LTI

Let's Solve

Whitepaper

Security Imperatives for Connected Vehicles

Authors:
Sachin Kulkarni
Manabendra Mukherjee

A Larsen & Toubro
Group Company

Contents

Executive Summary

Automobiles have come a long way since the iconic Model T's runaway success in early 20th Century. Two decades back, in 1996, General Motors introduced the first "Connected Car" with "OnStar" feature in Cadillac DeVille. Suddenly, a car could place a cellular call in case of medical emergency. Remote Diagnostic features were introduced in 2001, whereas Navigation and Network access devices made their way into the Car in 2003. In the year 2007, Data-driven Telematics was offered. Finally, in 2014, Audi introduced 4G LTE Wi-Fi hotspot access that was later deployed at a mass level by General Motors. Auto Industry had just begun to realize a very potent revenue stream by offering Consumers a "Connected" Experience.

It is estimated that global connected car market reached USD 32 billion in 2016. In fact, it is expected to reach USD 155 billion by 2022. There are expected to be more than 200 million connected vehicles around the world by 2020.

According to Strategy &, at the moment of initial purchase customers are willing to pay up to 15 percent of a car's list price, or as much as USD 10,000, for connected car technology.

However, with an increased number of connected cars on the road, the fear of hackers taking control of the car and causing collateral damages have also become realistic. A Kelly Blue Book survey found that 42% of consumers support cars being more connected, while 62 % feared that cars in the future would be easily hacked.

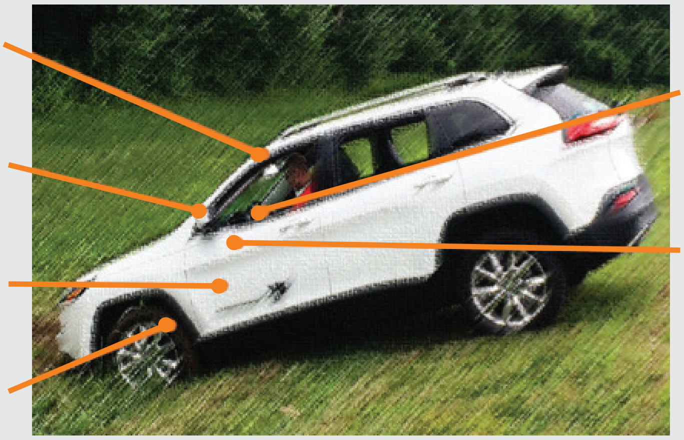
Connected Car architecture enables capability of vehicle communication with proximal vehicles (V2V), Infrastructure (V2I) and Application (V2X). All these communications are accomplished through a wireless messaging protocol – Dedicated Short Range Communication (DSRC) over Cellular Connection. Potential hackers would most likely begin from here.

By 2022, over **50%** of Connected Car revenue is expected to come from Volume Models up from **35%** in 2017, increasing profitability.

Jeep hack on a Highway

St. Louis (2015)

In a demonstration, ethical hackers Charlie Miller and Chris Valasek remotely took control of a Chysler Jeep, driven at 70 MPH on a Highway



A/C and Radio activated at maximum power

Windshield wiper turned on with wiper fluid blurring vision

Transmission was severed

Took control of Steering and engaged Brakes remotely

Chrysler's Uconnect feature allowed connectivity to car's infotainment system via cellular connection

Hackers rewrote the firmware of hardware for infotainment system and sent command to internal ECUs controlling engine and wheels

Chysler announced massive recall of 1.4 Million vehicle with unsafe Uconnect computer

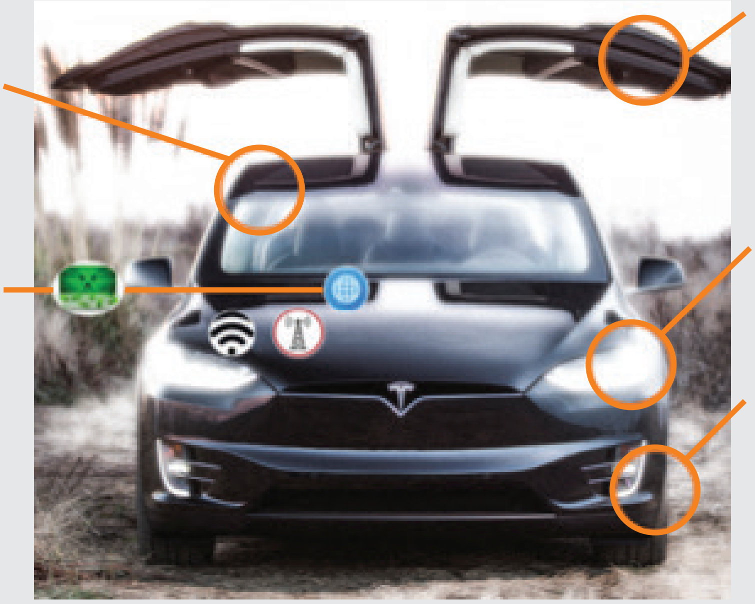
Cybersecurity as a real threat for Connected Vehicle was popularized in 2015, with an ethical hacking of Chrysler Jeep demonstrated to WIRED.com. In March 2016, the FBI, the Department of Transportation (DoT), and the National Highway Traffic Safety Administration (NHTSA) issued a public service announcement warning consumers about potential cybersecurity threats to connected cars.

Exhibit 1: Chrysler Jeep Security Vulnerability

The strong value proposition of Connected Vehicles, to seamlessly integrate a plethora of services including Infotainment, Safety, Security, Maintenance, Communication, Remote Updates, etc., also exposes serious security loopholes, which could be potentially exploited by rogue hackers or malicious programs. Few of the instances have already been exposed by ethical hackers/security researchers, who have gained remote access to the vehicle and virtually toyed around with the vehicle at the grave risk to the occupants. Since 2011, vehicle connectivity has been a target for Ethical hacking, starting from General Motors OnStar system to Chrysler and Tesla. However, these widely publicized exploits help Automakers identify the security gaps, and patch them with recall or over-the-air updates. Chrysler's Jeep had been hacked in 2013 when couple of security researchers gained access to Car's closed internal network through OBD-II ports. In 2016 (see Exhibit), they used infotainment systems cellular connection to gain access to the Controlled Area Network (CAN) bus. In 2017, the vehicle was hacked through the USB port.

The Unauthorized Xmas Show

Las Vegas (July 2017)



A Group of Chinese Security Researchers hacked into Tesla Model X

Pushed Malicious programs through car's web browser via Wi-Fi/ Cellular Network

Remotely controlled opening/closing of Doors and Trunks

Blinked lights in tune with streaming music from car's radio

Engaged Brakes remotely

In July 2017, a group of Chinese Security Researchers demonstrated in Las Vegas Black Hat convention that Tesla's premium Model X can be compromised. The same group also hacked into Model S in 2016.

Exhibit 2: Tesla Model X Security Vulnerability

Tesla has clearly revolutionized the concept of a reliable connected Electric Car as a means of long-range transportation leaving conventional vehicle makers in a quandary. However, a group of Chinese Security researchers clearly demonstrated that Model X is hackable over the air and passenger security can be compromised.

Tesla has been working along with the researchers to plug the security loopholes. However, in 2017 the researchers were able to breach additional vulnerabilities. Tesla's vehicle for mass Model 3 will probably inherit much of the qualities, as well as vulnerabilities of existing Models.

Potential Security Vulnerabilities

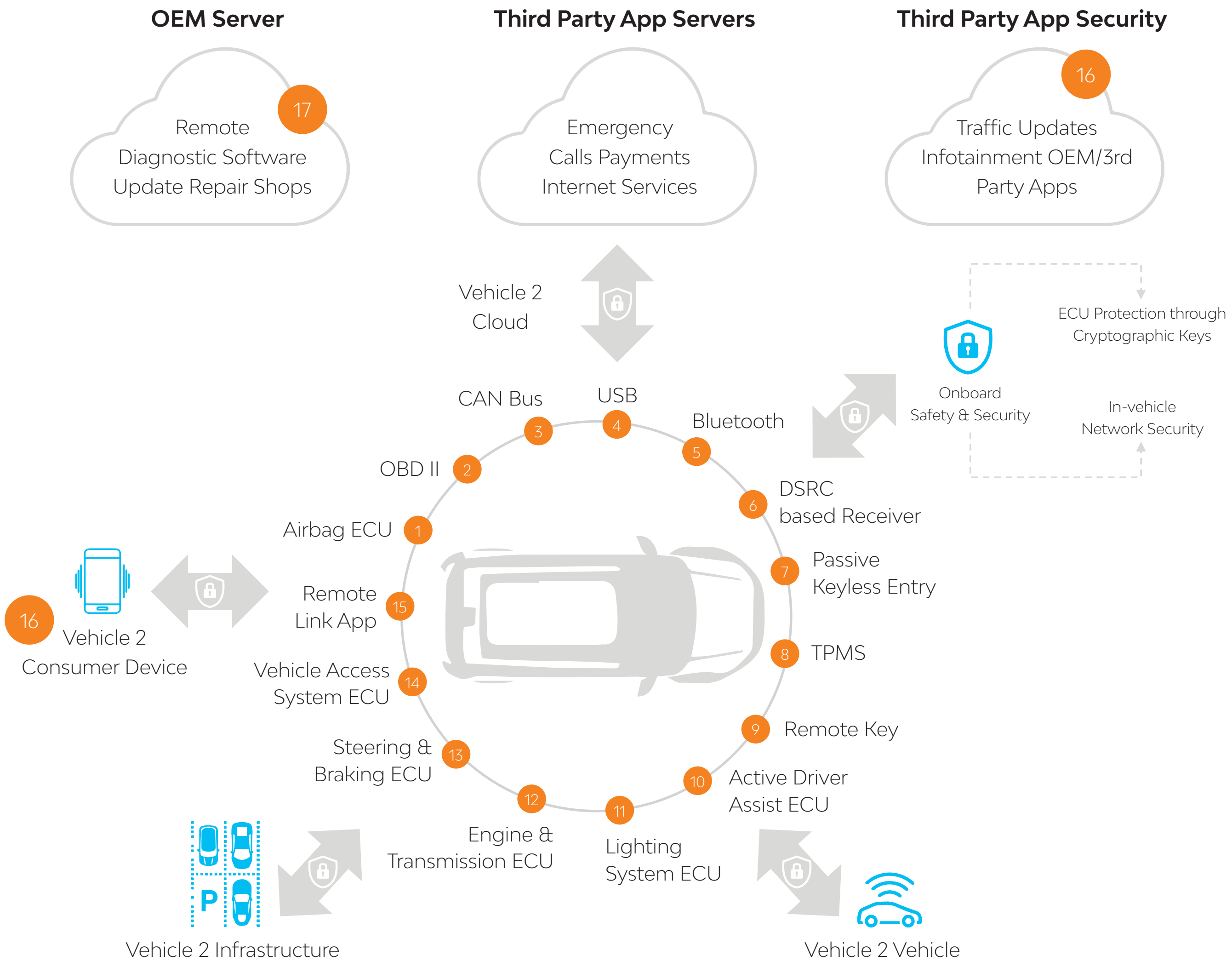


Exhibit 3: Connected Car Architecture & Vulnerabilities

In the future, Connected Vehicles (CVs) will accomplish a multitude of tasks while on road. They will communicate with legacy or modernized Traffic Infrastructure and sensors (V2I) wirelessly. Vehicles will be aware of presence of other vehicles, pedestrians, cyclists (V2V), etc. CV platform will support OEM and Third Party applications related to Traffic updates, Navigations, Weather, Entertainment and other uSmart homes.

For smart businesses to grow, CVs need to be integrated with the IoT ecosystem to offer an end-to-end connected experience.

However, as CVs rapidly transform the automotive experience, they would also become more vulnerable to a range of security threats due to presence of a mix of standard legacy and futuristic technologies.

ECUs

Modern CVs deploy more than 100 ECUs, which perform a plethora of functions ranging from Engine – Transmission Control, Airbag deployment to climate and infotainment control. Security attacks targeted towards ECUs mainly focuses on re-writing the firmware on compromised ECUs. The compromised ECU then propagates spurious messages to connected ECUs to confuse/override and intervene in their core functions rendering these "zombie" ECUs instigate abnormal behavior from the overall system.

CAN Bus

Controller Area Network (CAN) Bus is one of the primary communication platforms in CVs, which supports communication within a closed network of Electronic Controller Units (ECUs) through non-secure messages. An unauthorized access can manipulate these messages to send spurious communication to ECUs in order to effect unintended behavior.

Diagnostic Tools

Auto Manufacturers have used the built-in OBD-II ports to retrieve diagnostic codes and other information since 1996. Although these ports provide read-only access, some OEMs allow commands to be sent over CAN bus. There are tools available to allow malicious reading and manipulate data through CAN bus.

Infotainment

Automakers rely on Infotainment systems to provide feature-rich services and content to customers, often on a subscription basis. However, it is also an easy target for exploitation due to multiple connectivity channels established with various web services. Any vulnerability like - unencrypted API call or misconfigured server - may provide an opportunity for intrusion and Launchpad to attack other control units.

Keyless Entry

Remote keyless entry feature allows communication between a remote fob or Smart phone and vehicle over Bluetooth, NFC or Internet. These codes may be 'tapped' by devices and replayed back to gain access to the vehicle directly.

Vehicle Communication

Within the vehicle, On Board Equipment (OBE) manages all V2V, V2I and V2X communications. OBEs integrate with CAN bus to collect important information like vehicle speed, brake system status, etc. and communicate with external entities. Thus, a compromised vehicle may broadcast false data to the environment with a catastrophic effect.

Unauthorized APIs and Third Party App Security

Attack surface of CVs extend beyond car itself. It can include external Wi-Fi, Cellular Network, as well as extend to Cloud-based apps and any security loophole that may exist. Auto Manufacturers need to co-operate and develop secure APIs for mobile application developers to use. This involves clearly defining means for authenticating transactions, encrypting and integrity checking.

Smartphones

Smartphones are either replacing or working along with Fobs in performing operations. In addition, Smart Phones are also becoming an extension to Apple CarPlay or Android Auto. Thus, a compromised Smart phone typically provides a mean to attack the OS of the CV as well.

Potential Exploitation Methods	Severity
Unauthenticated API (e.g. Remote Features)	🟡
Mobile App Vulnerabilities	🟡
Reverse engineer Firmware/Modify MCU to bypass security controls or change functionality	🔵
Locally / Remotely exploit Self-Driving Vehicle (SDV) Code	🔵
Infiltrate Supply Chain to install Malware and possibly inject into an entire ecosystem	🔵
Physically interface via USB port to install malware	🔵
Identify methods to circumvent Safety features	🔵
Monitor messaging traffic for an extended time	🟡
Knowledge of vehicle location, regular routes taken, and duration of stay	🟡
Infect with Ransomware to restrict/limit use	🔵
Implement Denial of Service against traffic infrastructure	🔵
Exploit weak cryptographic features	🔵
Exploit unchanged/weak passwords used somewhere in a CV's software	🟡
Spoof Sensors (e.g. LIDAR, GPS)	🔵
Steal or Crash Autonomous vehicle	🔵
Coordinate attack on vehicle/infra (Denial of Service, Internet and Wireless domains)	🔵
Overload circuit board	🔵

Counter Strategies to enhance security

Automotive Industry has realized that collaboration and information sharing will be key to address the multi-front threat to CV ecosystem. Automotive Information Sharing and Analysis Center (Auto-ISAC) was set up in 2015 to share best practices and help design multi-layer hardware and software systems that are harder to hack. Auto-ISAC has compiled a framework of Best Practices to cover Organizational and Technical aspects of Cyber Security, which was published in January 2016 (Exhibit 4).

Vehicle Cybersecurity Governance

Define executive oversight | Define R&R to align organization | Communicate oversight responsibility | Dedicate appropriate resources | Establish processes to ensure compliance

Risk Assessment & Management

Establish Risk Assessment Process | Establish Risk Management Process | Develop Risk Communication Process| Monitor & Evaluate changes in identified Risk | Supply Chain Risks | Assess supplier compliance to Security Guidelines | Assess/Evaluate Risk at Vehicle Development Stages

Security by Design

Assess and address security threats in Design Process| Reduce surface of attack | Create layered defenses | Identify & protect trust boundaries | Conduct Security design review during development | Secure connection within/outside the vehicle | Limit network interactions | Limit network interaction | Evaluate component for integrity & security | Test for software vulnerability | Test/Validate Vehicle Security system | Authenticate/validate all software updates | Consider data privacy risks/requirements

Threat Detection & Protection

Assess Risks/Deposition of threats/vulnerabilities | Inform Risk-based decisions | Routine scanning and testing of High Risk area | Anomaly detection for OS, services and connected functions | Outline vulnerability disclosure from external parties | Report threats and vulnerabilities to third parties

Incidence Response & Recovery

Document Incidence response lifecycle | Establish Incident response team | Periodic testing/Incidence simulation | Identify & validate source of incident in a vehicle | Determine potential fleet-wide impact | Contain to eliminate/lessen severity | Promote Timely/appropriate action | Restore standard vehicle functionality | Notify Stakeholders | Improve response plans over time

Training & Awareness

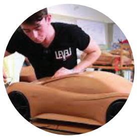
Establish training programs across ecosystem | Include IT/Mobile/vehicle specific Cyber security | Educate on security awareness, R&R | Tailor training & awareness programs to roles

Collaboration & Engagement

Review information before release to Third Party | Engage with industry bodies | Engage with Governmental bodies | Engage with academic institutions/Cybersecurity researchers | Form partnerships and collaborative agreements

Exhibit 4: Auto-ISAC Best Practices for Cyber Security

The holistic approach towards securing the CV ecosystem will have to extend beyond the technology stack. Exhibit-5 encompasses changes necessitated across Automotive Value Chain (Design to After Sales) to ensure that all weak links are covered.



Design

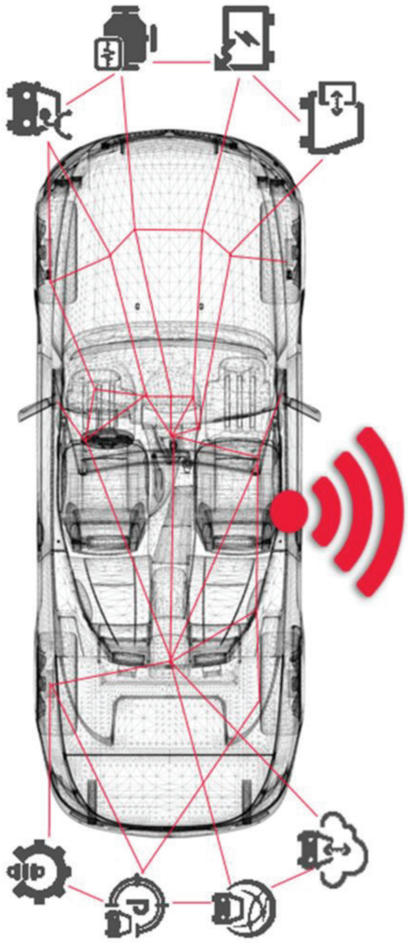
- Ensure right technologies (routing, Connectivity, security, etc) designed in the early development
- Choose connectivity partner, management platform and design features based on service offerings

Manufacturing

- Enable convergence of networking and IoT solutions to automate operations, mitigate risk and maximize uptime
- Leverage vehicle-prognostic data to improve quality, reliability and safety of the vehicle

Testing

- Test each individual services (3D Map, real-time updates, traffic, weather apps) before shipping



After-Sales

- Secure over-the-air (OTA) updates
- Partnering with aftermarket solution providers and third party security experts

Pre-Sales

- Prevent theft, hijacking or remote control of vehicle during customer demo
- Enforce certificate-based security to prevent unauthorized registration of VIN in mobile app and misuse

Shipping

- Disable connected services before transit
- Protect telematics SIM card physically, as well as with automated rules
- Shut-off communication to discourage hacking and illicit use of car's connections

Exhibit 5: Security across Vehicle Life Cycle

Security by Design

Cryptographic Key Implementation

Some of the auto manufacturers have been implementing Cryptographic key-based security to address the CAN messaging vulnerabilities. This is typically one-time generated Data tags, which is sent between ECUs, along with Message. The receiving ECU generates an independent Data Tag, based on the Message and matches with receiving tag. A perfect match indicates authentic source of message. Typically, keys are assigned to ECUs during the Final stage of vehicle Assembly. These keys are stored at an Enterprise level for future reference. Any subsequent changes due to servicing needs is initiated by a request from Service department to the central server, which issues a new Key. This key is passed on to the dealer for further action at dealer end. The mechanism addresses the CAN bus vulnerabilities of connected vehicle.

Vehicle Platform Security

Segmentation

Vehicles should employ multiple CAN buses, which segregate between Safety Critical and Non-Safety Critical Operations. Additionally, separation must be maintained between external interface/gateway and Can Buses. Gateway security devices can be used to achieve separation.

Secure Configurations

CVs often deploy Operating system within the vehicle. Wireless Access Points (WAPs) are provided for Consumer convenience. However, configurations should be made as restrictive as possible.

Secure Updates

Vehicle software updates are increasingly moving towards Over-the-Air (OTA) and ability to rollback after a negative result/error is also becoming important. However, software updates need to pass rigorous certification/testing requirements, and they should be least intrusive in terms of customer convenience and vehicle operation.

Interface Filtering

Attackers often exploit unprotected interfaces to gain access to non-safety critical interfaces. Security control incorporating Firewall defenses must filter incoming traffic for malware messages by defining and bounding type of data to be included in message.

Secure Protocol

Present day CVs communicate with devices over Bluetooth Low Energy (BLE) and Wi-Fi hotspot/access points. Security Architecture must protect unintentional connection with unknown/unsecure devices and allow intrusion.

Mobile App Security

CV mobile app development should incorporate certificate pinning to prevent man-in-the-middle (MITM) attacks over untrusted networks

Traffic Infrastructure Security

Traffic infrastructure and equipment that provide GPS signal, support Toll payments and monitoring traffic speed and radio equipment that facilitates DSRC communication between Infrastructure and vehicles, etc are spread across geographies and not necessarily connected. Traffic infrastructure in V2I environment will be a mix of modernized and legacy infrastructure. This poses as significant target for attackers.

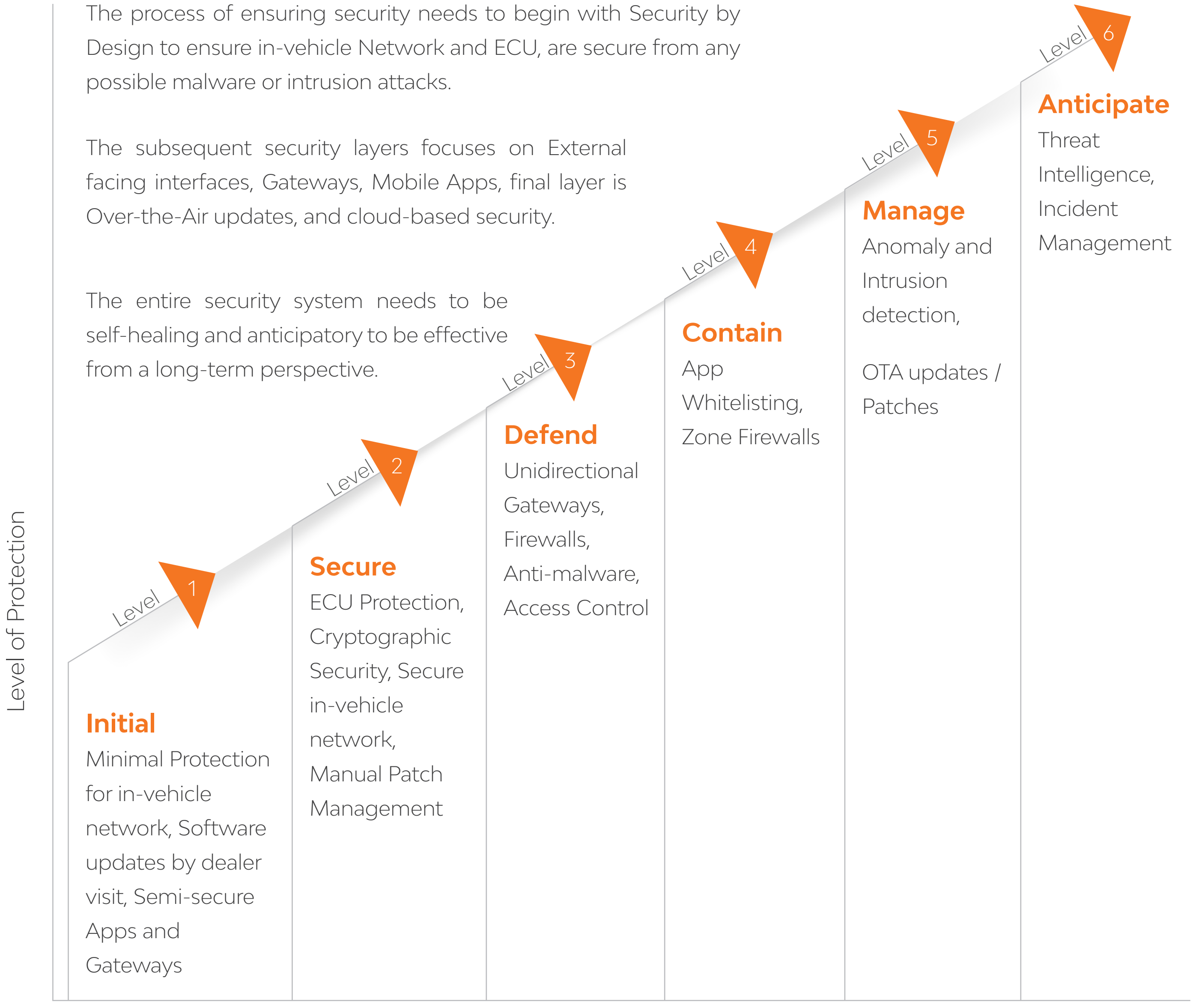
However, following preventive mechanism can improve the safety of Traffic Infrastructure to a great extent-

- Device Management
- Monitoring
- Malware defense
- Wireless Access Controls

The process of ensuring security needs to begin with Security by Design to ensure in-vehicle Network and ECU, are secure from any possible malware or intrusion attacks.

The subsequent security layers focuses on External facing interfaces, Gateways, Mobile Apps, final layer is Over-the-Air updates, and cloud-based security.

The entire security system needs to be self-healing and anticipatory to be effective from a long-term perspective.



Level 1

Initial

Minimal Protection for in-vehicle network, Software updates by dealer visit, Semi-secure Apps and Gateways

Level 2

Secure

ECU Protection, Cryptographic Security, Secure in-vehicle network, Manual Patch Management

Level 3

Defend

Unidirectional Gateways, Firewalls, Anti-malware, Access Control

Level 4

Contain

App Whitelisting, Zone Firewalls

Level 5

Manage

Anomaly and Intrusion detection,

OTA updates / Patches

Level 6

Anticipate

Threat Intelligence, Incident Management

Exhibit 6: Automotive Cyber Security Maturity Model

Capabilities of Key Solution Providers*

The existing Automotive Cyber security market is dominated by niche players and Chip Makers. The market is also witnessing rapid consolidation and M&A activities. However, current capabilities majorly focuses on four layers of security around CV-

ECU level firewall security, Hardware Security Module or cryptographic in-vehicle network security, External interface security through network access filters/remote security management and Safeguarding Over-the-Air updates and Vehicle to Cloud communication

	OTA & Cloud Security (V2C)	External Interface Security (V2X)	In-Vehicle Network Security	In-Vehicle ECU Protection	IoT Platform for App Development	
Argus Cyber Security Ltd. Israel	●	●	●	●	Unknown	Acquired by Continental AG in 2017
Arilou Technologies Ltd. Israel	Unknown	●	●	●	Unknown	Acquired by NNG Global services in 2016
Cisco Systems Inc. USA	●	●	●	Unknown	Unknown	Hyundai Partnering with CISCO
Covisint Corporation USA	●	Unknown	Unknown	Unknown	●	Hyundai BlueLink built on Covisint platform Acquired by OpenText
ESCRYPT Embedded Security Germany	●	●	●	●	Unknown	Volkswagen implemented CycurLIB in vehicles
Harman International Industries USA	●	●	●	●	●	Acquired by SAMSUNG
Infineon Technologies AG Germany	●	●	●	Unknown	Unknown	
Intel Security USA	Unknown	Unknown	Unknown	Unknown	Unknown	SoC Chip-based security
Secunet AG Germany	Unknown	●	●	Unknown	Unknown	
TowerSec USA	Unknown	●	●	●	Unknown	Acquired by HARMAN in Jan 2016
Trillium Inc. Japan	●	●	●	●	●	

* Based on publicly available information as of Jan 2018. This is not a recommendation for Product selection. Actual product offering and capabilities may vary based on proprietary information, continuous product enhancement / technological innovation or business strategy.

Conclusion

The advent of semi-autonomous, and gradually fully autonomous vehicle will create a complex ecosystem of vehicle communication, involving two-way data transfer between vehicle sensors, other vehicles, traffic infrastructure, cloud service providers up to Smart homes and Smart cities. Managing security the ecosystem will be a key subsystem.

The global automotive cyber security market is expected to grow at a CAGR of 13.2% between 2016-2021, to reach USD 31.8 Million.

Gartner predicts that by 2019, two automotive companies will be fined for vehicle software design negligence that results in inconsistent technology performance or Cyber-attacks. Network security and Communication Channels will be key areas to witness explosive growth. Disruptive technologies, such as big data, machine learning and AI can help build a better, safer and more secure CV ecosystem.

References

Cloud Security Alliance

https://cloudsecurityalliance.org/download/connected-vehicle-security/

Auto Information Sharing and Analysis Center

https://www.automotiveisac.com/best-practices/

Intel.com

https://www.intel.com/content/www/us/en/automotive/automotive-security-best-practices-white-paper.html

WIRED.com

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

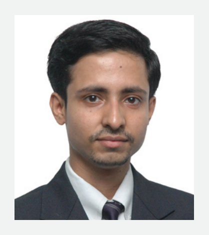
https://www.usatoday.com/story/tech/2017/07/28/chinese-group-hacks-tesla-second-year-row/518430001/

https://www.strategyand.pwc.com/reports/connected-car-2016-study

About the Authors

Sachin Kulkarni
Lead Consultant, Thought Partner Digital Consulting & Advisory, LTI

Sachin has over 20 years of experience across Manufacturing and Information Technology, and has been leading Strategic Consulting engagements, Global Transformation programs, establishing and operationalizing Automotive & Digital Consulting in addition to new client acquisition.



Manabendra Mukherjee
Senior Consultant, Digital Consulting & Advisory, LTI

Manabendra has over 13 years of experience across Manufacturing and Information Technology, and has been assisting clients in various transformation programs embrace Next-gen Digital Technologies, including IIoT, Robotic Automation, Cognitive Computing to drive productivity and business growth.