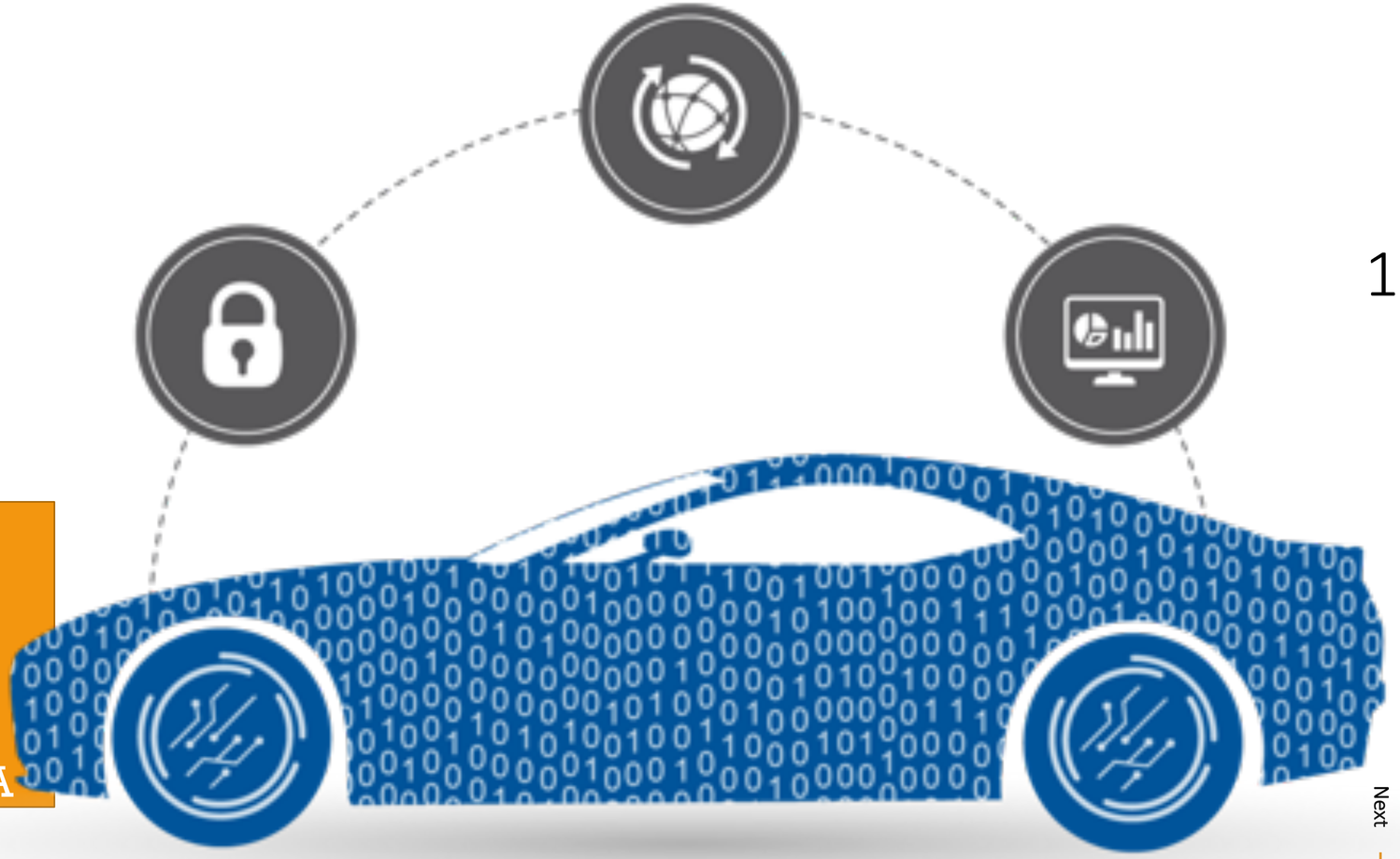
Cyber Security Challenges and Opportunities for Autonomous Vehicle

Dr. Neeli R. Prasad
CTO
Neeli.Prasad@SmartAvatar.nl
SmartAvatar B.V.
Amsterdam, NLD & Mountain View, CA, USA



Vehicle Transforming into Software-Enabled Vehicle Architecture

F-22 Raptor Fighter Jet

~ 1,500,000 lines of code

Boeing 787

~ 13,000,000 lines of code

Social Medial Platform "FB"

~ 61,000,000 lines of code

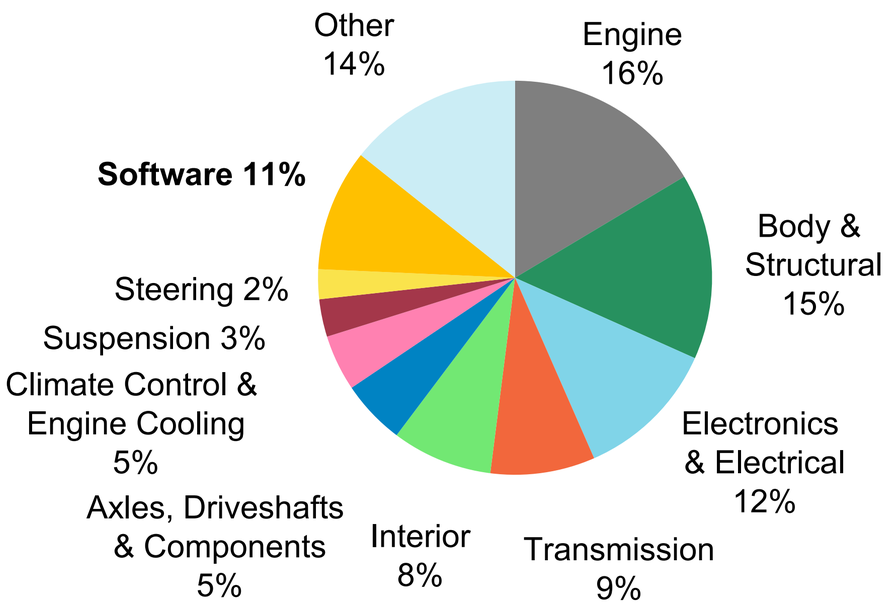
Modern High-End Vehicle

100,000,000+ lines of code with Intelligent Edge Computing onboard

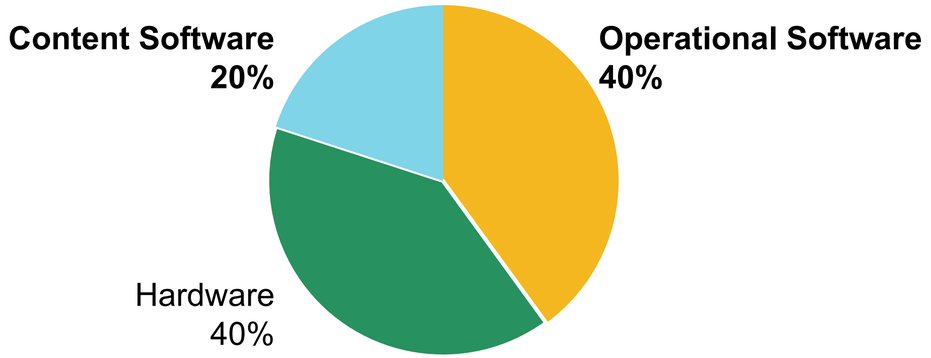
Previous
Next

Change in Vehicle Value from Hardware to Software

Today



The "Future"



Autonomous Vehicle will Generate Tera Bytes of Data per Hour!

Automotive Cybersecurity Challenges

In the computer game Watch Dogs, developed by French video game developer Ubisoft, protagonist Aiden Pearce is able to use a highly specialised mobile device to gain access to the operating system of a hyper-connected future Chicago, enabling him to hack directly into moving vehicles and take control of their electrical systems using Wi-F. Purple Griffon, June 11, 2020

What about Trust?

Tele-Operation for AV

How Secure is your Tele-Operation?

Human-in-the-Loop

Commercial Vehicles

Farming & Agriculture

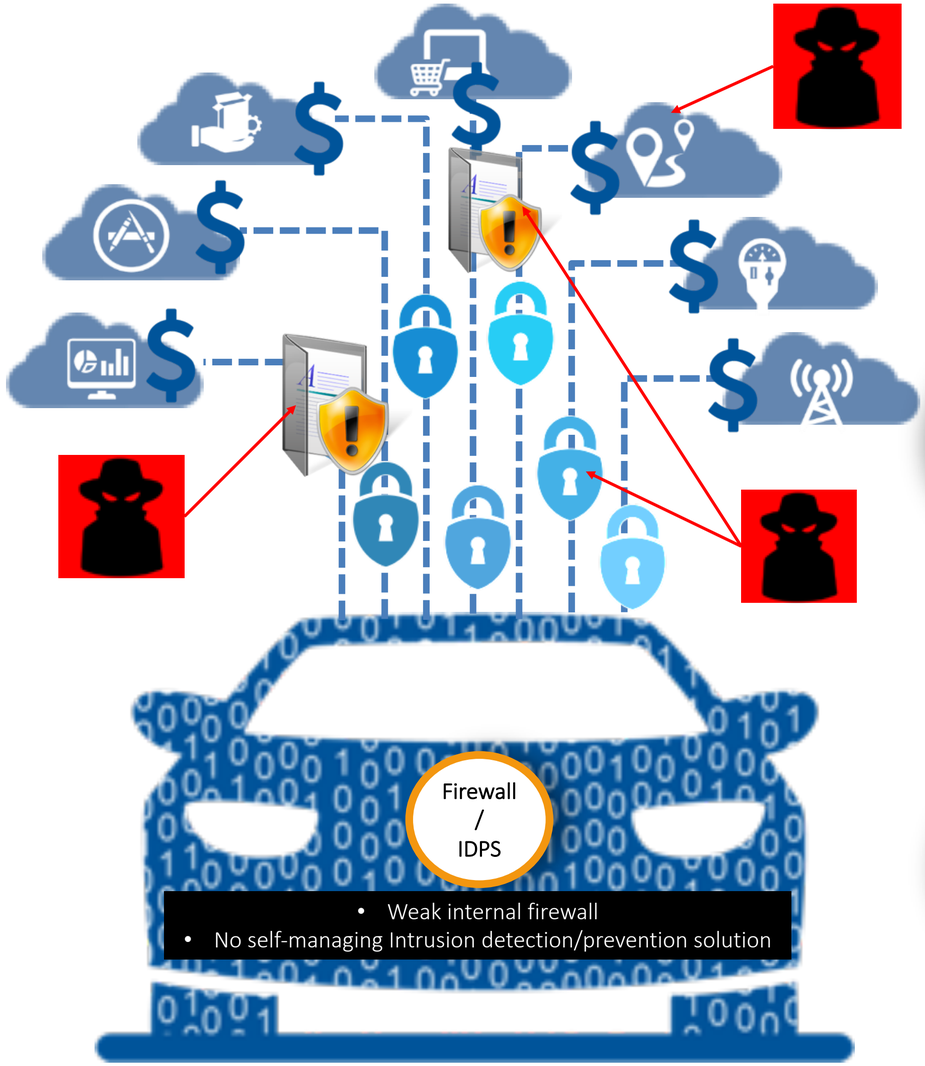
Mining

Construction

.....

Previous
Next

Vehicle-to-Cloud Communications Open to Cyber Attacks & Data Breach



Cloud

Fragmented cloud platform with inconsistent security
Weak security (username & password) for apps & services

Connect

Public Untrusted WiFi
Tethering with Cellular/WiFi

In-Vehicle Network

Open OBDII port & access to open CAN (Control Area Network)
Unencrypted communication over in-vehicle networks (CAN)

Autonomous Vehicle Open Challenges & Threats

Trust of Passengers?

Privacy

Security & privacy mechanisms for AV?
AV trust and privacy of passengers?

New Threats in AV?

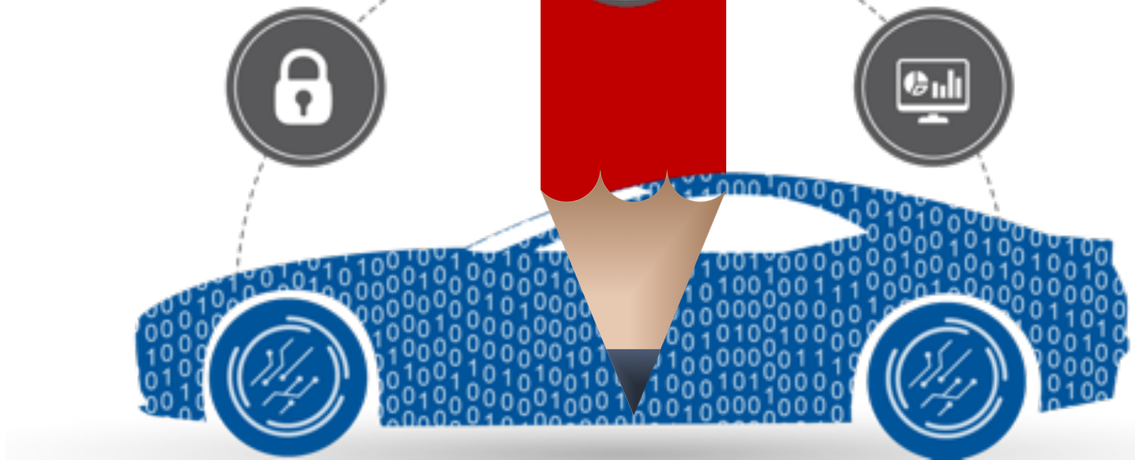
Attack

How can AV be attacked?
How is it different from Connected Vehicle?
How is it different from cyberspace?

How to Manage the Risks?

Hijack

Remote hijack of AV electronics with intention of causing crash?
Can the data stored onboard of vehicle be unlocked and exploited?
Is the risk management plan identified, defined and can it be mitigated or controlled?

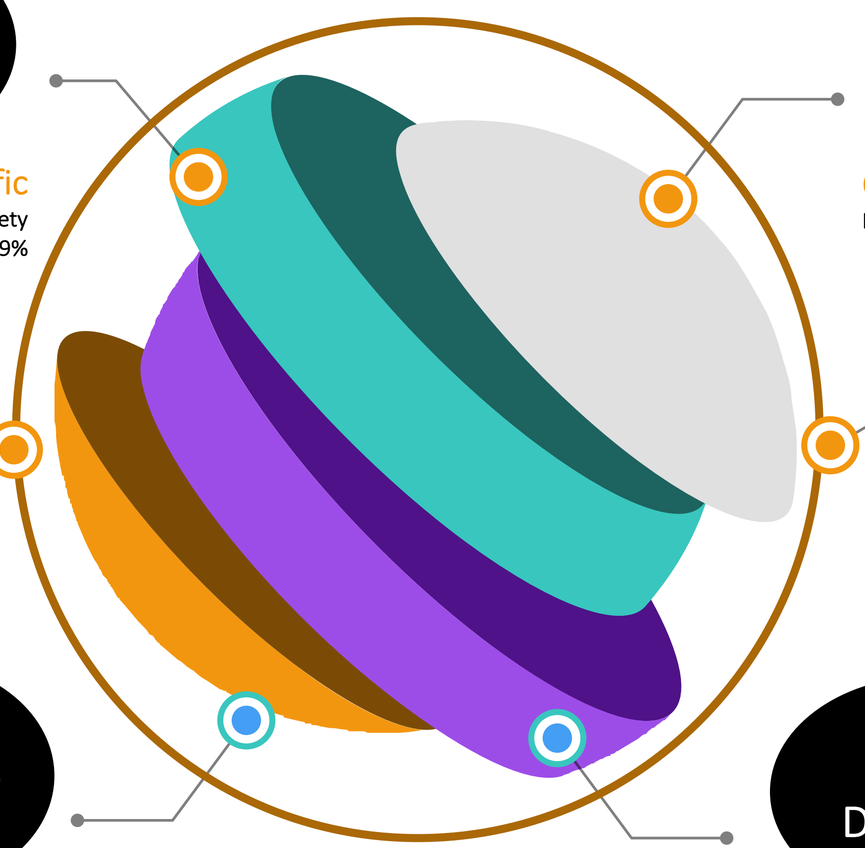


What's Next in Automotive Security?

1. SECURE Over-the-Air Updates
2. Building TRUST for Safer Driving
3. PROTECTING PRIVACY of Driver & Passenger
4. Creating a More SECURE ECOSYSTEM
5. PROTECTING Vehicle To Cloud Communication

Previous
Next

Autonomous Vehicle: Technical Challenges & Lack of Legal Framework



Safety

Ability to Cope with Urban Traffic

Not enough practical testing to ensure the safety reliability > 99.99999%

Outdated Law

Outdated law & regulations

Due to treat of public safety

Liability

Liability & Risk Model

The absence of vehicle operator or OEM liability

Data Ownership

General Data Protection Regulation

AV must comply with GDPR and adds an additional layer of security challenges to protect data theft

Unsecure

Unsecure Connectivity & Connected System

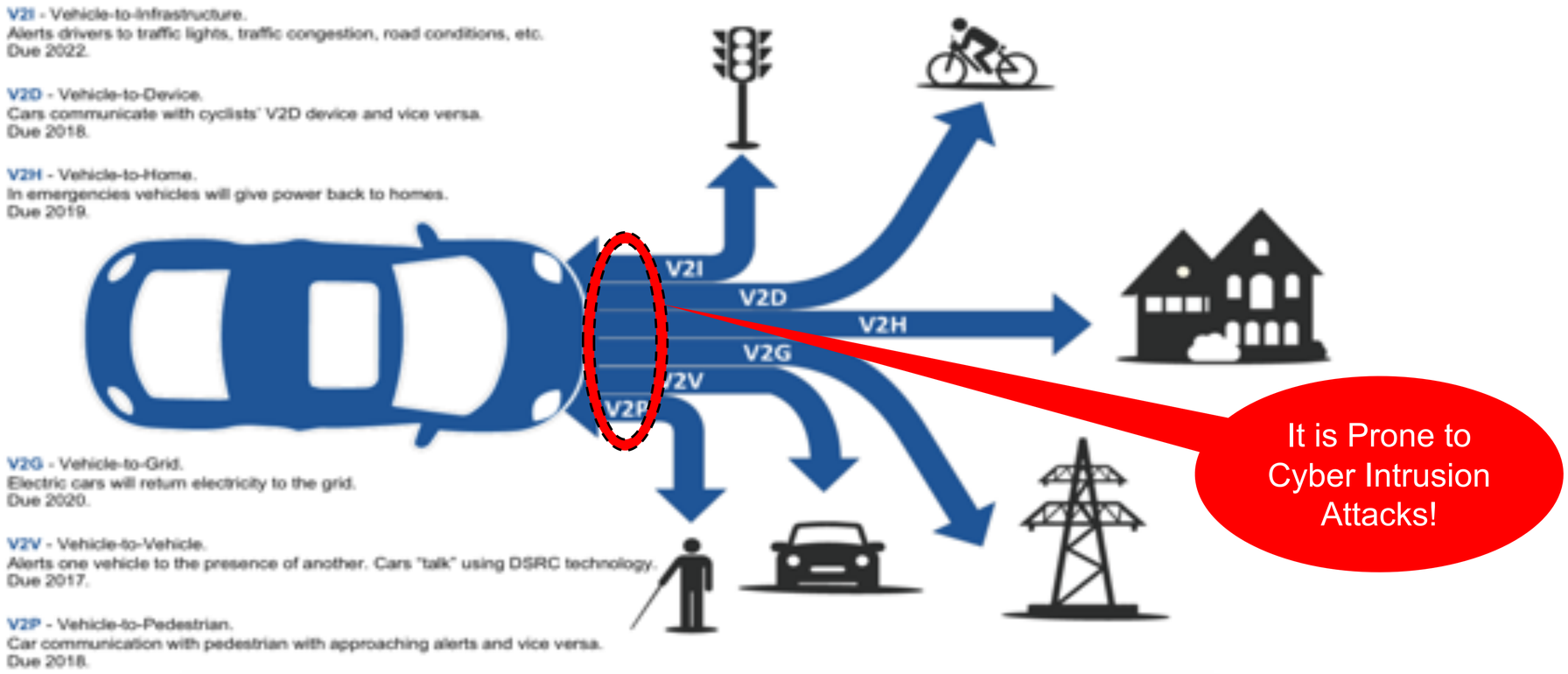
Bluetooth, WiFi, 5G/4G, V2X, in-vehicle CAN & entertainment, navigation, etc.

Ethical Dilemma

Moral & Ethical Dilemma

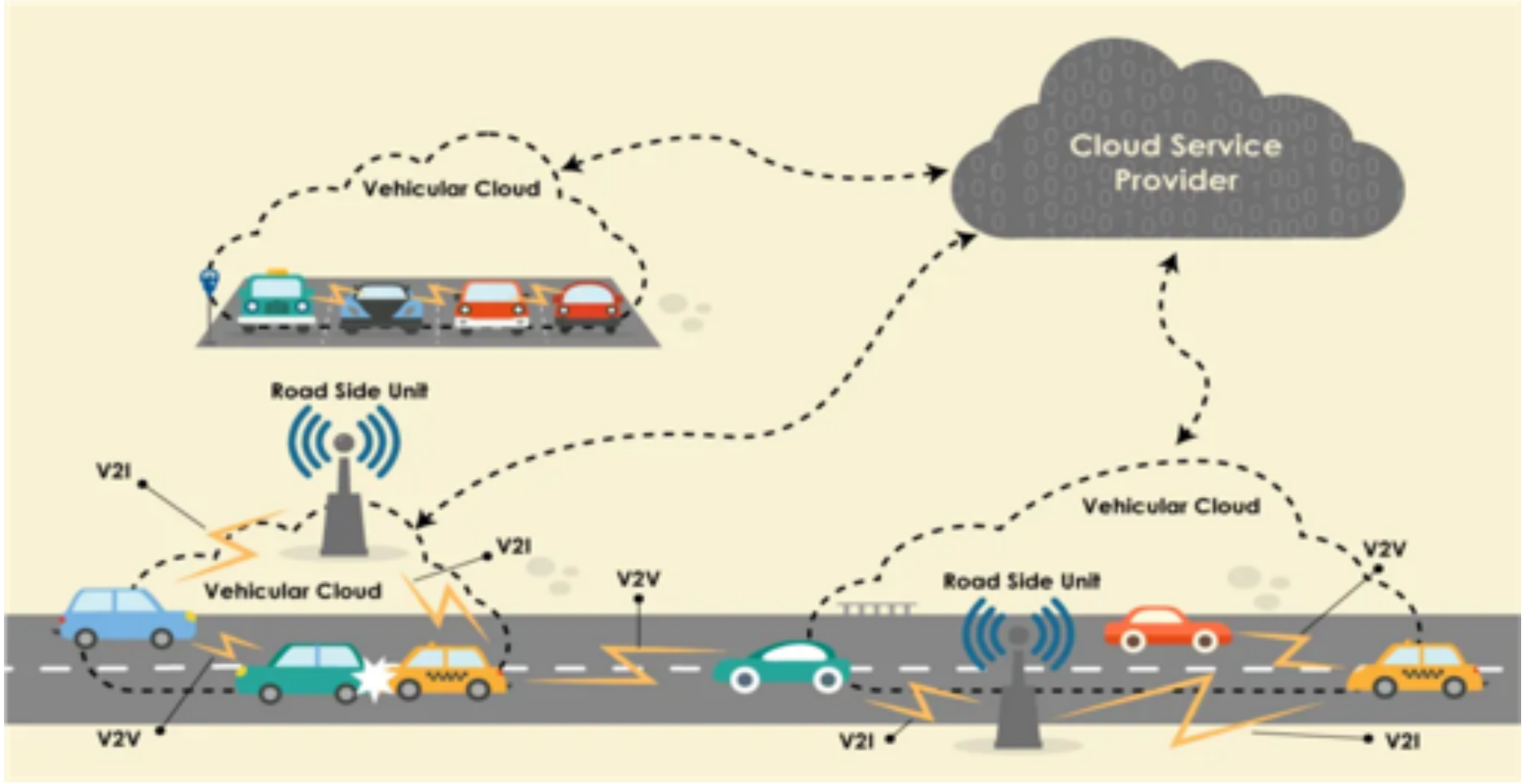
Hackers mess with the logic of these ethical machines, national security & societal backlash

Vehicle-to-Everything (V2X) Communications to Humans, Environment, Society & Industry



Is there Any Secure Channel in V2X Connection?

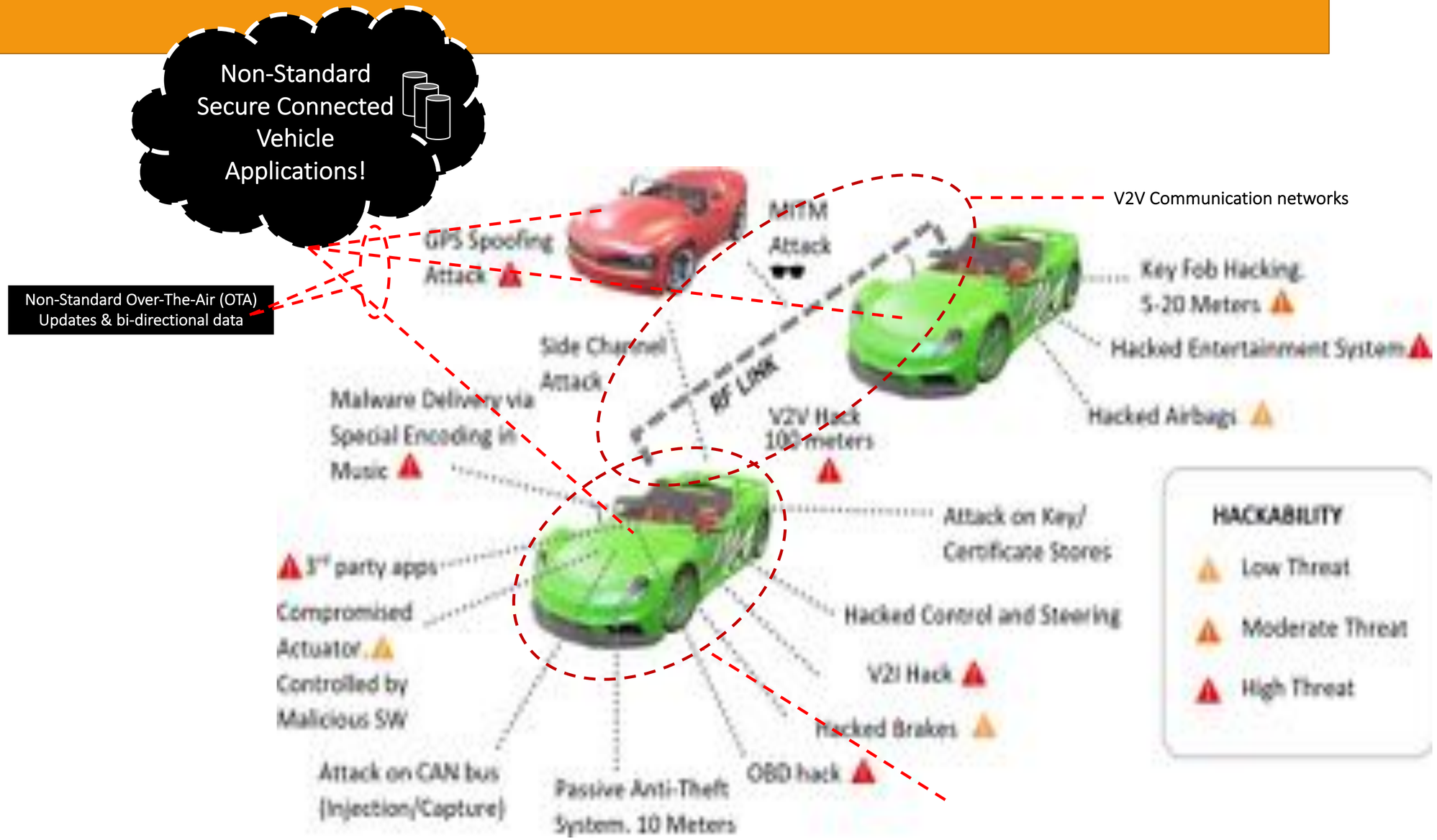
Vehicular Ad hoc Networks (VANET)



Reference: Convergence of Secure Vehicular Ad Hoc Network and Cloud in Internet of Things, Neeli Prasad, et. al.

Previous
Next

Vulnerabilities and Threat Levels



Potential Targets for In-Vehicle Cyber Attack
"Data Is The New Oil"

Privacy

Confidentiality

Real-Time Constraints

Integrity

Flexible Communication

Non-Repudiation

Previous
Next

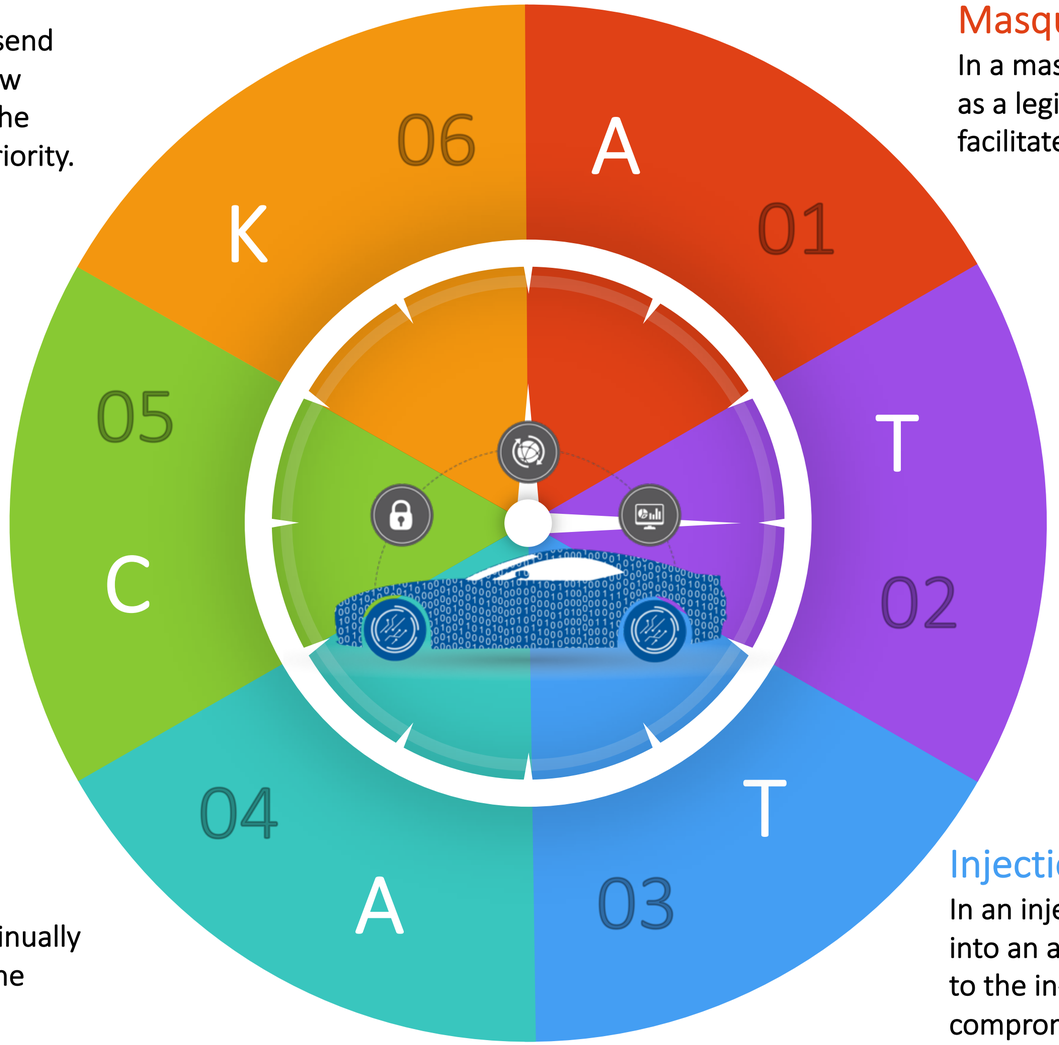
In-Vehicle Security Threats

DoS Attack

DoS attacks occur when attackers continually send high priority messages that block legitimate low priority messages. In a standard CAN packet, the identifier segment determines the message priority.

Masquerading Attack

In a masquerading attack, an attacker masquerades as a legitimate node. CAN vulnerabilities that facilitate masquerading attacks



Bus-off Attack

Bus-off attacks occur when attackers continually send bits both in the identifier field and in other fields, which causes the ECU's transmit error counter to then be incremented.

Eavesdropping Attack

Eavesdropping attacks occur when unauthorized individuals are able to gain access to vehicular messages.

Replay Attack

In a replay attack, attackers continually resend valid frames to impede the vehicle's real-time functioning.

Injection Attack

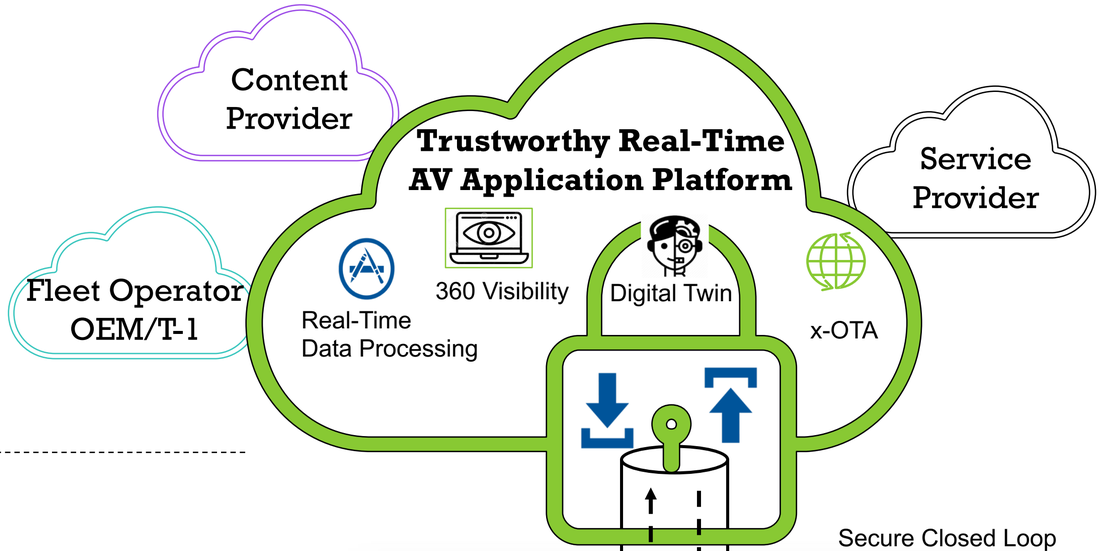
In an injection attack, attackers inject fake messages into an automotive bus system. Attackers can gain entry to the in-vehicle network through OBD-II ports, compromised ECUs, or infotainment & telematics systems.

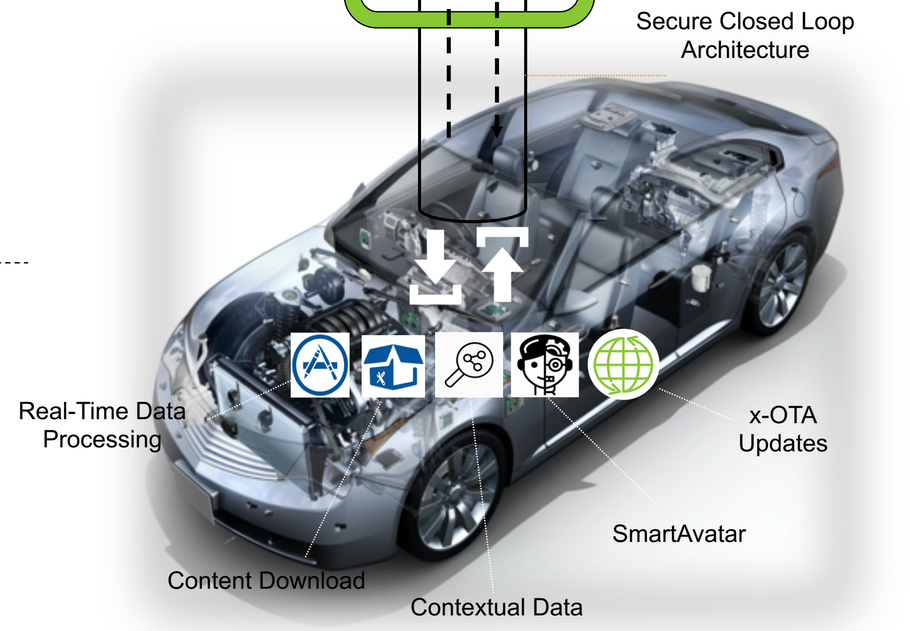
Trustworthy & Secure AV Software-Defined Vehicle Architecture

Off-board Intelligence (Cloud & Backend)

Trustworthy Connectivity

On-board Intelligence (In-Vehicle)





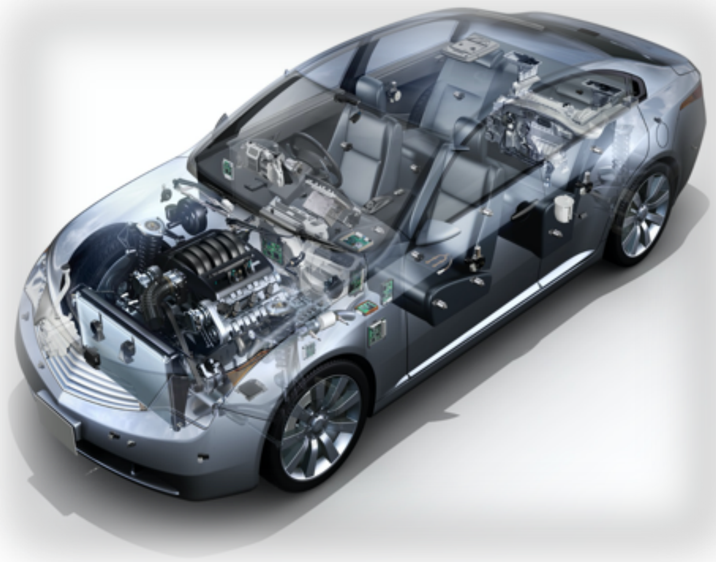
Trustworthy Cloud Platform:
- Comprehensive standardized secured x-OTA management
- Dynamic Digital Twin)
- Real-time data processing
- Secure distributed data management

Secure & Trustworthy Connectivity
- Trustworthy authentication & authorization
- Zero trust cybersecurity

Embedded Platform:
- Comprehensive x-OTA service for IVI, TCU, GW, ECU, etc.
- Contextual data acquisition with cloud managed policy
- Secure point-to-point in-vehicle communication

Previous
Next

In-Vehicle Hardware & Software Security Building Blocks



Security software and services

- Anti-malware
- Network enforcement
- Biometrics
- Cryptographic services
- Anomaly detection
- Over-The-Air (OTA) updates
- Other

Hardware Security Services for Secure Applications

- Device identification
- Isolated execution
- Message authentication
- High cryptographic performance

Hardware Security Building Blocks

- Platform boot integrity and chain of trust
- Secure storage (Keys and data)
- Secure communication
- Secure debug
- Tamper detection and protection from side channel attacks

Previous
Next

Cloud Security Services

1. SECURE Authenticated Channel to The Cloud
2. REMOTE MONITORING of Vehicle Activity
3. THREAT Intelligence Exchanges
4. SECURE Over-The-Air Updates
5. CREDENTIAL Management

Previous
Next

Conclusions & Future Work

1. Define how automotive OEMs engage with their suppliers and broader ecosystem “Supply chain security”.
2. Mandate entire AV supply chains to adopt more software security like practice “Security development lifecycle”.
3. Allow vehicle features to change and evolve as OEM improve their technology & 3rd party developers extend it “Operating securely for the full lifecycle".

AV will not only require a cross-domain self-managing security solution, it will also need to be updated more frequently than your smartphone today.

Previous
Next

Thank you

SmartAvatar

Enabling Trusted Software Defined IoT

LinkedIn: Neeli Prasad

https://SmartAvatar.nl