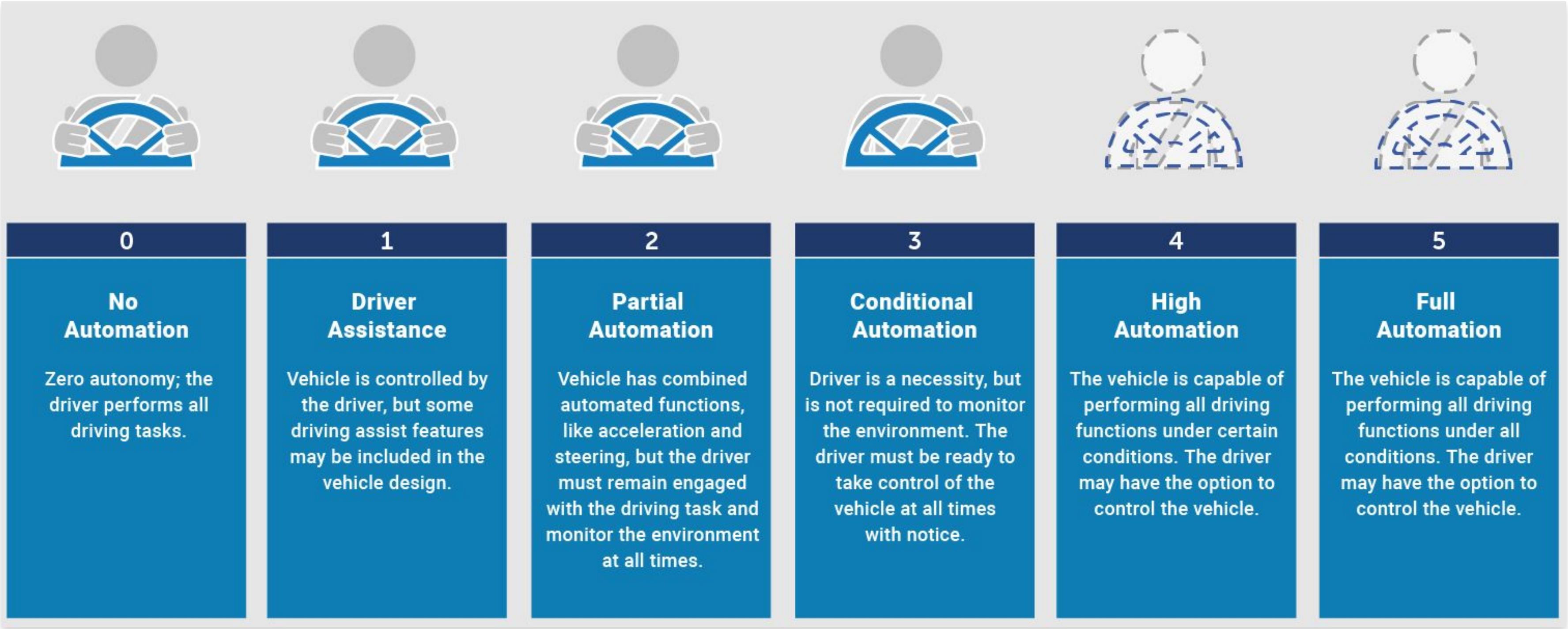
Autonomous Vehicle Cybersecurity

Threats, Vulnerability, Risks, Mitigations, Implementation challenges

PRANEETH VARMA

Tech Lead, Automotive Product Cybersecurity

Autonomous Vehicle - SAE Automation Levels

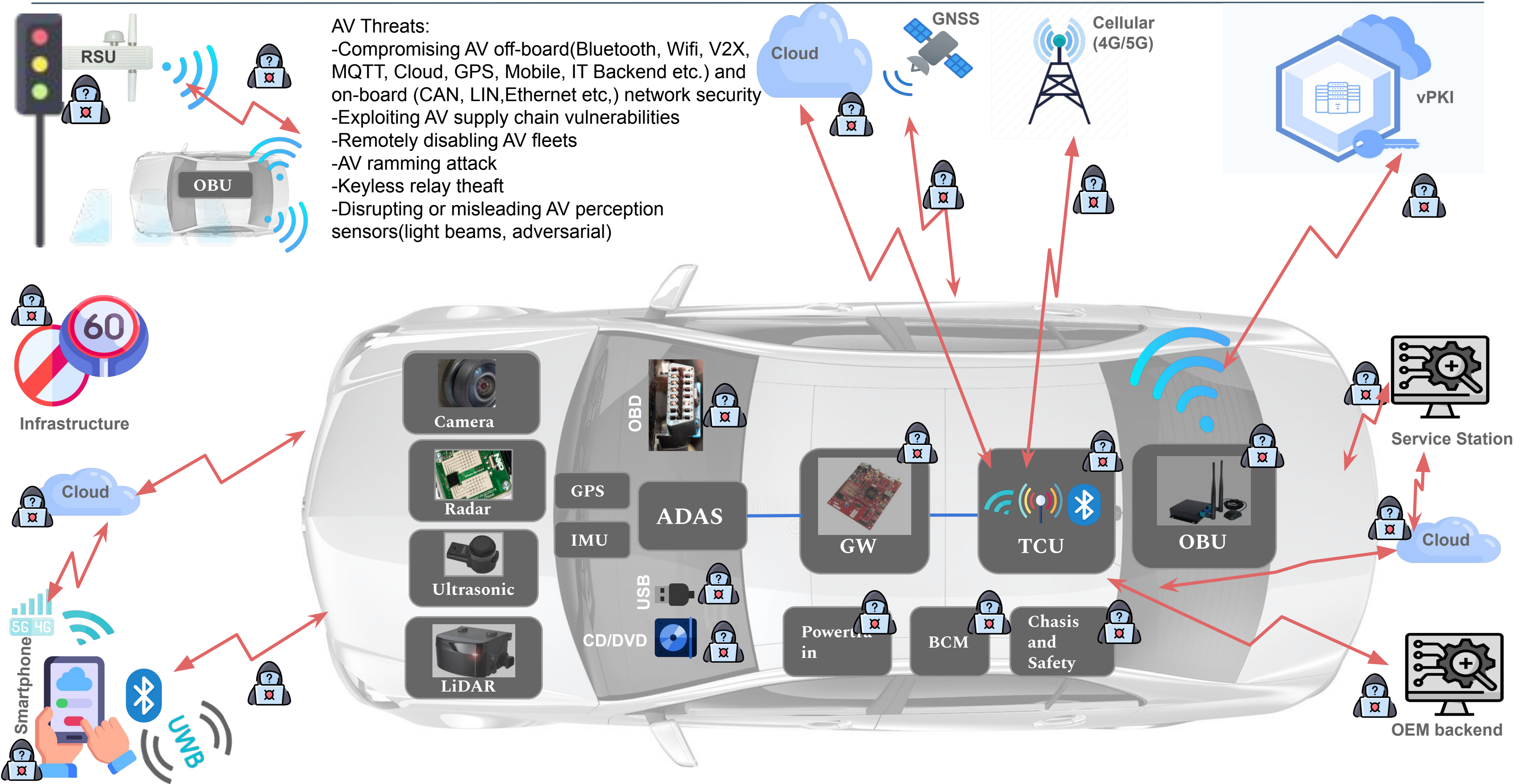


0	1	2	3	4	5
No Automation	**Driver Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

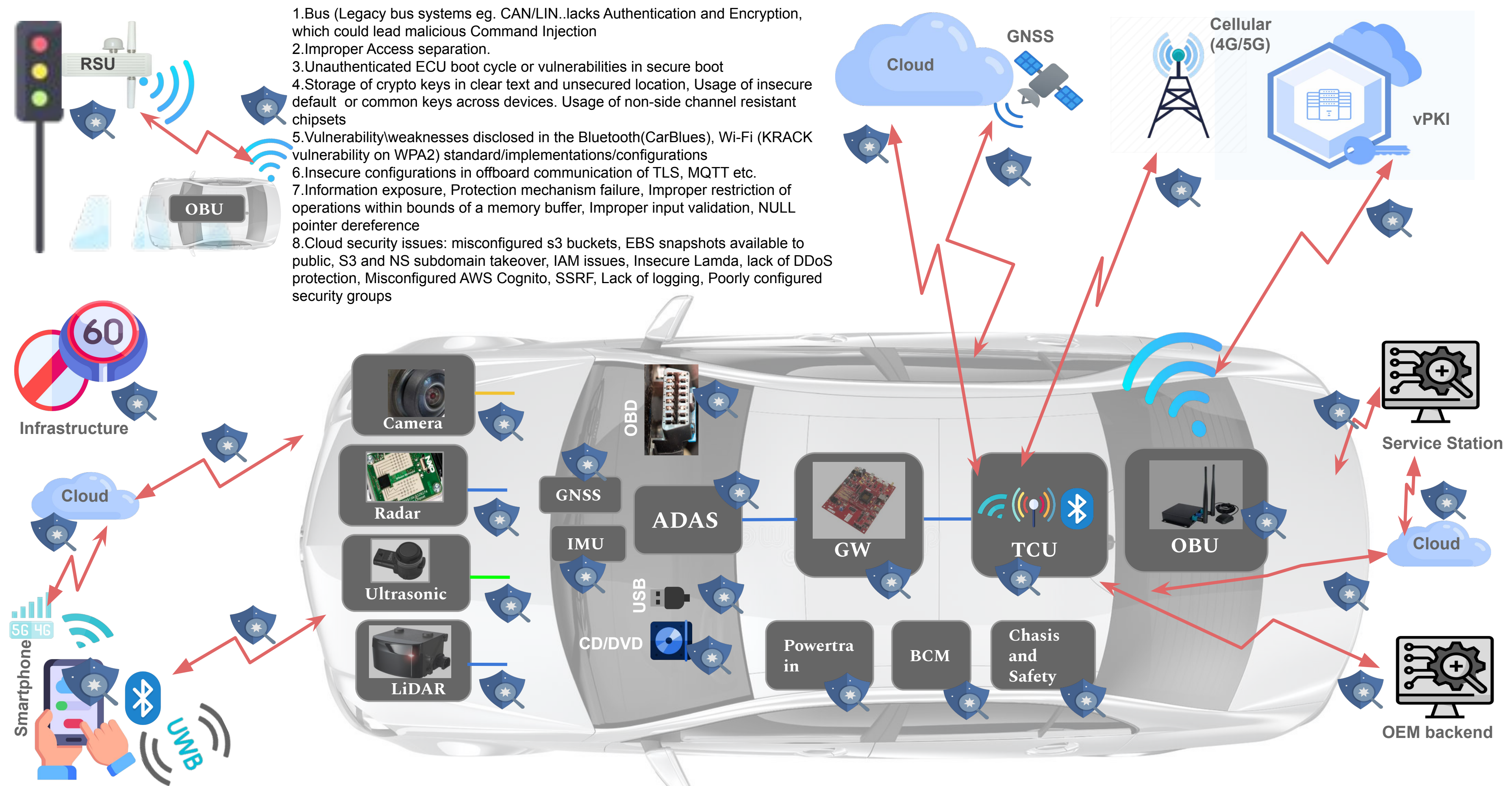
Ref: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety

Autonomous Vehicle - Threats

AV Threats:
-Compromising AV off-board(Bluetooth, Wifi, V2X, MQTT, Cloud, GPS, Mobile, IT Backend etc.) and on-board (CAN, LIN,Ethernet etc,) network security
-Exploiting AV supply chain vulnerabilities
-Remotely disabling AV fleets
-AV ramming attack
-Keyless relay theaft
-Disrupting or misleading AV perception sensors(light beams, adversarial)



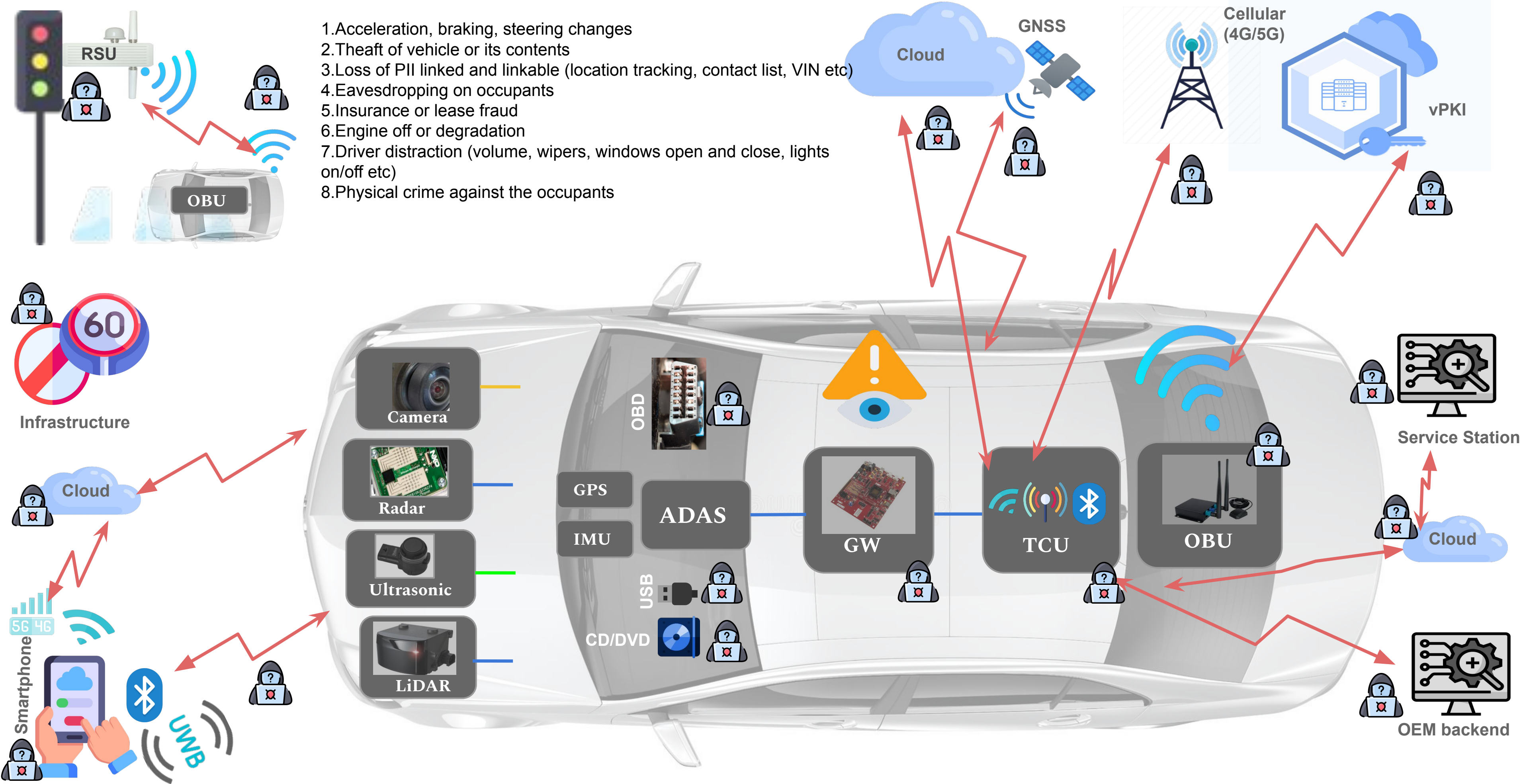
Autonomous Vehicle - Vulnerabilities



1.Bus (Legacy bus systems eg. CAN/LIN..lacks Authentication and Encryption, which could lead malicious Command Injection
2.Improper Access separation.
3.Unauthenticated ECU boot cycle or vulnerabilities in secure boot
4.Storage of crypto keys in clear text and unsecured location, Usage of insecure default or common keys across devices. Usage of non-side channel resistant chipsets
5.Vulnerability\weaknesses disclosed in the Bluetooth(CarBlues), Wi-Fi (KRACK vulnerability on WPA2) standard/implementations/configurations
6.Insecure configurations in offboard communication of TLS, MQTT etc.
7.Information exposure, Protection mechanism failure, Improper restriction of operations within bounds of a memory buffer, Improper input validation, NULL pointer dereference
8.Cloud security issues: misconfigured s3 buckets, EBS snapshots available to public, S3 and NS subdomain takeover, IAM issues, Insecure Lamda, lack of DDoS protection, Misconfigured AWS Cognito, SSRF, Lack of logging, Poorly configured security groups

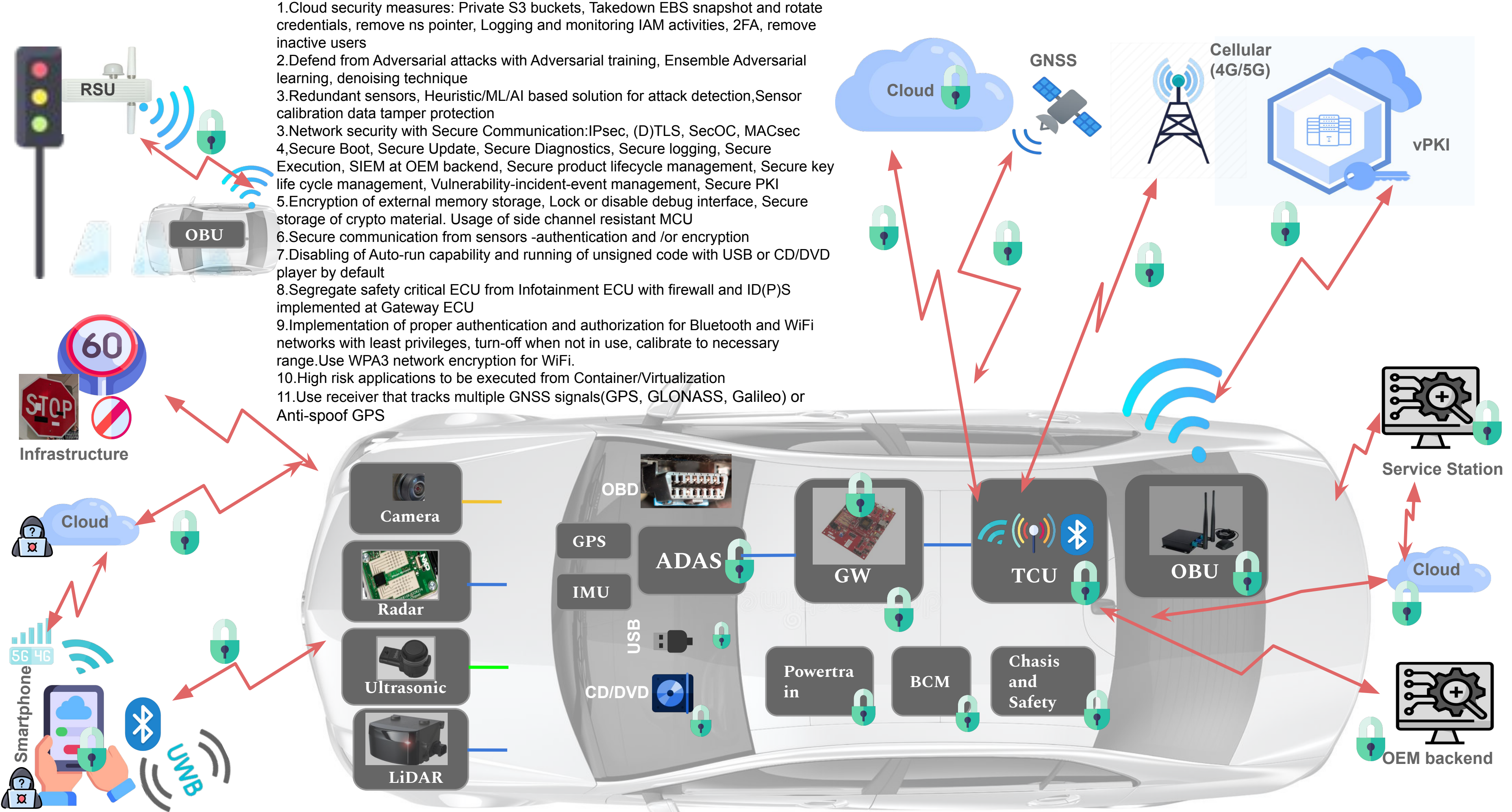
Autonomous Vehicle - Risks

1.Acceleration, braking, steering changes
2.Theaft of vehicle or its contents
3.Loss of PII linked and linkable (location tracking, contact list, VIN etc)
4.Eavesdropping on occupants
5.Insurance or lease fraud
6.Engine off or degradation
7.Driver distraction (volume, wipers, windows open and close, lights on/off etc)
8.Physical crime against the occupants



Autonomous Vehicle - Countermeasures

1.Cloud security measures: Private S3 buckets, Takedown EBS snapshot and rotate credentials, remove ns pointer, Logging and monitoring IAM activities, 2FA, remove inactive users
2.Defend from Adversarial attacks with Adversarial training, Ensemble Adversarial learning, denoising technique
3.Redundant sensors, Heuristic/ML/AI based solution for attack detection,Sensor calibration data tamper protection
3.Network security with Secure Communication:IPsec, (D)TLS, SecOC, MACsec
4,Secure Boot, Secure Update, Secure Diagnostics, Secure logging, Secure Execution, SIEM at OEM backend, Secure product lifecycle management, Secure key life cycle management, Vulnerability-incident-event management, Secure PKI
5.Encryption of external memory storage, Lock or disable debug interface, Secure storage of crypto material. Usage of side channel resistant MCU
6.Secure communication from sensors -authentication and /or encryption
7.Disabling of Auto-run capability and running of unsigned code with USB or CD/DVD player by default
8.Segregate safety critical ECU from Infotainment ECU with firewall and ID(P)S implemented at Gateway ECU
9.Implementation of proper authentication and authorization for Bluetooth and WiFi networks with least privileges, turn-off when not in use, calibrate to necessary range.Use WPA3 network encryption for WiFi.
10.High risk applications to be executed from Container/Virtualization
11.Use receiver that tracks multiple GNSS signals(GPS, GLONASS, Galileo) or Anti-spoof GPS



Autonomous Vehicle - Implementation Challenges

Mechanism	Layer	Description	Challenges
SecOC, UDS Service 0x27, UDS Service 0x29, DoIP	Layers 5-6-7	Autosar SecOC: Standard from AUTOSAR, computes CMAC or signature to the I-PDU -Freshness management by appending timer (or) counter	SecOC: To perform TARA and derive the critical signals for protection UDS 0x27 and 0x29: Symmetric or Asymmetric UDS security approach to be chosen
TLS, DTLS	Transport Layer 4	-End to End Security -Collection of protocols: Handshake, Change Cipherspec, Alert, Application data	Generation and sharing of client and server certificates, Configuring cipher suites, Selection of TLS library with light weight and secure from open-souce vulnerabilities
IPsec	Network Layer 3	-Encrypts IP payload of any kind TCP, UDP, ICMP etc. -Collection of protocols: AH, ESP, IKE -Can not protect DHCP and ARP traffic	Complex and suitable for offboard communications
MACsec	Data link Layer 2	-MACsec (IEEE 802.1AE) can protect all DHCP and ARP traffic -MACsec is point-to-point security protocol providing data confidentiality, integrity, replay protection and origin authenticity for traffic over layer 1 or layer 2 links of ethernet LANs -MACsec built in encryption and decryption combined with key authentication for additional security at layer 2, provided at cost effective with silicon vendor point of view	Triggers a change in silicon or a necessity for external ethernet extension card
Ethernet link	Physical Layer 1	1000 Base TX, 100 Base T1, 1000 Base T1, Multi-Gig	-Plausibility checks & Redundant communication -Change in design with respect to GW, Tools, Design to replace legacy networks operated on CAN

Autonomous Vehicle - Security Attributes & Countermeasures

Security Attributes

- Data origin authenticity
- Integrity
- Controlled access (authorization)
- Freshness
- Non repudiation
- Privacy/anonymity
- Confidentiality
- Availability

Countermeasures

- Controller Authentication - for confidential information
- Encrypted Communication -
- SecOC - for authentic signal based communication
- Gateway Firewalls
- TLS/DTLS
- IPsec
- Packet filtering
- Device Authentication - authentication of client and server, data integrity
- VLAN/IPSec

Challenges

- AI/ML security
- vPKI for V2X security
- IDPS is difficult to be realised with AVs!
- IDS needs thorough validation & verification before deployment in AVs!
- Event Logging and reporting
- Incident management
- End of life destruction of keys
- Functional Safety and Cybersecurity reconciliation & concepts implementation ……..more

Autonomous Vehicle - Security

Thank you