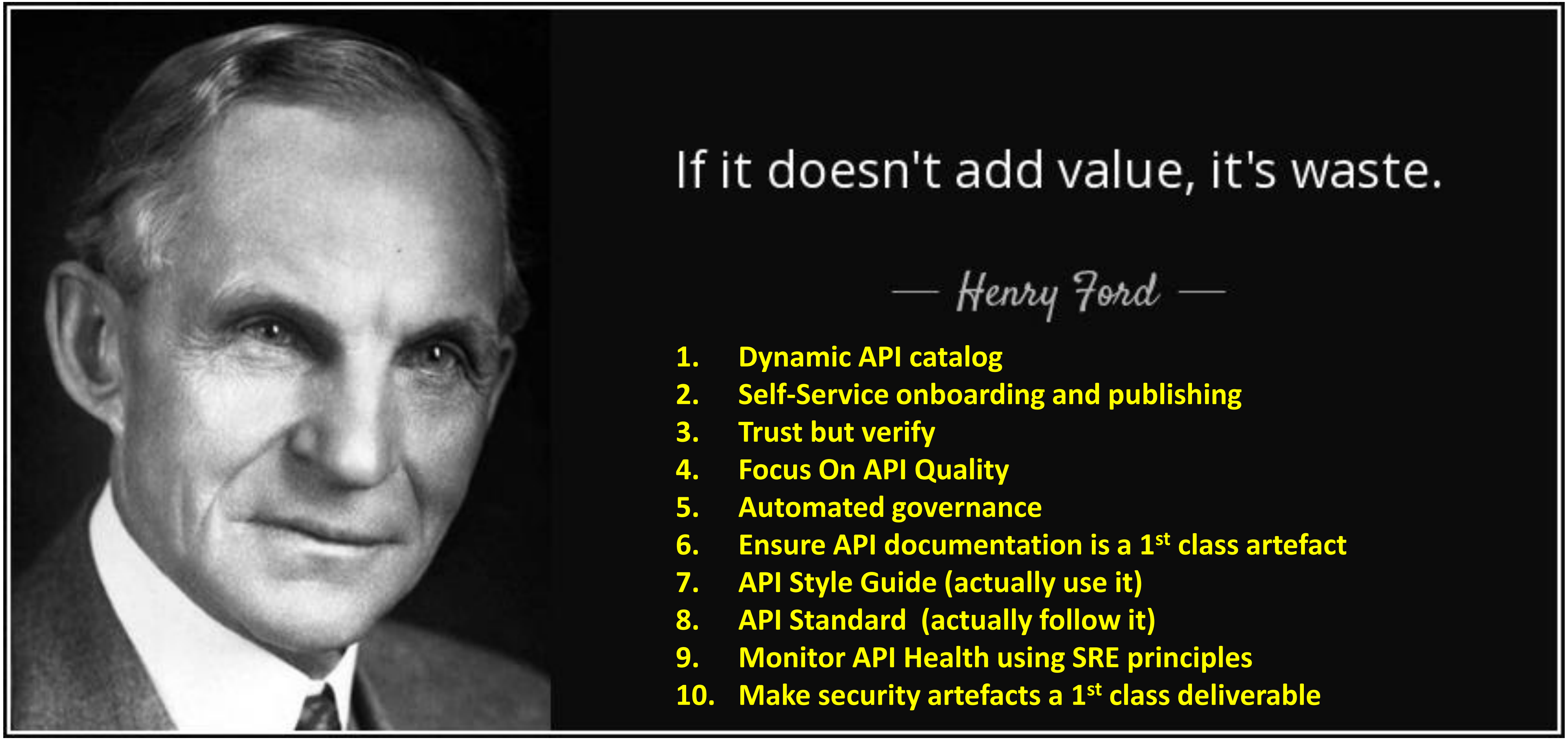
Business Logic Exploitation → Exposure of internal data in error messages or response payloads

Lack of Visibility and Oversight → Lack of proactive alerts during a data breach

Automated Scanning, Credential Stuffing → Fraud carried out using stolen credentials or API keys

API Vulnerabilities Impact All Industries and Digital Ecosystems

Make The Right Thing The Easiest Thing To Do



If it doesn't add value, it's waste.

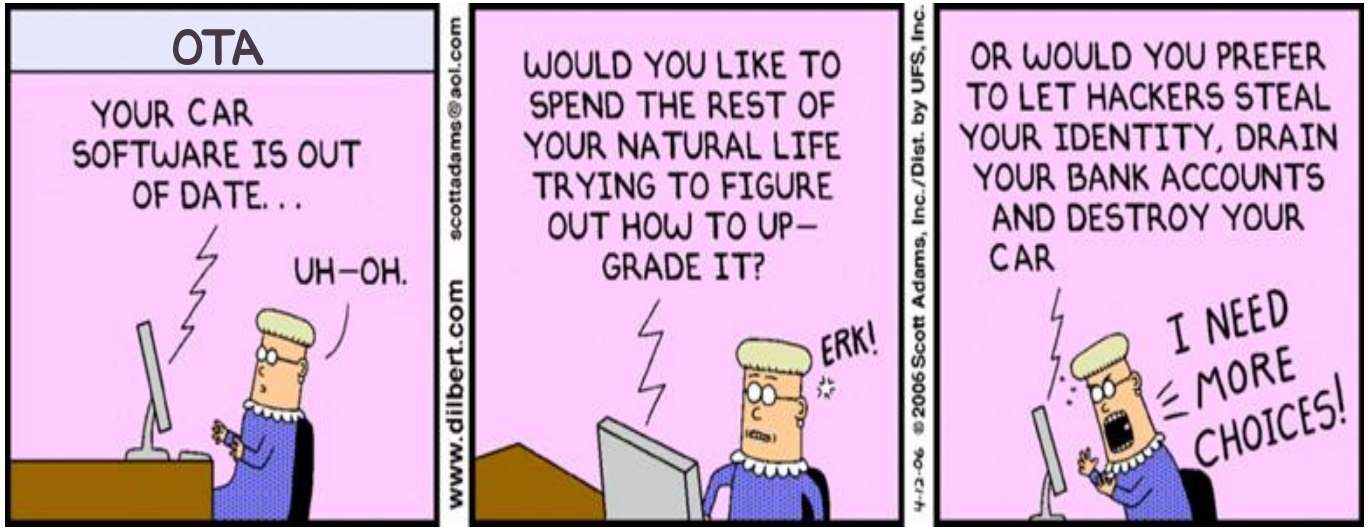
— Henry Ford —

1. Dynamic API catalog
2. Self-Service onboarding and publishing
3. Trust but verify
4. Focus On API Quality
5. Automated governance
6. Ensure API documentation is a 1st class artefact
7. API Style Guide (actually use it)
8. API Standard (actually follow it)
9. Monitor API Health using SRE principles
10. Make security artefacts a 1st class deliverable

Darren Shelcusky

Vehicle & Connected Cybersecurity

Time To Deliver On The OTA Promise

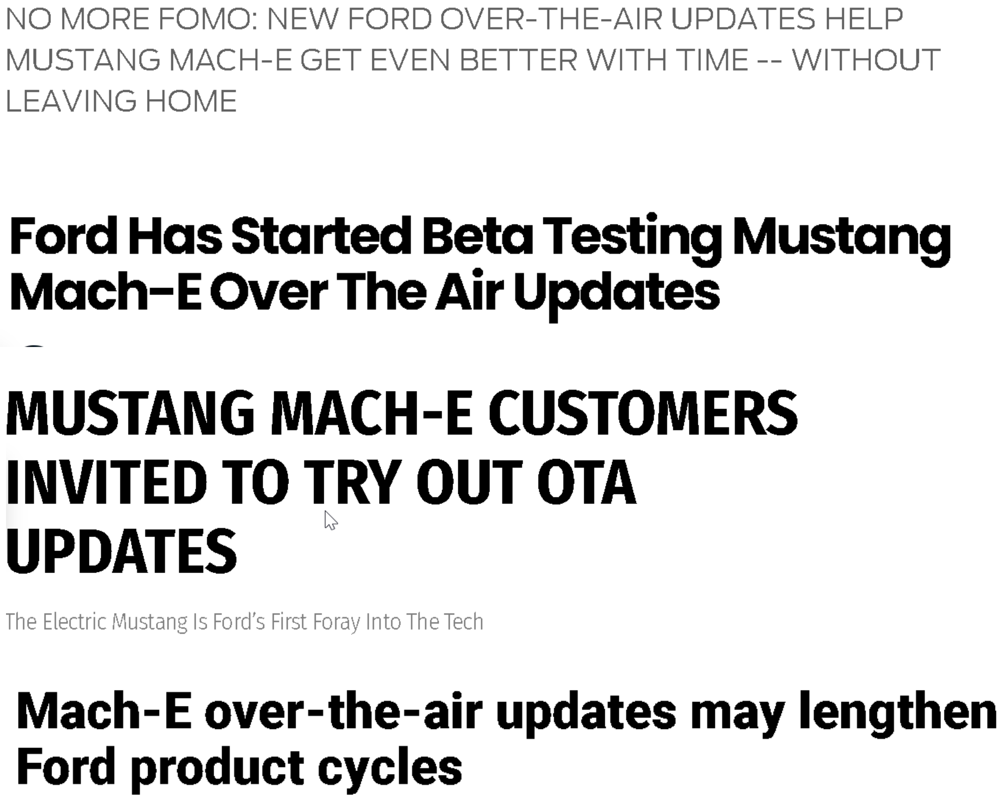

OTA
YOUR CAR SOFTWARE IS OUT OF DATE...
UH-OH.
WOULD YOU LIKE TO SPEND THE REST OF YOUR NATURAL LIFE TRYING TO FIGURE OUT HOW TO UPGRADE IT?
ERK!
OR WOULD YOU PREFER TO LET HACKERS STEAL YOUR IDENTITY, DRAIN YOUR BANK ACCOUNTS AND DESTROY YOUR CAR
I NEED MORE CHOICES!

scottadams@aol.com

www.dilbert.com

4-12-06 © 2006 Scott Adams, Inc./Dist. by UFS, Inc.

Modern Vehicles Require More Frequent Software Updates


NO MORE FOMO: NEW FORD OVER-THE-AIR UPDATES HELP MUSTANG MACH-E GET EVEN BETTER WITH TIME -- WITHOUT LEAVING HOME

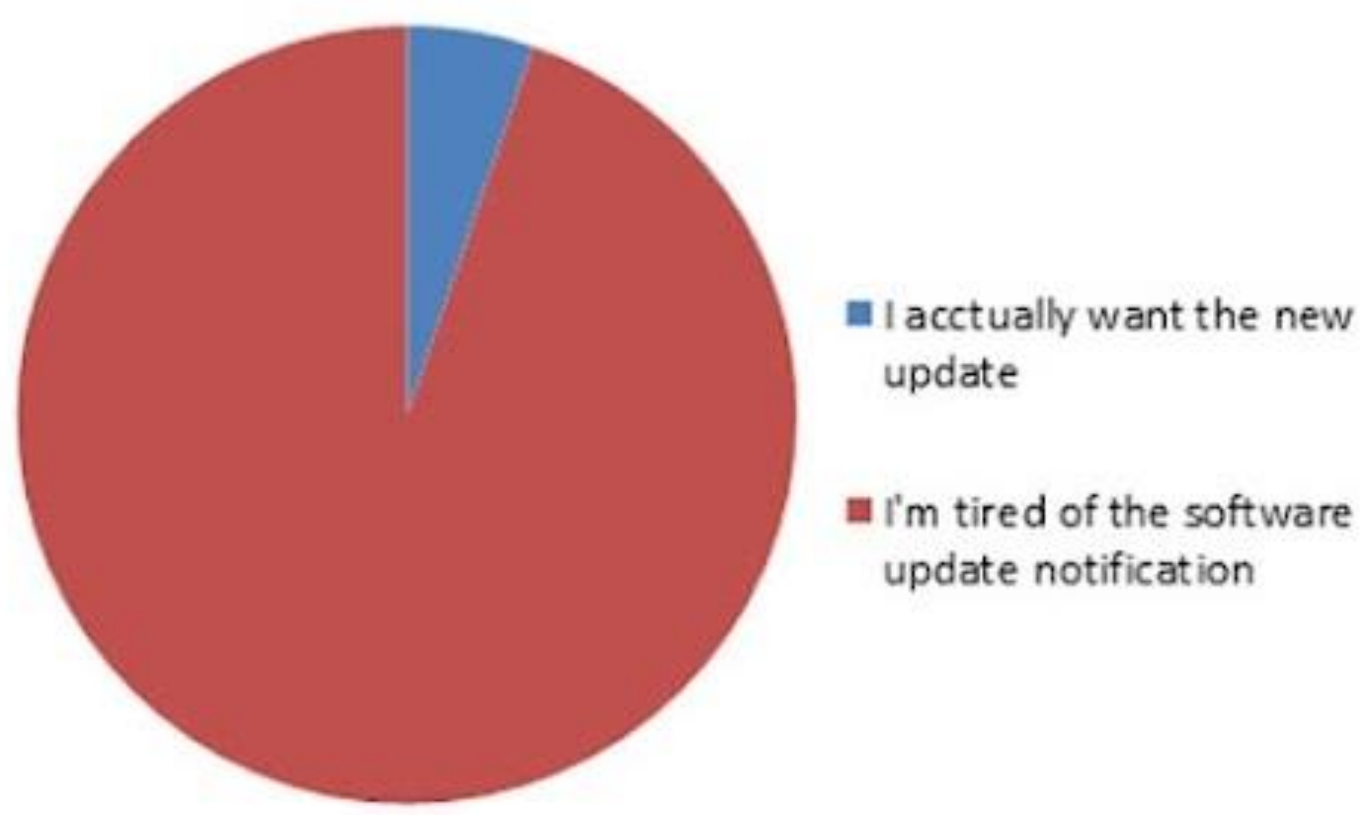
Ford Has Started Beta Testing Mustang Mach-E Over The Air Updates

MUSTANG MACH-E CUSTOMERS INVITED TO TRY OUT OTA UPDATES

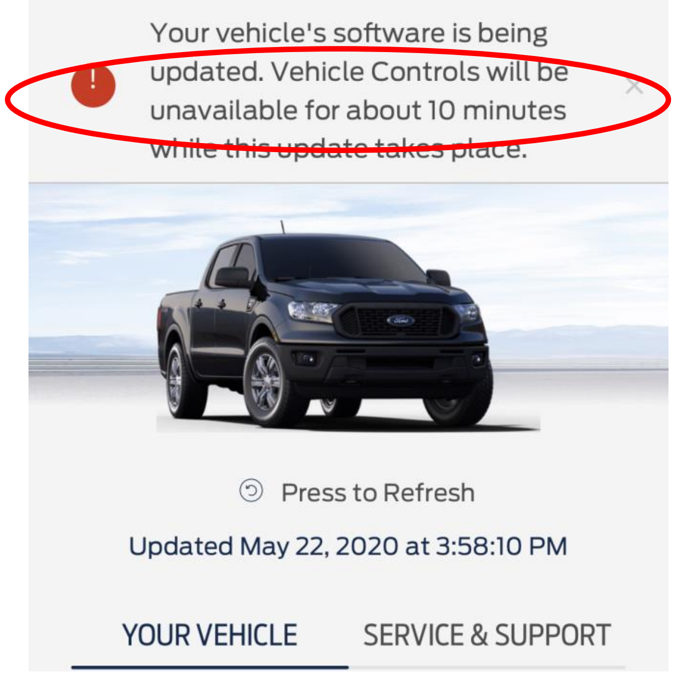
The Electric Mustang Is Ford's First Foray Into The Tech

Mach-E over-the-air updates may lengthen Ford product cycles

Reasons Why People Update Software



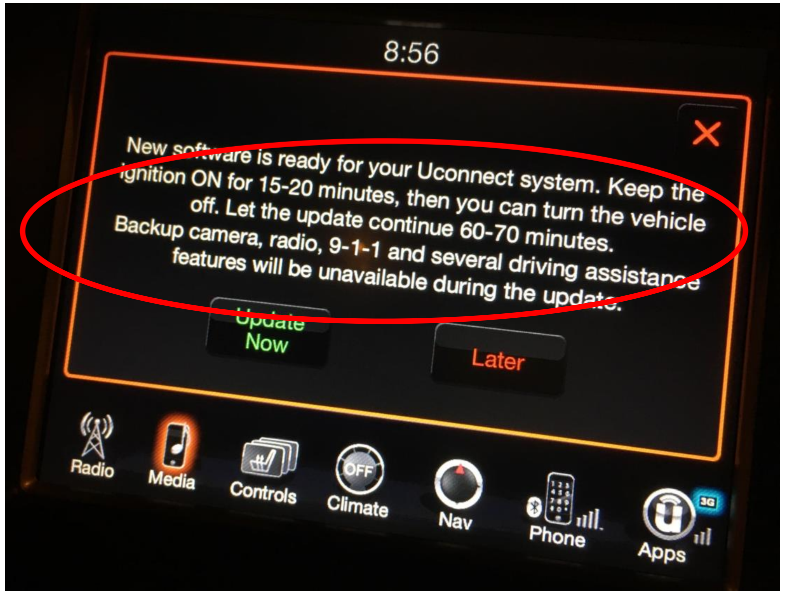
Updates Can Create Poor Customer Experiences



Your vehicle's software is being updated. Vehicle Controls will be unavailable for about 10 minutes while this update takes place.

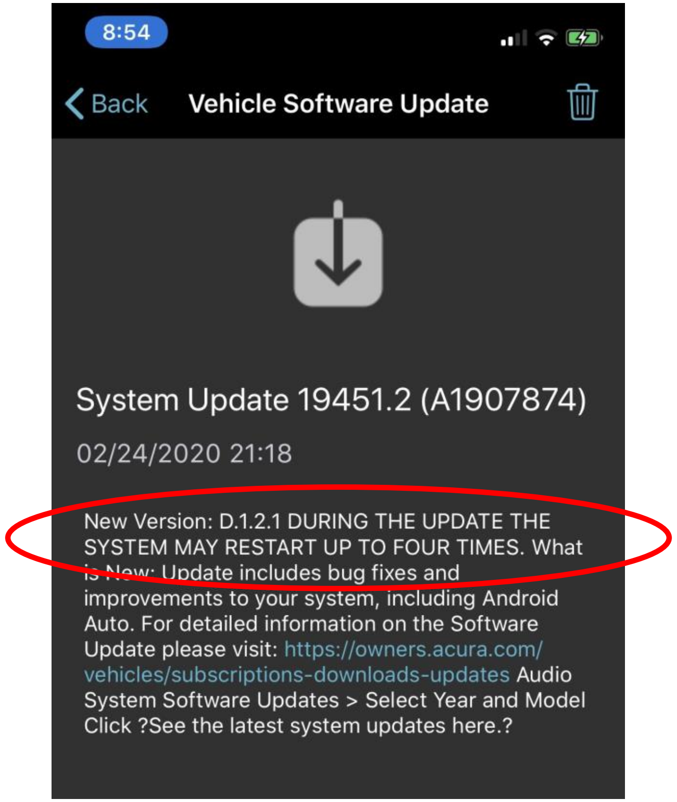
Press to Refresh

Updated May 22, 2020 at 3:58:10 PM



8:56

New software is ready for your Uconnect system. Keep the ignition ON for 15-20 minutes, then you can turn the vehicle off. Let the update continue 60-70 minutes. Backup camera, radio, 9-1-1 and several driving assistance features will be unavailable during the update.



Vehicle Software Update

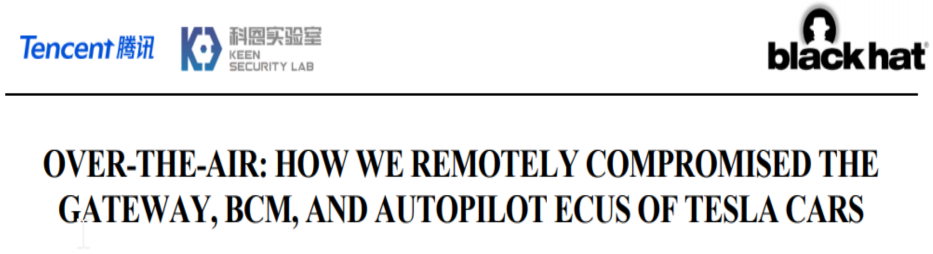
System Update 19451.2 (A1907874)

02/24/2020 21:18

New Version: D.1.2.1 DURING THE UPDATE THE SYSTEM MAY RESTART UP TO FOUR TIMES. What is New: Update includes bug fixes and improvements to your system, including Android Auto. For detailed information on the Software Update please visit: https://owners.acura.com/vehicles/subscriptions-downloads-updates Audio System Software Updates > Select Year and Model Click ?See the latest system updates here.?

Building A Robust And Customer Friendly Update Platform Is Complex

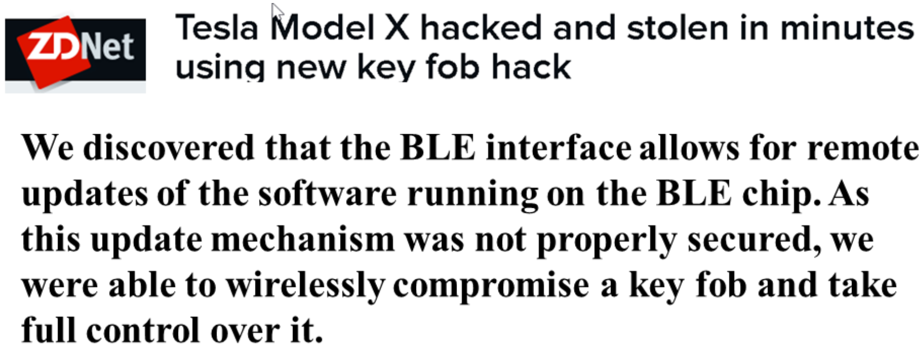
The Update Software Process Can Introduce Vulnerabilities



Tencent 腾讯 科恩实验室 KEEN SECURITY LAB black hat

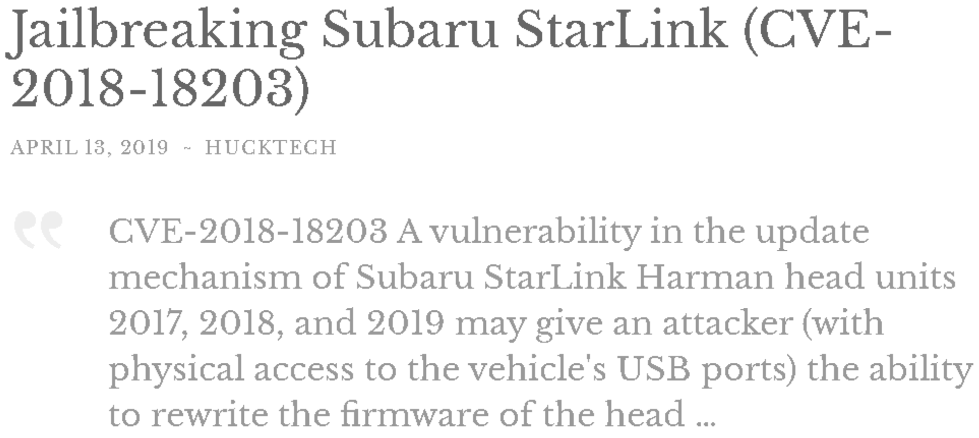
OVER-THE-AIR: HOW WE REMOTELY COMPROMISED THE GATEWAY, BCM, AND AUTOPILOT ECUS OF TESLA CARS

Consumer Group Calls Teslas 'The World's Most Hackable Cars' Forbes



ZDNet Tesla Model X hacked and stolen in minutes using new key fob hack

We discovered that the BLE interface allows for remote updates of the software running on the BLE chip. As this update mechanism was not properly secured, we were able to wirelessly compromise a key fob and take full control over it.



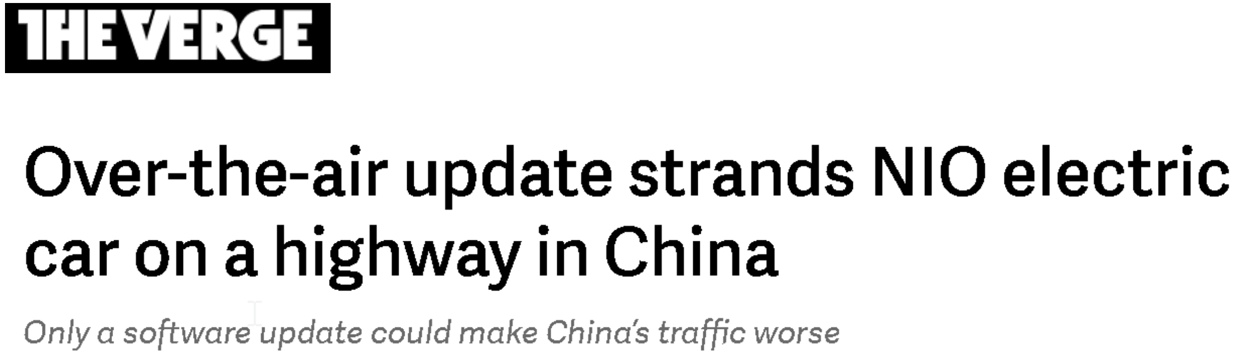
Jailbreaking Subaru StarLink (CVE-2018-18203)

APRIL 13, 2019 - HUCKTECH

> CVE-2018-18203 A vulnerability in the update mechanism of Subaru StarLink Harman head units 2017, 2018, and 2019 may give an attacker (with physical access to the vehicle's USB ports) the ability to rewrite the firmware of the head …

Vehicle Updates Can Themselves Be Compromised

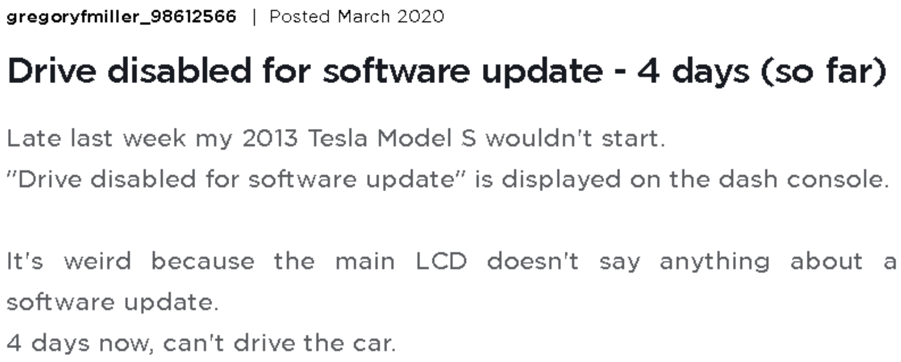
Failure Is An Option



THE VERGE

Over-the-air update strands NIO electric car on a highway in China

Only a software update could make China's traffic worse

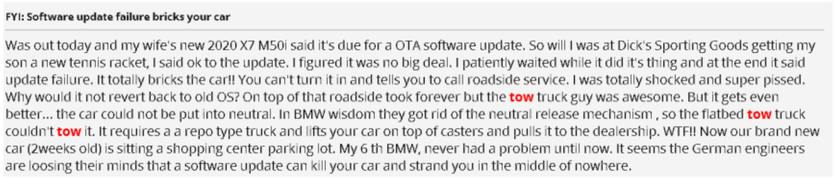


gregoryfmiller_98612566 | Posted March 2020

Drive disabled for software update - 4 days (so far)

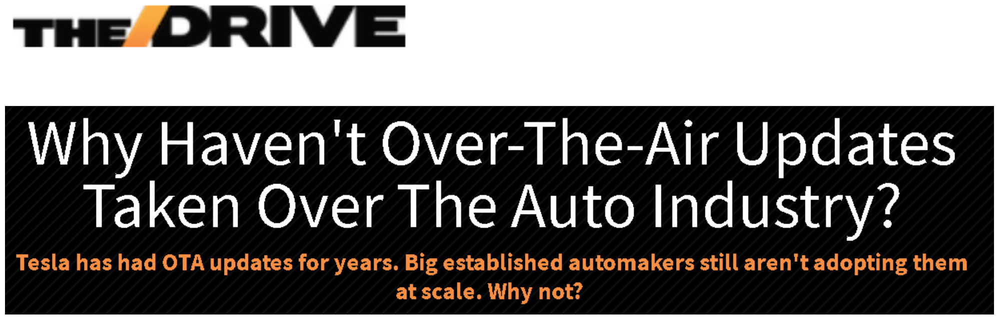
Late last week my 2013 Tesla Model S wouldn't start.
"Drive disabled for software update" is displayed on the dash console.

It's weird because the main LCD doesn't say anything about a software update.
4 days now, can't drive the car.



FYI: Software update failure bricks your car

Was out today and my wife's new 2020 X7 M50i said it's due for a OTA software update. So will I was at Dick's Sporting Goods getting my son a new tennis racket, I said ok to the update. I figured it was no big deal. I patiently waited while it did it's thing and at the end it said update failure. It totally bricks the car!! You can't turn it in and tells you to call roadside service. I was totally shocked and super pissed. Why would it not revert back to old OS? On top of that roadside took forever but the **tow** truck guy was awesome. But it gets even better... the car could not be put into neutral. In BMW wisdom they got rid of the neutral release mechanism , so the flatbed **tow** truck couldn't **tow** it. It requires a a repo type truck and lifts your car on top of casters and pulls it to the dealership. WTF!! Now our brand new car (2weeks old) is sitting a shopping center parking lot. My 6 th BMW, never had a problem until now. It seems the German engineers are loosing their minds that a software update can kill your car and strand you in the middle of nowhere.



THE DRIVE

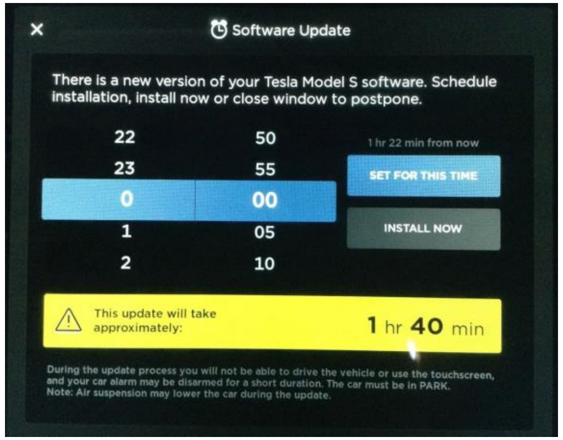
Why Haven't Over-The-Air Updates Taken Over The Auto Industry?

Tesla has had OTA updates for years. Big established automakers still aren't adopting them at scale. Why not?

Why Don’t More Vehicles Update Their Software Automatically?

Customer Interest

Not Enough Battery Power



Software Update

There is a new version of your Tesla Model S software. Schedule installation, install now or close window to postpone.

22	50
23	55
0	00
1	05
2	10

1 hr 22 min from now

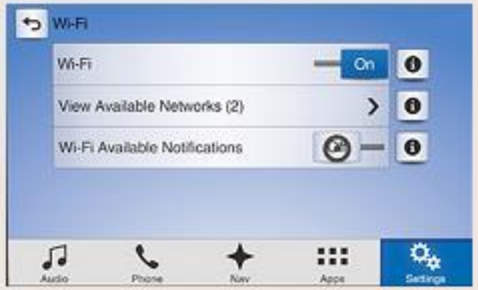
This update will take approximately: 1 hr 40 min

During the update process you will not be able to drive the vehicle or use the touchscreen, and your car alarm may be disarmed for a short duration. The car must be in PARK. Note: Air suspension may lower the car during the update.

Consent and Control
Limited Time Window

Failed Updates

Cell Service + Data + Flash Storage = $$$



Wi-Fi

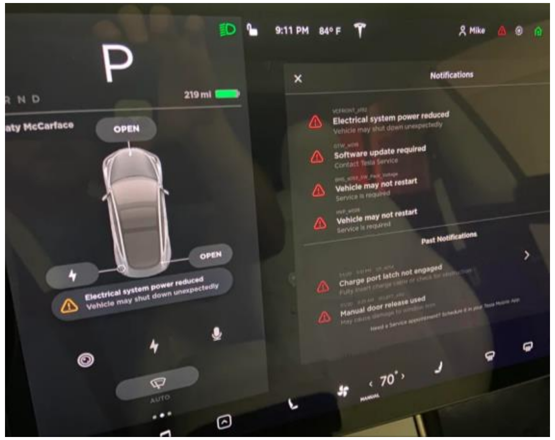
Wi-Fi: On

View Available Networks (2)

Wi-Fi Available Notifications

Data + HW Costs

Legacy Architectures



Electrical system power reduced
Vehicle may shut down unexpectedly

Notifications

Electrical system power reduced
Vehicle may shut down unexpectedly

Software update required
Contact Tesla Service

Vehicle may not restart
Service is required

Vehicle may not restart
Service is required

Past Notifications

Charge port latch not engaged

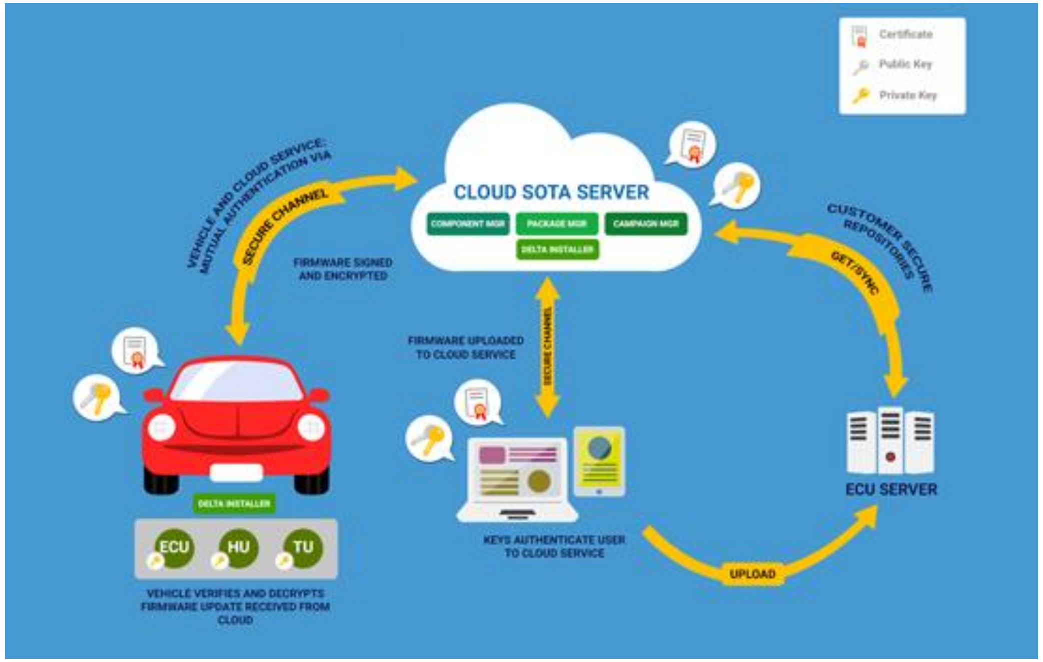
Manual door release used

Coordinated Updates

Abandoned Software

Security Of Vehicle Software Updates

- Sign and encrypt update packages
- Ensure the upgrade procedure is authenticated
- Use secure boot for integrity validation
- Use secure storage for secrets
- Automatically revert to previous version when updates fail
- Have a rescue mode to fall back when all software updates fail


Certificate
Public Key
Private Key
CLOUD SOTA SERVER
COMPONENT MGR
PACKAGE MGR
CAMPAIGN MGR
DELTA INSTALLER
VEHICLE AND CLOUD SERVICE: MUTUAL AUTHENTICATION VIA
SECURE CHANNEL
FIRMWARE SIGNED AND ENCRYPTED
CUSTOMER SECURE REPOSITORIES
GET/SYNC
FIRMWARE UPLOADED TO CLOUD SERVICE
SECURE CHANNEL
DELTA INSTALLER
ECU
HU
TU
VEHICLE VERIFIES AND DECRYPTS FIRMWARE UPDATE RECEIVED FROM CLOUD
KEYS AUTHENTICATE USER TO CLOUD SERVICE
UPLOAD
ECU SERVER

Source: excelfore

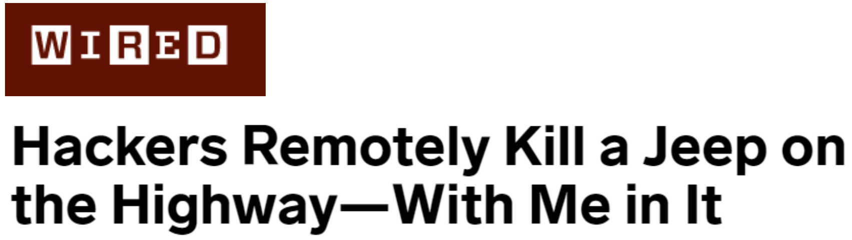
Securing the Vehicle Ecosystem

Mike Westra

Vehicle & Connected Cybersecurity

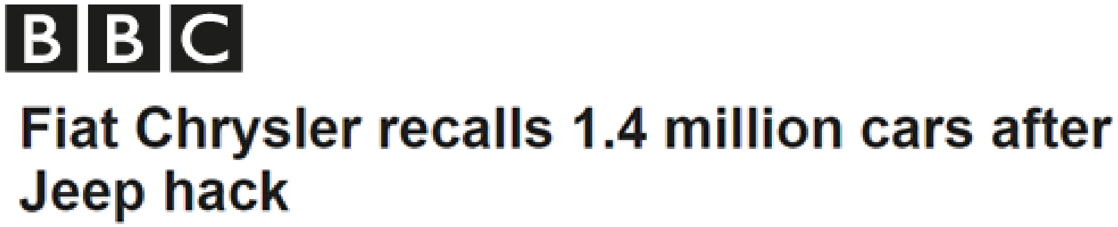
"Don't worry. I'm sure it's just a software glitch."

What Is The Cost Of A Single Automotive Hack?



WIRED

Hackers Remotely Kill a Jeep on the Highway—With Me in It

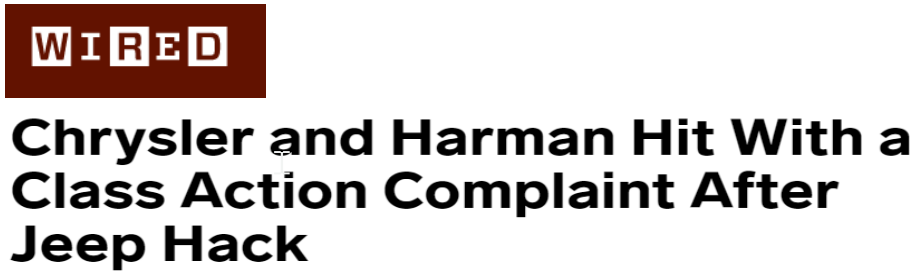


BBC

Fiat Chrysler recalls 1.4 million cars after Jeep hack

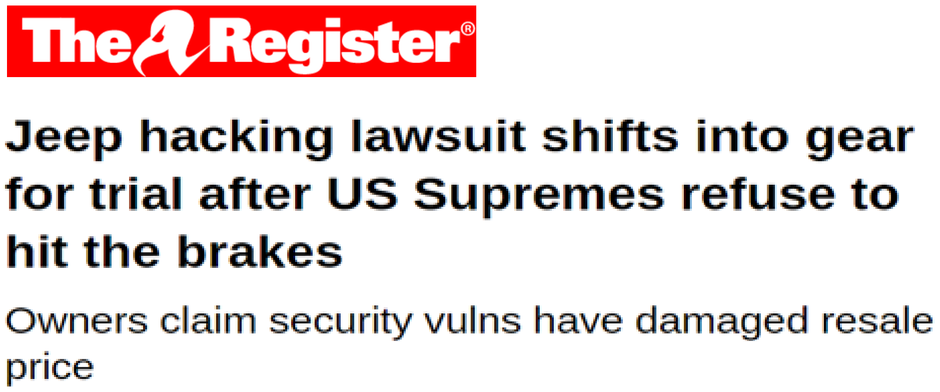
Source: Upstream Security Global Automotive Report 2019

A single vehicle cyber hack can cost an automaker over $1.1 billion dollars



WIRED

Chrysler and Harman Hit With a Class Action Complaint After Jeep Hack



The Register®

Jeep hacking lawsuit shifts into gear for trial after US Supremes refuse to hit the brakes

Owners claim security vulns have damaged resale price

Primary Drivers of Software Cybersecurity

Connectivity: as seamless connectivity to OEMs and 3rd parties is added, it increases direct and indirect cyber security risks (direct remote access, user data, abuse of services, theft, etc.)

Autonomy: Level 2 systems increasingly allowing more direct user automation as graduations towards full autonomy

- Degrees from map-based cruise to autonomous parking give systems direct control of the vehicle for the first time

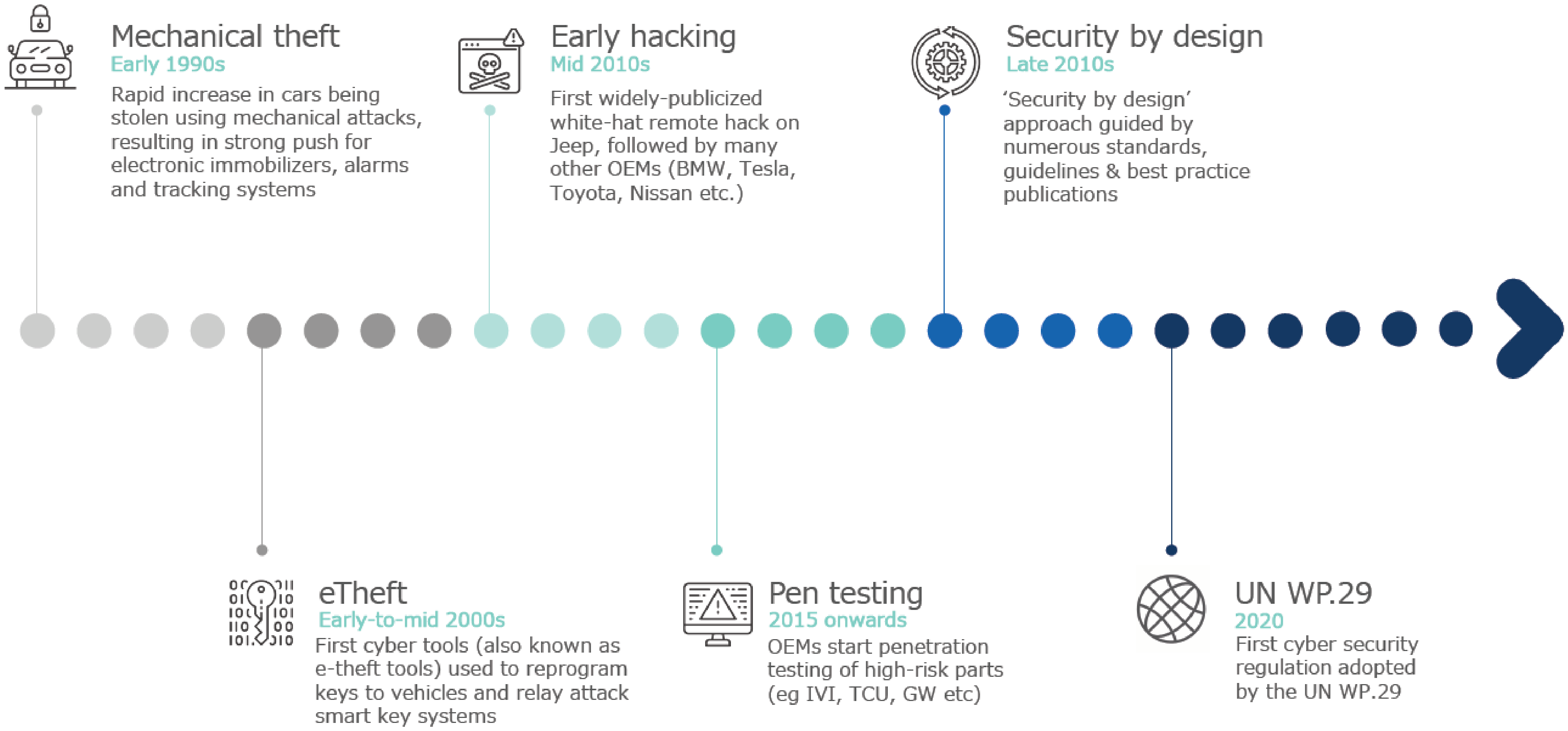
Regulatory: Increasing appetite to directly regulate vehicle cyber security

- UNECE will directly tie TYPE approval with meeting cyber security around key areas (connectivity, direct backend, consumer interfaces, etc)
- Privacy regulations vary widely (from GDPR to California privacy opt-in)

Business drivers

- Drive for increased speed for features, data, 3rd party integration, partnerships
- Shared Mobility will drive increased car sharing and need to manage identity
- ECU consolidation, understanding that software drives vehicle

History of Automotive CyberSecurity



Mechanical theft
Early 1990s
Rapid increase in cars being stolen using mechanical attacks, resulting in strong push for electronic immobilizers, alarms and tracking systems

eTheft
Early-to-mid 2000s
First cyber tools (also known as e-theft tools) used to reprogram keys to vehicles and relay attack smart key systems

Early hacking
Mid 2010s
First widely-publicized white-hat remote hack on Jeep, followed by many other OEMs (BMW, Tesla, Toyota, Nissan etc.)

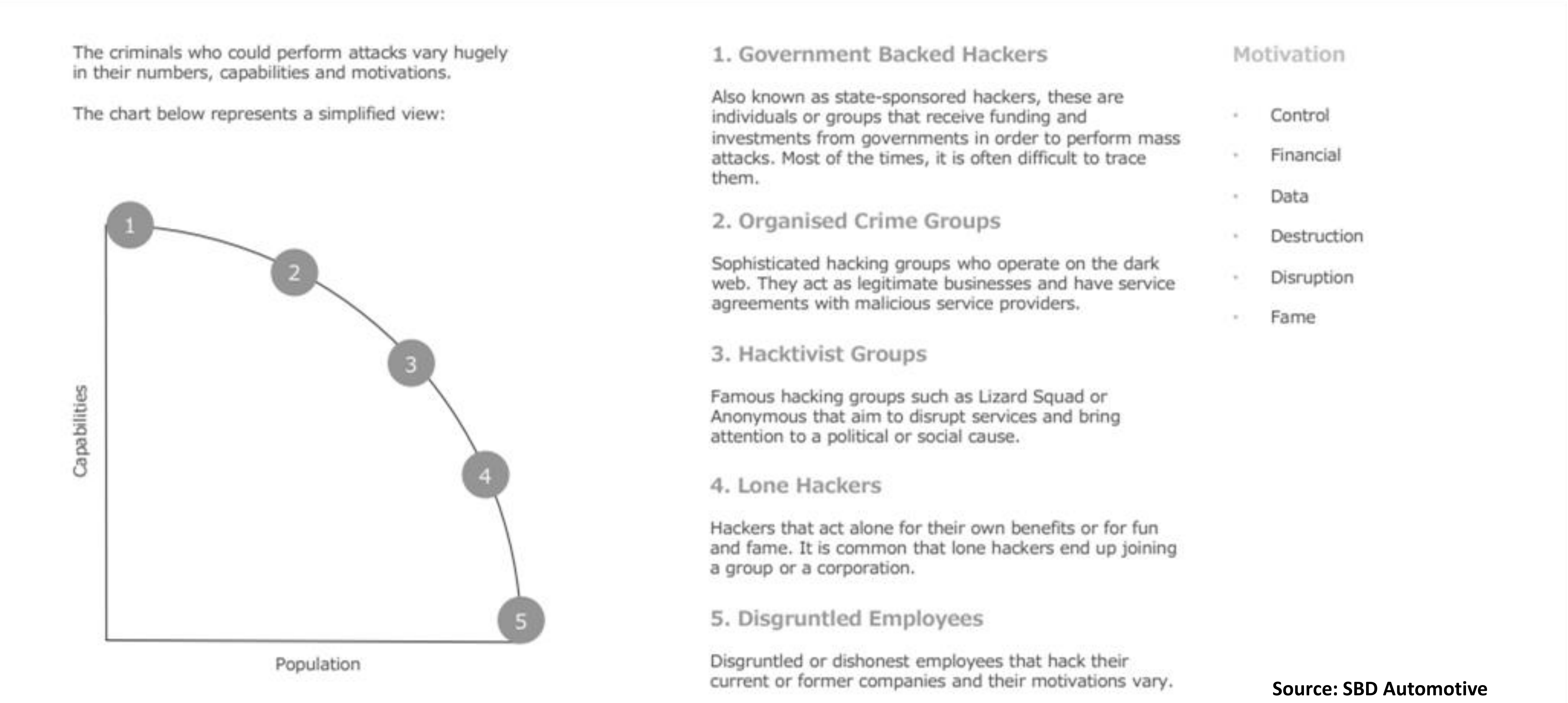
Pen testing
2015 onwards
OEMs start penetration testing of high-risk parts (eg IVI, TCU, GW etc)

Security by design
Late 2010s
'Security by design' approach guided by numerous standards, guidelines & best practice publications

UN WP.29
2020
First cyber security regulation adopted by the UN WP.29

Source: SBD Automotive

Who Is Attacking Vehicles?



The criminals who could perform attacks vary hugely in their numbers, capabilities and motivations.

The chart below represents a simplified view:

1
2
3
4
5
Capabilities
Population

1. Government Backed Hackers

Also known as state-sponsored hackers, these are individuals or groups that receive funding and investments from governments in order to perform mass attacks. Most of the times, it is often difficult to trace them.

2. Organised Crime Groups

Sophisticated hacking groups who operate on the dark web. They act as legitimate businesses and have service agreements with malicious service providers.

3. Hacktivist Groups

Famous hacking groups such as Lizard Squad or Anonymous that aim to disrupt services and bring attention to a political or social cause.

4. Lone Hackers

Hackers that act alone for their own benefits or for fun and fame. It is common that lone hackers end up joining a group or a corporation.

5. Disgruntled Employees

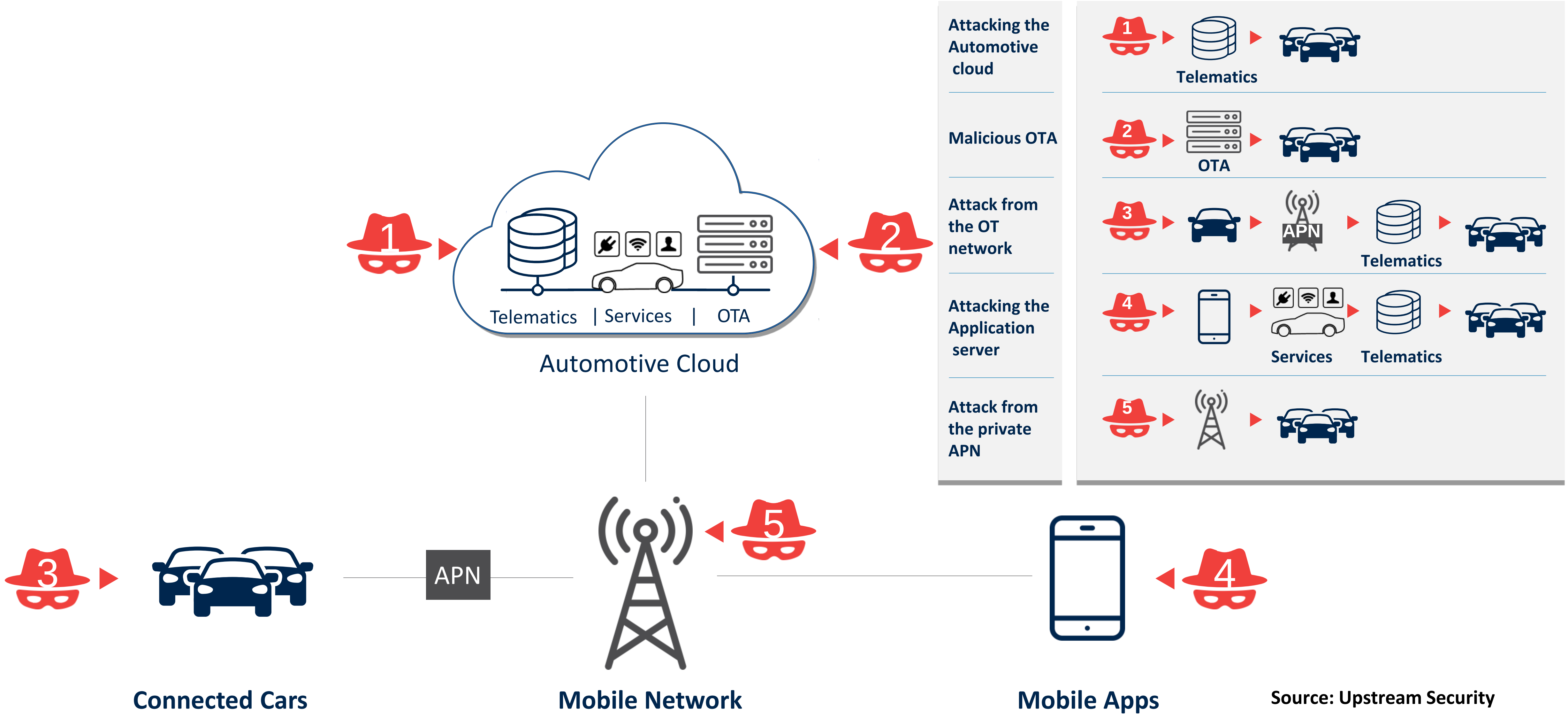
Disgruntled or dishonest employees that hack their current or former companies and their motivations vary.

Motivation

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

Source: SBD Automotive

Vehicle Ecosystem Attack Vectors

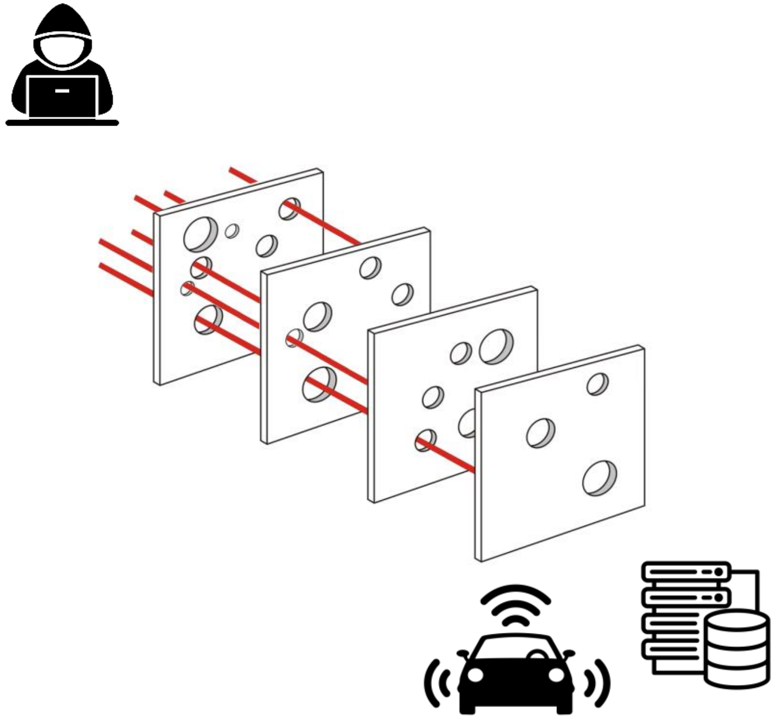


Attacking the Automotive cloud	1 ▸ Telematics ▸
Malicious OTA	2 ▸ OTA ▸
Attack from the OT network	3 ▸ ▸ APN ▸ Telematics ▸
Attacking the Application server	4 ▸ ▸ Services ▸ Telematics ▸
Attack from the private APN	5 ▸ ▸

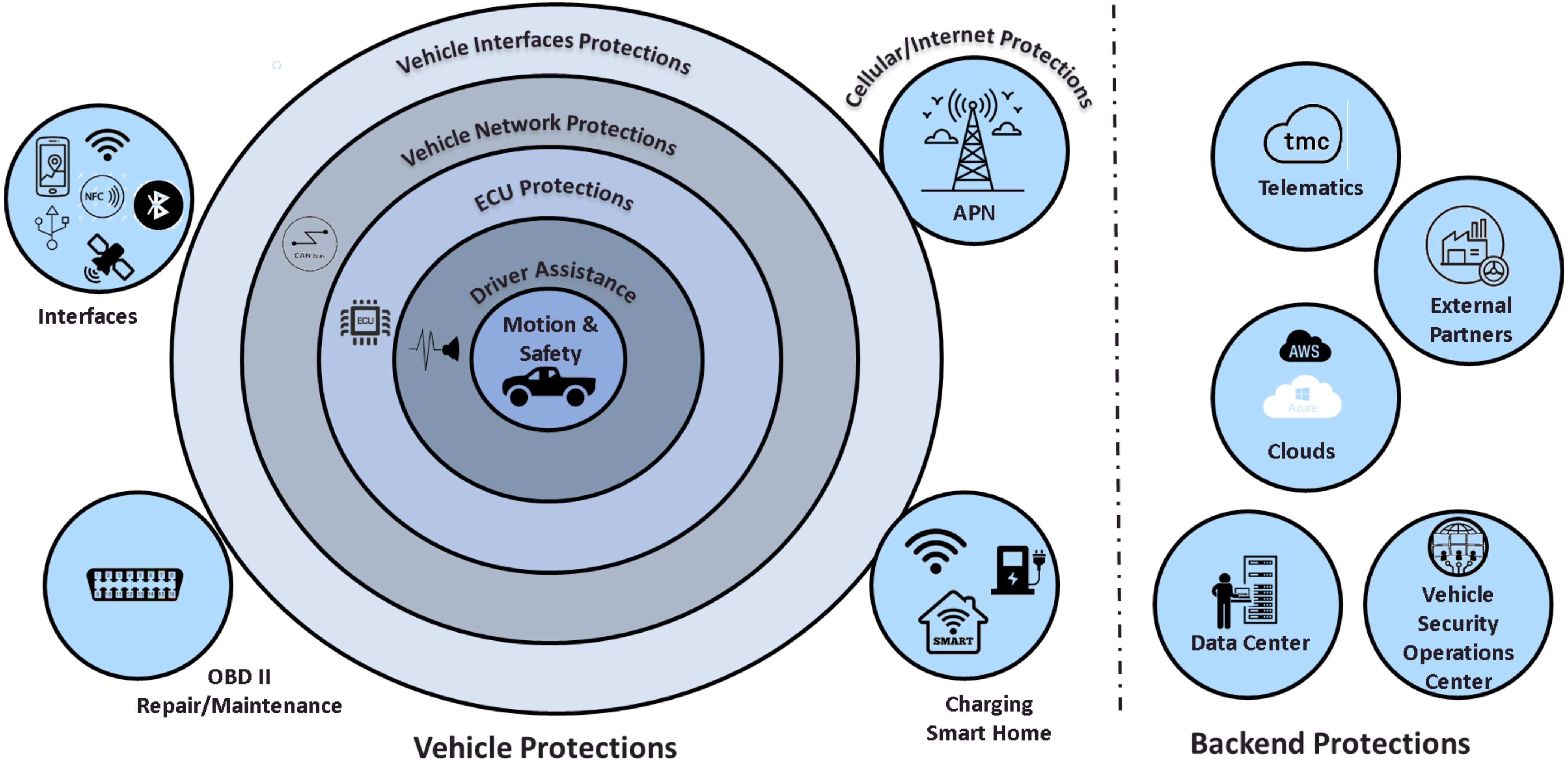
Source: Upstream Security

Cybersecurity Approach: Defense-in-Depth

- A defense-in-depth approach utilizes layers of Cybersecurity measures to maintain product security
- No single layer is exclusively relied upon; access controls, physical barriers, redundant and diverse security functions, and emergency response measures are used
- Defense-in-depth is designed to compensate for human, mechanical, electrical, software, and other failures
- If an attack penetrates or bypasses one layer, another Cybersecurity layer contains the attack and continues to maintain a sufficient degree of protection

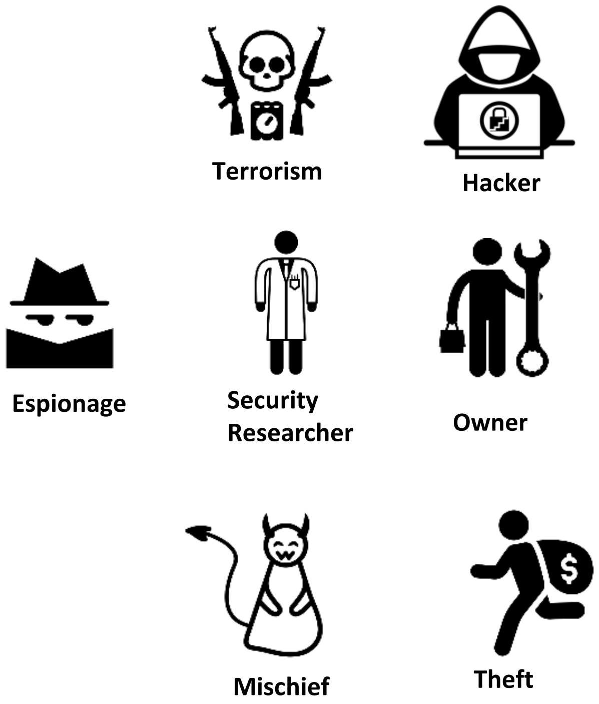


Tech Stack Defense-In-Depth Model



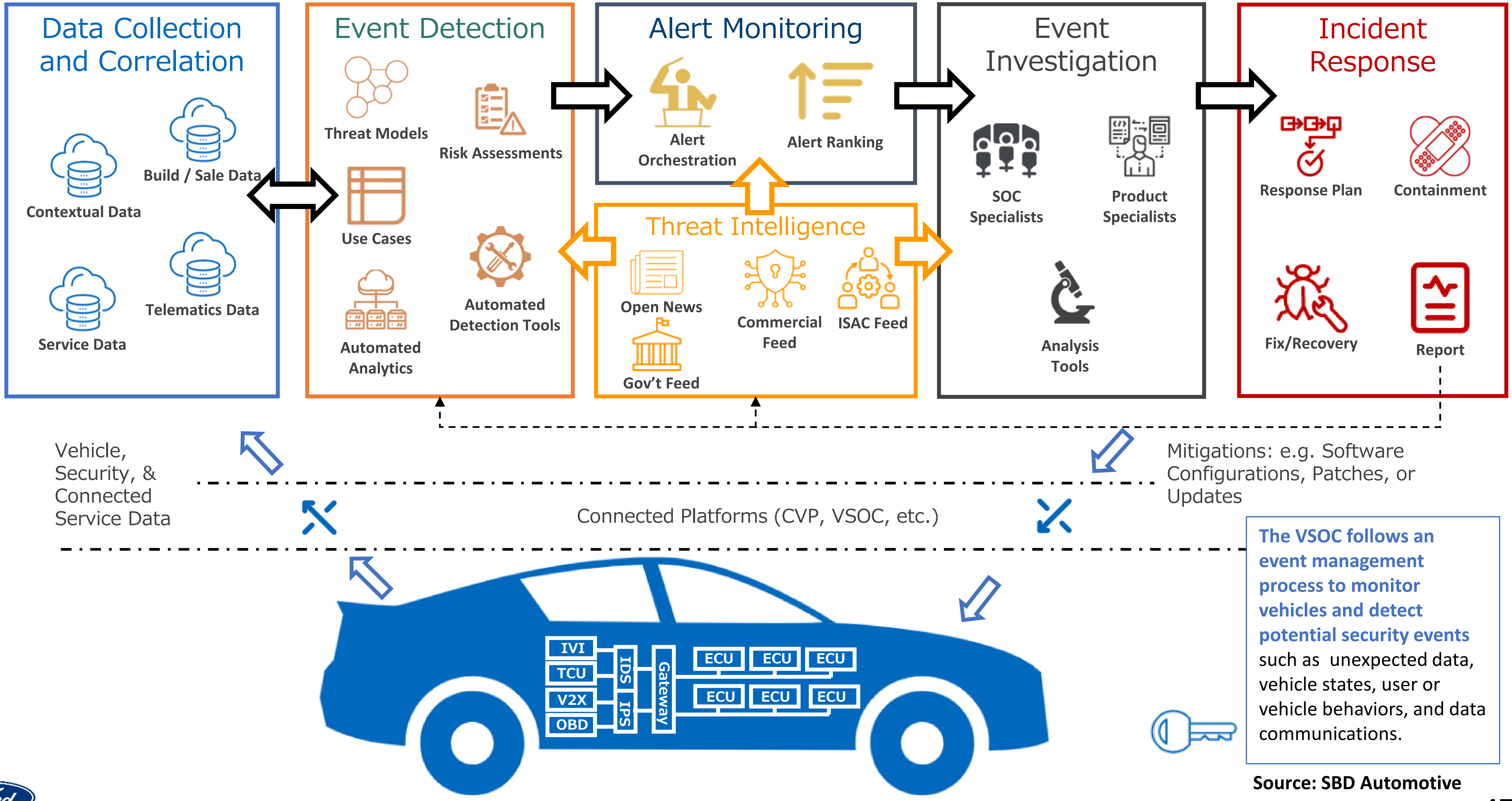
Cybersecurity Approach: Vehicle Security Operations Center (VSOC)

- The amount and value of connected vehicle data is increasingly attractive to criminals
- The range and potential impact of attacks is increasing with the expansion of connected services to full-vehicle OTA and increased vehicle autonomy
- Some attacks could lead to injury or death, while many others can cause significant financial, reputational or operational damage



VSOCs Can Help Detect And Remediate Vehicle Attacks

VSOC Elements



Data Collection and Correlation
Build / Sale Data
Contextual Data
Telematics Data
Service Data

Event Detection
Threat Models
Risk Assessments
Use Cases
Automated Detection Tools
Automated Analytics

Alert Monitoring
Alert Orchestration
Alert Ranking

Threat Intelligence
Open News
Commercial Feed
ISAC Feed
Gov't Feed

Event Investigation
SOC Specialists
Product Specialists
Analysis Tools

Incident Response
Response Plan
Containment
Fix/Recovery
Report

Vehicle, Security, & Connected Service Data

Connected Platforms (CVP, VSOC, etc.)

Mitigations: e.g. Software Configurations, Patches, or Updates

IVI
TCU
V2X
OBD
IDS
IPS
Gateway
ECU
ECU
ECU
ECU
ECU
ECU

The VSOC follows an event management process to monitor vehicles and detect potential security events such as unexpected data, vehicle states, user or vehicle behaviors, and data communications.

Source: SBD Automotive

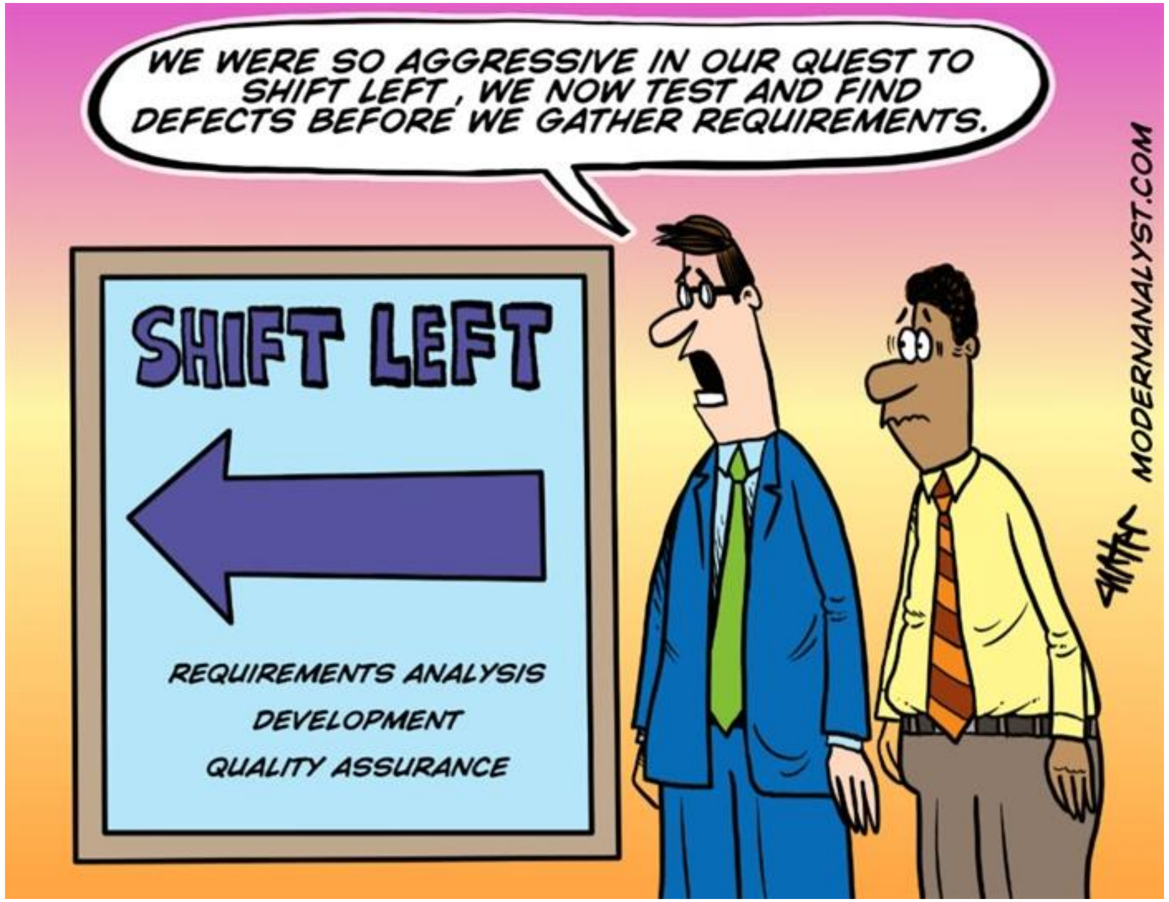
Cybersecurity Digital Twins

Approach: Generate a vehicle digital twin to continuously monitor its exposure to cyber security risks throughout its lifetime

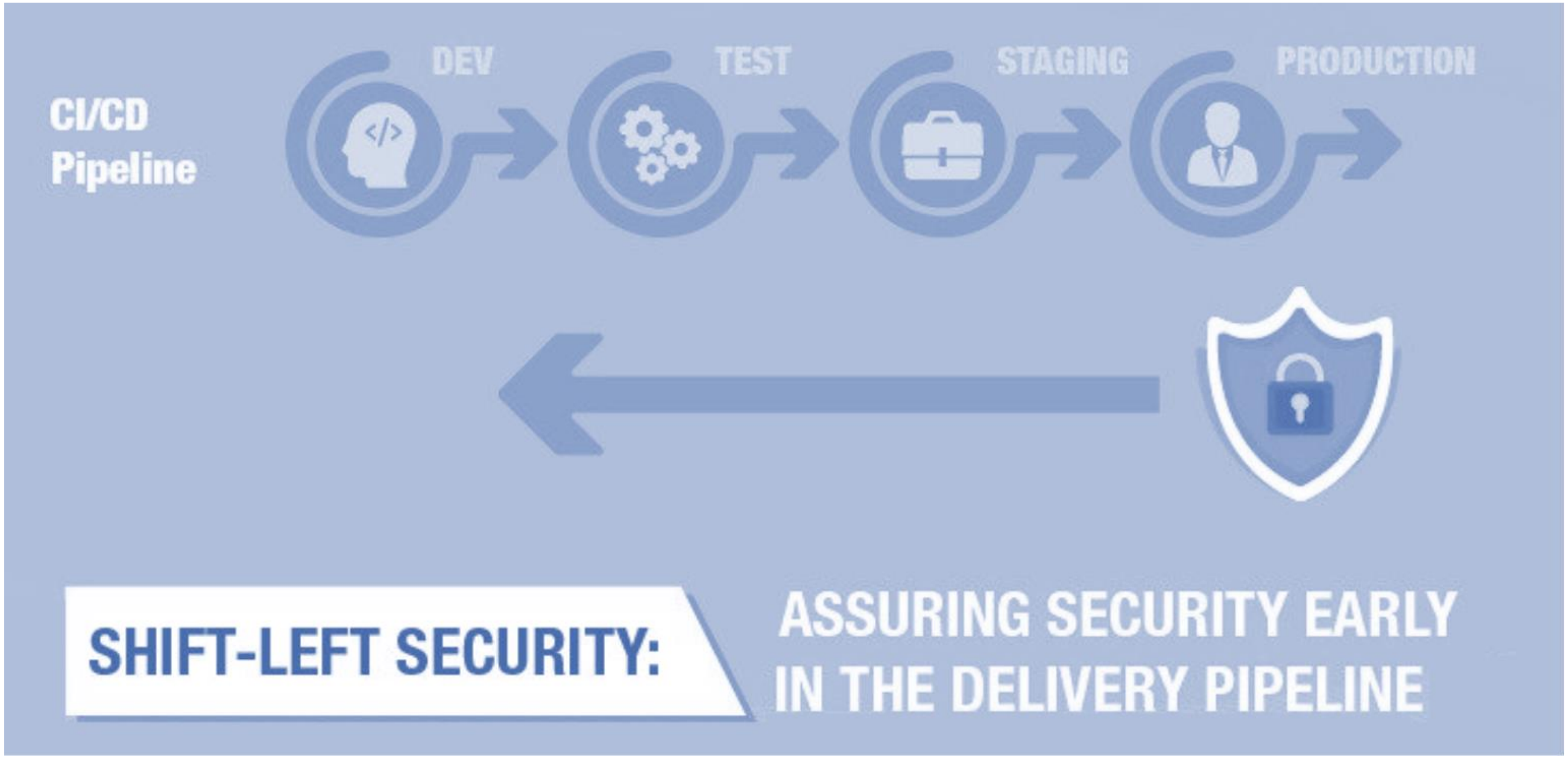
- A digital twin is a real-time, virtual replica of a vehicle
- Digital twins use machine learning and data normalization to profile and detect vehicle anomalies in real-time
- Cybersecurity regulations require OEMs to monitor vehicle risks throughout its lifetime

Time To Shift Left On Security

Mike Westra

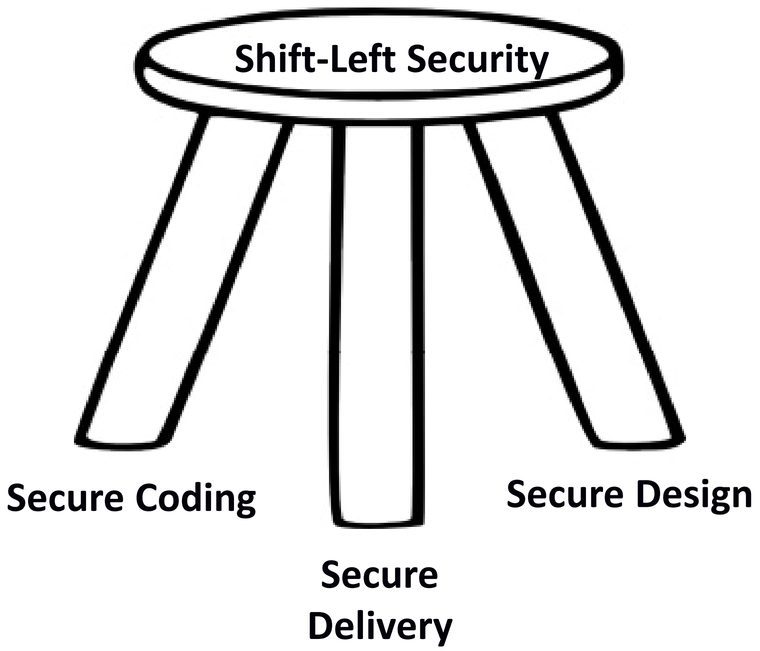

WE WERE SO AGGRESSIVE IN OUR QUEST TO SHIFT LEFT, WE NOW TEST AND FIND DEFECTS BEFORE WE GATHER REQUIREMENTS.
SHIFT LEFT
REQUIREMENTS ANALYSIS
DEVELOPMENT
QUALITY ASSURANCE
MODERNANALYST.COM

What Is Shift-Left Security?



Shifting Left Is Positioning A Process That Is Performed Later In The Development Cycle To A Point Early In The Delivery Lifecycle

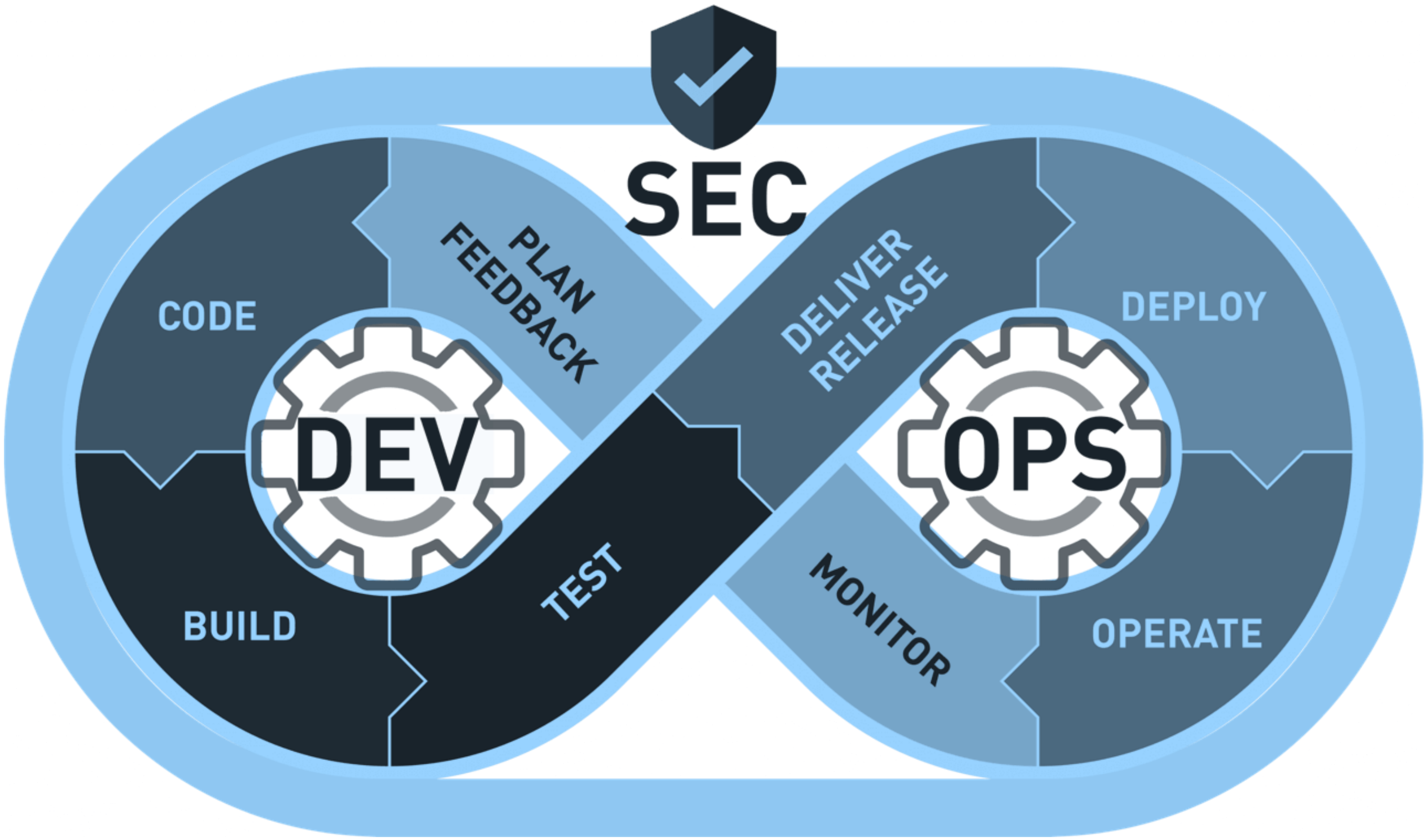
Shift-Left And The Connected Ecosystem



- The growing reliance on software exposes OEMs to a multitude of threats
- Shift-left considers security from the onset and is pervasive throughout the software development process
- OEMs must enable software development processes that identify and fix vulnerabilities during design and development rather than testing and repairing vulnerabilities later

Security Consideration is Needed From The Start – Further Up Stream

Continuous Software Delivery (DevSecOps)

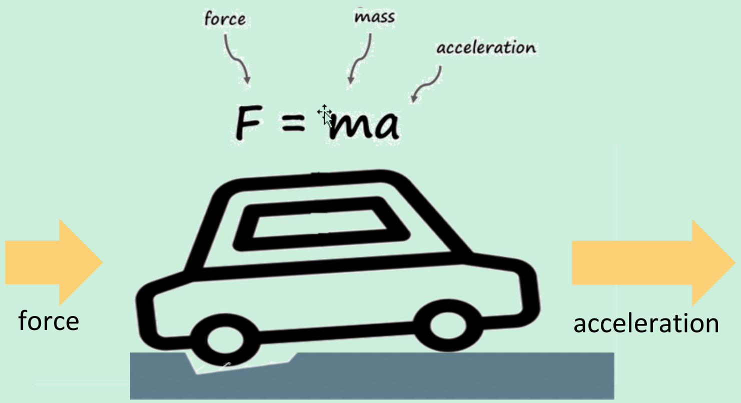


DevSecOps Integrates Security Measures Into A Software Delivery Pipeline

Safety Is Not The Same As Security

Hacker
Owner
Mischief
Security Researcher
Espionage
Terrorism
Thief

A security threat exclusively originates from **human behavior** where an individual or group intentionally wishes to harm people or property, or profit from their actions

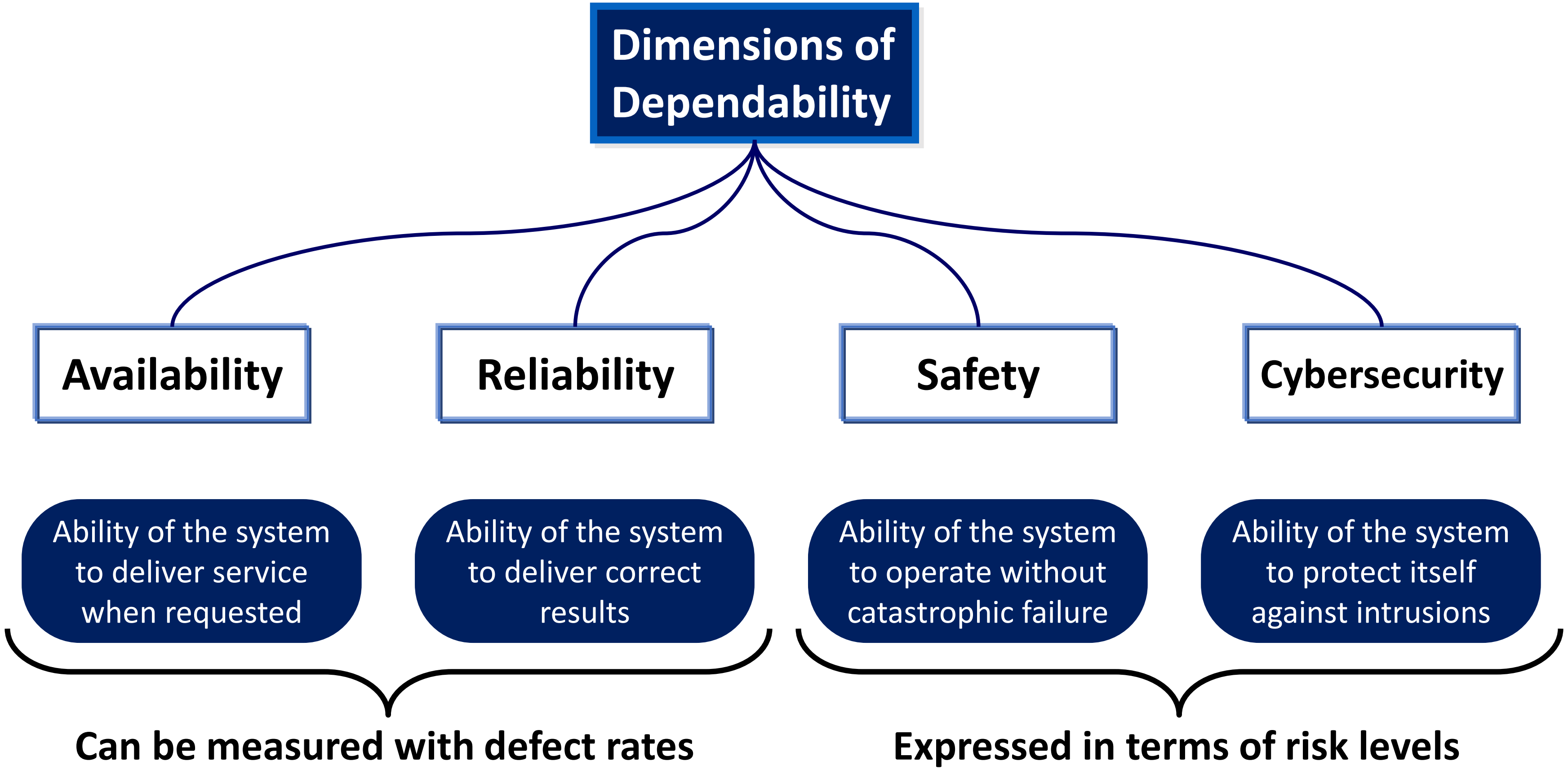


A safety risk originates from **a force of nature (physics),** or an unintended or **accidental human behavior**

Security employs a **preventative approach**, which is required for the ongoing assurance of vehicle safety during its lifetime

Safety And Security Are Often Mistakenly Used Interchangeably

Software Dependability Has Multiple Dimensions



Dimensions of Dependability

Availability

Reliability

Safety

Cybersecurity

Ability of the system to deliver service when requested

Ability of the system to deliver correct results

Ability of the system to operate without catastrophic failure

Ability of the system to protect itself against intrusions

Can be measured with defect rates

Expressed in terms of risk levels

Cybersecurity Impacts All Dimensions of Software Dependability

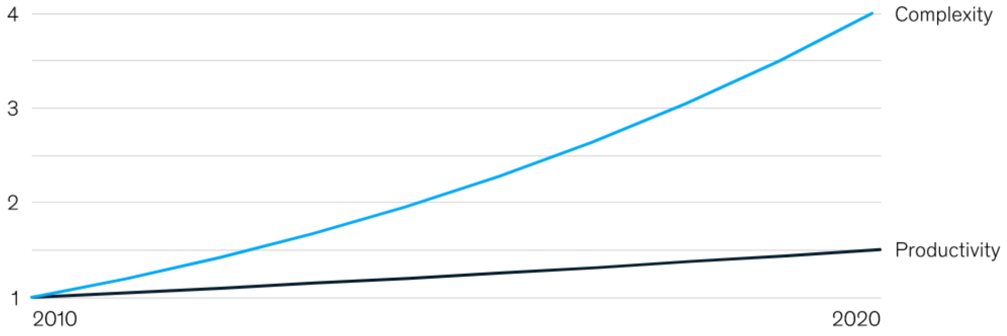
Automakers Are At A Critical Tipping Point For Software

- Most automaker software development practices significantly lag behind other industries
- Areas of concern include
  - Agile practices
  - Continuous integration
  - Automated testing
- Automakers have traditionally viewed software as secondary to hardware, or a necessary evil
- Automakers must revisit software development approaches, as software is a prime value driver in manufactured products

McKinsey & Company

Software complexity is increasing more quickly than productivity.

Relative growth of software complexity and productivity over time, indexed for automotive features

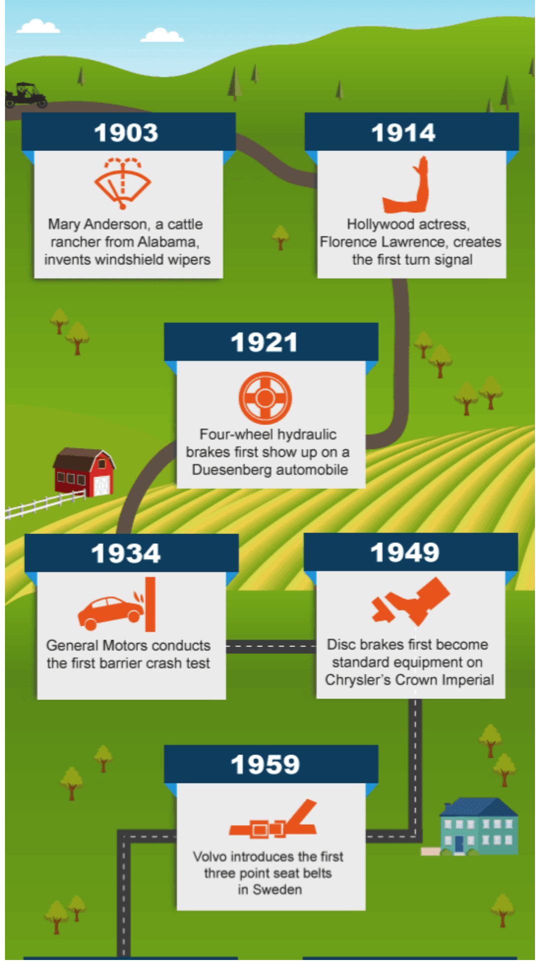


Lisa Boran

Cybersecurity Legislation
Friend or Foe?

Our vehicles are 100% compliant
I disconnected them from the Internet
How did you do that?
© D.Fletcher for CloudTweaks.com

History of Vehicle Safety



1903
Mary Anderson, a cattle rancher from Alabama, invents windshield wipers

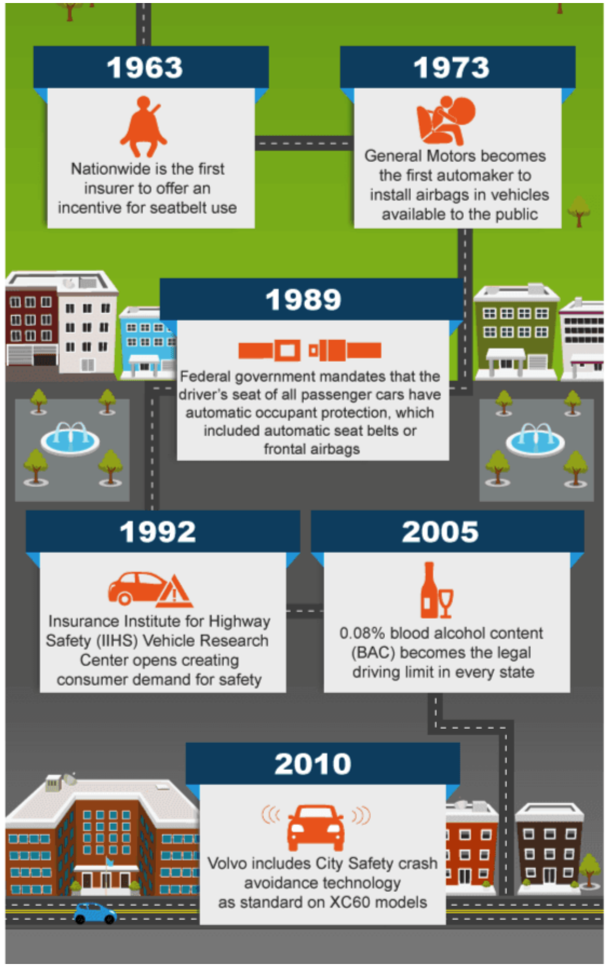
1914
Hollywood actress, Florence Lawrence, creates the first turn signal

1921
Four-wheel hydraulic brakes first show up on a Duesenberg automobile

1934
General Motors conducts the first barrier crash test

1949
Disc brakes first become standard equipment on Chrysler's Crown Imperial

1959
Volvo introduces the first three point seat belts in Sweden



1963
Nationwide is the first insurer to offer an incentive for seatbelt use

1973
General Motors becomes the first automaker to install airbags in vehicles available to the public

1989
Federal government mandates that the driver's seat of all passenger cars have automatic occupant protection, which included automatic seat belts or frontal airbags

1992
Insurance Institute for Highway Safety (IIHS) Vehicle Research Center opens creating consumer demand for safety

2005
0.08% blood alcohol content (BAC) becomes the legal driving limit in every state

2010
Volvo includes City Safety crash avoidance technology as standard on XC60 models

- Public awareness played a large part in the history of vehicle safety
- Today there are strong consumer demands for vehicle safety
- The vehicle safety journey took many years to mature

Source: Nationwide Insurance

Vehicle Cybersecurity Has Matured At A Much Quicker Timeline

Vehicle Cybersecurity Maturation

Early days-2016
The 'Quick fix' Era

OEMs largely ignored cyber, or under-estimated the risk, until several high profile demonstration hacks prompted action to 'test and fix' prior to launch.

2016-2020
The 'Best practice' Era

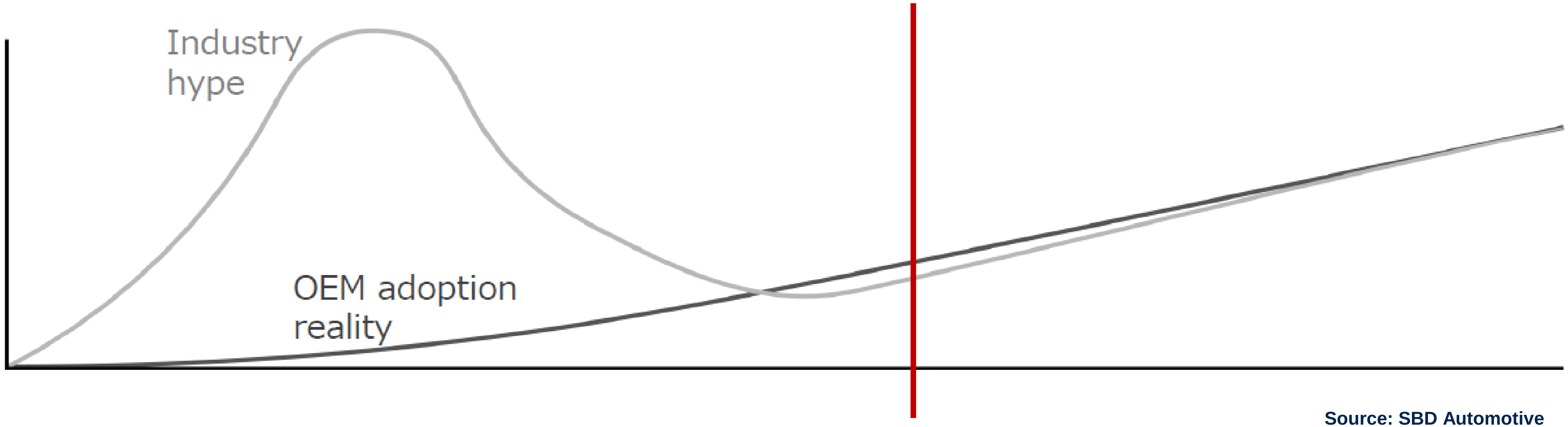
The automotive industry collaborates to develop best practice development guidelines – the start of 'Secure By Design'.

2020-2025
The 'Legislation' Era

OEMs work with the authorities to standardise and audit the cyber development process – from initial concept through to post-SOP incident response.

2025+
The 'Maturity' Era

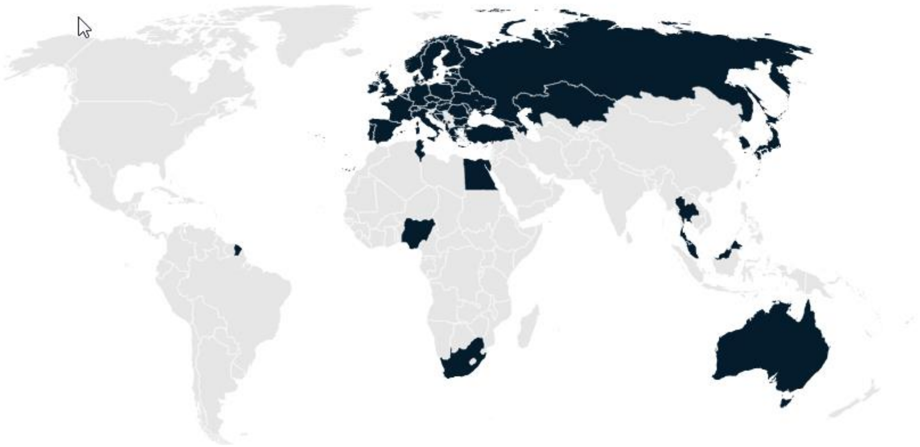
Cyber security becomes a mature part of each OEM's vehicle development process.



Source: SBD Automotive

We Are Here

UNECE WP.29 Vehicle Cybersecurity Regulations



1st Qtr 2021 – Regulation becomes effective

2022 – UNECE Cybersecurity regulations start – New Vehicles (EU & Japan w/ OTA)

2024 – All vehicle sales in EU and Korea
Japan (All w/OTA & New Vehicles w/o OTA)

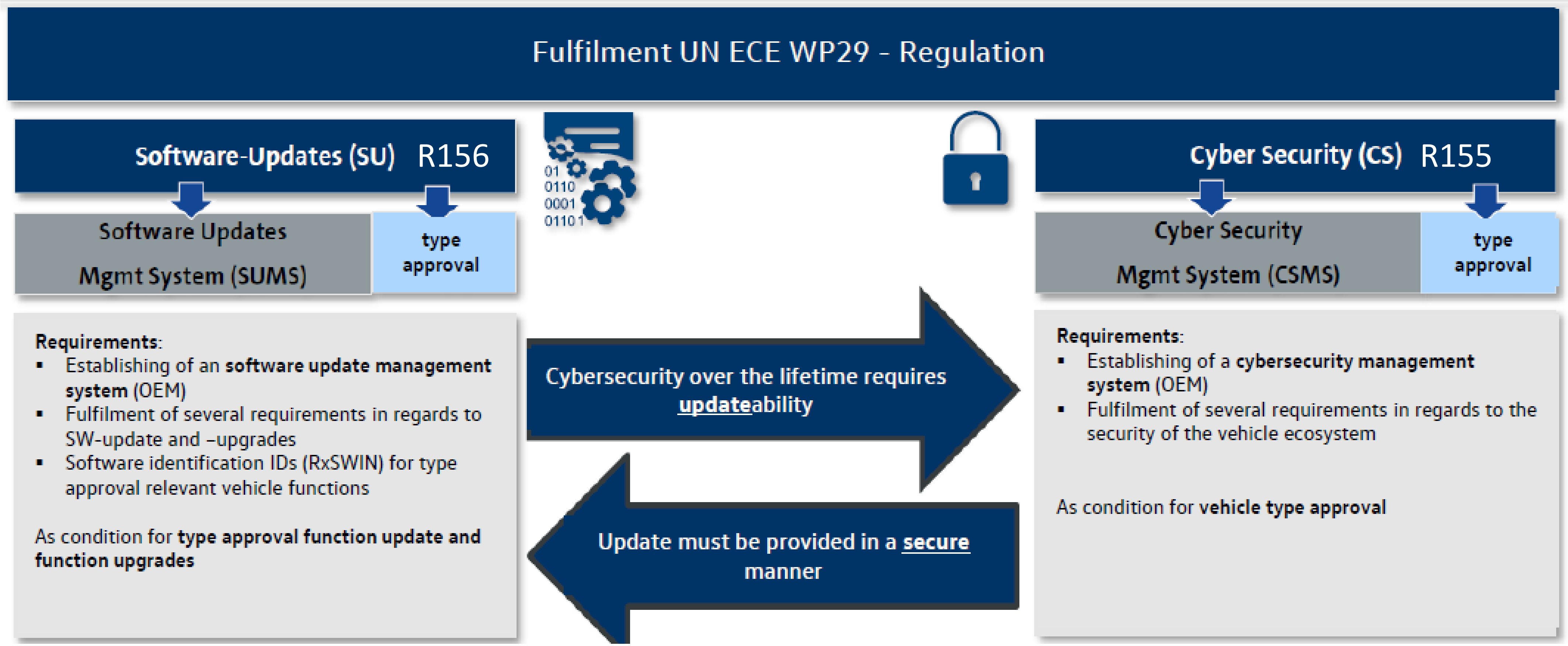
2026 - All vehicles in Japan w/o OTA

Similar to the EPA, who certifies that vehicles comply with emissions and fuel economy regulations, independent bodies must certify that a vehicle type complies with UNECE Cybersecurity regulations before it can be sold in UNECE countries

Vehicle sales in **56** countries will be impacted by the UNECE Cybersecurity regulations

76 – # of required threats w/mitigations mandated by UNECE Cybersecurity regulations

WP.29 Regulation Relationship



Fulfilment UN ECE WP29 - Regulation

Software-Updates (SU) R156

Software Updates Mgmt System (SUMS)

type approval

Requirements:

- Establishing of an **software update management system** (OEM)
- Fulfilment of several requirements in regards to SW-update and –upgrades
- Software identification IDs (RxSWIN) for type approval relevant vehicle functions

As condition for **type approval function update and function upgrades**

Cybersecurity over the lifetime requires **updateability**

Update must be provided in a **secure** manner

Cyber Security (CS) R155

Cyber Security Mgmt System (CSMS)

type approval

Requirements:

- Establishing of a **cybersecurity management system** (OEM)
- Fulfilment of several requirements in regards to the security of the vehicle ecosystem

As condition for **vehicle type approval**

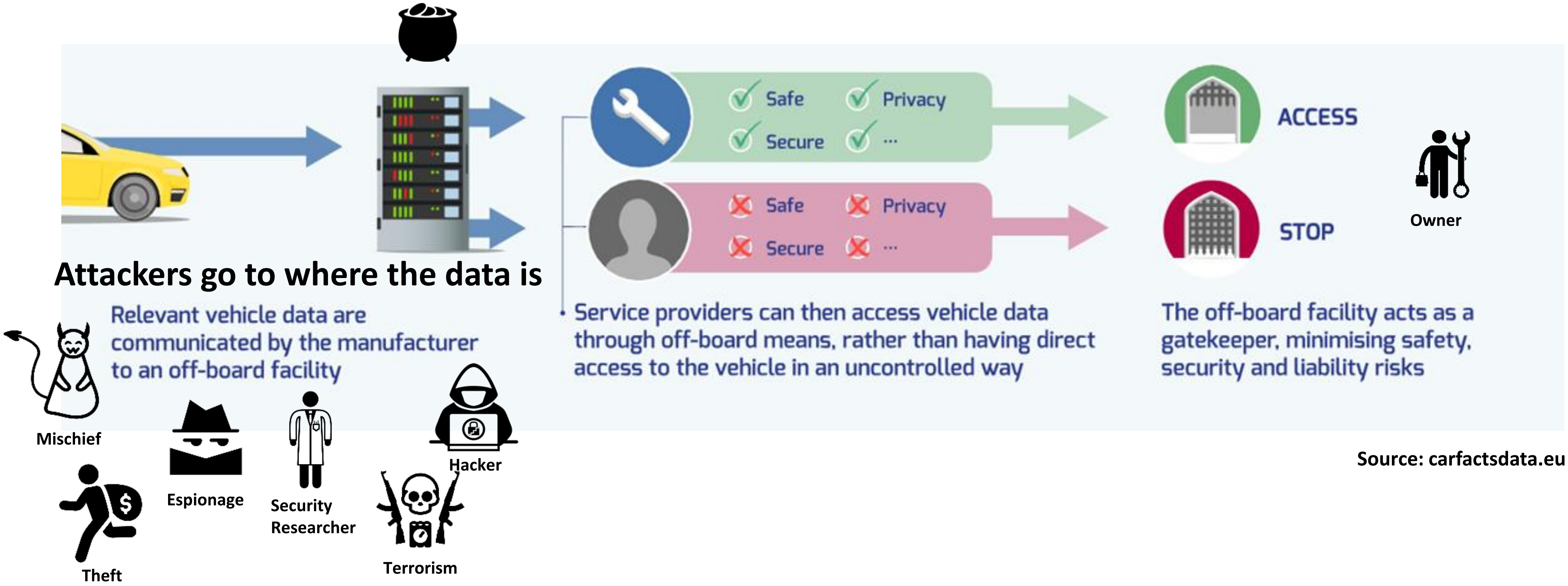
CSMS/SUMS Certification And Whole Vehicle Type Approval Required

United States Cyber Regulation Landscape

- The United States is a self-certification country
- NHTSA issued "updated" 2020 cybersecurity best practices
  - Applicable to all organizations designing and manufacturing vehicle electronic systems and software
  - This includes aftermarket accessories
- GTR nations are meeting now - will likely select requirements from UNECE to be met by countries under 1998 Agreement to keep harmonization

GTR Conclusions/Agreements Expected To Be Finalized In April 2021

Neutral Server Legislation Introduces Increased Risks



Attackers go to where the data is

Relevant vehicle data are communicated by the manufacturer to an off-board facility

- Service providers can then access vehicle data through off-board means, rather than having direct access to the vehicle in an uncontrolled way

The off-board facility acts as a gatekeeper, minimising safety, security and liability risks

Source: carfactsdata.eu

OEMS Cannot Guarantee The Privacy, Consent, Or Security Of Customer Data When It Is Stored On A Neutral Server

Key Messages

- Cybercrime is extremely profitable
- APIs are the favorite attack vectors
- Digital ecosystems are driving transformation and growth
- Software and Security are essentially invisible
- Continuous delivery is driving software and innovations
- Software velocity of automotive lags other industries

- Open-source software is both good and bad
- Remote software updates are no longer optional
- Safety and Security are interdependent
- Cyber regulations are impacting software delivery practices
- Software is an increasing portion of a vehicle’s BOM
- Automation is required to “fail fast” and maintain product safety

Questions

Sale
Connected Appliances
klossner
"CAN I INTEREST YOU IN A FIREWALL FOR YOUR TOASTER?"