Enhancing Connected Car Adoption: Security and Over The Air Update Framework

Muzaffar Khurram
IBB Consulting Group
Philadelphia, USA
mkhurram@ibbconsulting.com

Hemanth Kumar, Adi Chandak , Varun Sarwade, Nitu Arora, Tony Quach
IBB Consulting Group
Philadelphia, USA

***Abstract*— a comprehensive security solution is no longer an option, and needs to be designed bottom-up into the car software. The architecture needs to be scalable and tiered, leveraging the proven technologies, processes and policies from the mature industries. The objective is to detect, defend and recover from any attack before harm comes to passengers, data and instrumentation. No matter how hardened security is there is always a need to patch any security vulnerabilities. This paper presents high level framework for security and over the air (OTA) framework.**

Keywords—Internet of things; hardware assisted security; smart over the air update system; connectivity architecture; electronic control unit

I. INTRODUCTION

The Automotive Sector will become an integral part of the digital world by 2020, when 75% of cars shipped globally are expected to have wireless connectivity [1]. OEMs and adjacent players will be challenged to offer new services and reform prevailingly long product life-cycles. The central risks to vehicular safety will no longer be limited to its physical security, but rather augmented by how we want the car to adapt to our progressive digital world.

The connected car is a logical application of the Internet of Things (IoT) that is beginning to redefine the consumer driving experience. As vehicular connectivity expands to include untrusted networks and automotive embedded systems become more open (figure 1), the stakes for digital security threats turn potentially life threatening. Furthermore, today's car is an evolution of patchwork systems that were never designed with cyber security in mind. Subsequently, how can this long-established industry that is going "online" through ad-hoc, untrusted networks catch-up to defend against modern cyber-attacks?

Fortunately, the automotive sector can make some fundamental adjustments without having to reinvent the "wheel" entirely. OEMs could leverage from other industries that are mature in their data security infrastructure and design security into the vehicle software architecture from the ground-up. The criticality is to protect the stored data and the data in motion that is associated with control units which can ultimately lead to a car's physical manipulation. Additionally, connected cars should be re-architected with modularized software and control units with Role Based Access Control (RBAC) and proactive measures for software updates and rapid fixes using an over-the-air (OTA) system.

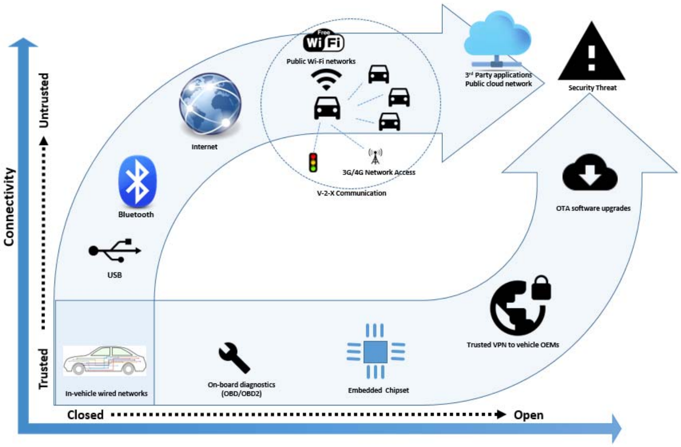

Fig 1: Evolution of connected car from trusted connectivity and closed systems to untrusted networks and open systems

II. MANAGED COMPONENTS IN CONNECTED CARS

The reality is, what's new about today's automobile developments are its computer systems. This "software device"/car contains around ten million lines of code, which is more than a mission critical fighter jet [2] and that is executed across 50 to 100 embedded computers [3] - electronic control units (ECUs). The ECUs are further connected to physical sensors and actuators handling different tasks, such as engine control, anti-spin system, and mirror adjustment (Figure 2).

Also, forthcoming to vehicular embedded system design is the integrated ECU, which eliminates the need for a distributed architecture [4]. The benefit is that the bill of material (BoM) can be reduced, as functionalities like window, door and seat controllers are consolidated onto a single hardware platform through employing virtualization schemes; automotive chipset vendors are offering hardware platforms optimized for integration, performance and cost. The potential downside to this integration is the removal of processors that once were isolated on their own sub networks and thus more secured.

Complementarily, OEMs are increasingly eliminating mechanical links between driver controls that operate the wheels or engine. Instead, they are transitioning to the fly-by-wire (FBW) concept, similar to the aircraft industry, where controls are converted to electronic signals transmitted by wires to operate the car - modern vehicles now accelerate by wire, change gears by wire, and even sometimes brake by wire. While all of these technologies improve the car's intelligence, environmental response, control and reliability, and reduce its weight and production costs, it also introduces vulnerability to security attacks.

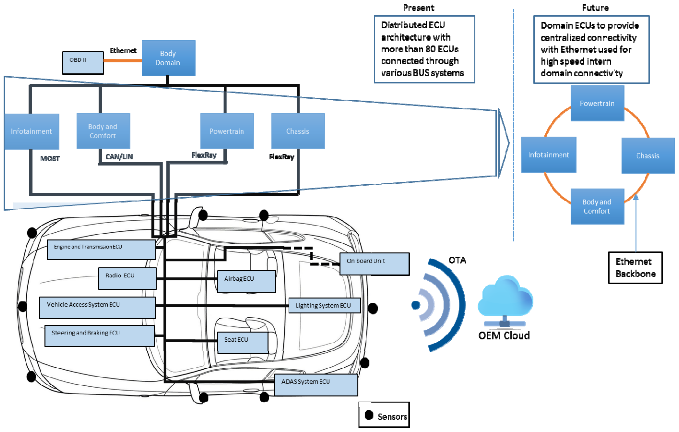

Fig 2: In-vehicle embedded system architecture

Adding to this vulnerability is the trend that a smart car's connectivity is no longer limited to trusted networks (Figure 3). As the car becomes more connected to the Internet, un-trusted networks, ad-hoc vehicle-to-vehicle and infrastructure networking (M2M), the level of security vulnerability increases to the threat of passenger safety. Recent security incidents show intrusions through the infotainment and control systems of the vehicle where hackers took over car systems through wireless connectivity. One of the more recent examples is the Nissan Leaf's system breach through its CarWings application that allowed hackers to control the heating and air conditioning. While this doesn't pose a significant safety risk, it could cause the battery to deplete and leave the driver stranded [5]. All of these threats warrant deploying security infrastructure that is robust, tiered and scalable to the new security challenges.

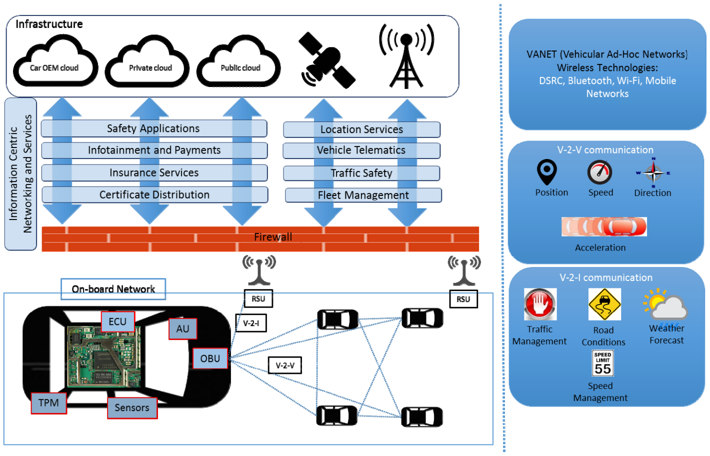

Fig 3: Connectivity architecture

III. THREAT ANALYSIS

As the car moves between trusted and untrusted networks, it's critical to analyze the threats and attacks it's vulnerable to and come up with a comprehensive security architecture plan. Figure 4 shows one of the ways to conceptualize threats based on different connectivity interfaces, distance and their potential impact level. In general, the threat impact increases as the distance from which an attack can be initiated. More vehicles will be impacted if a specific vulnerability can be targeted over the internet versus over Bluetooth or USB. Also severity of the threat increases many fold if the attack is targeted on the key functions of a car like brakes, accelerator, steering, etc. irrespective of the connectivity interface and distance.

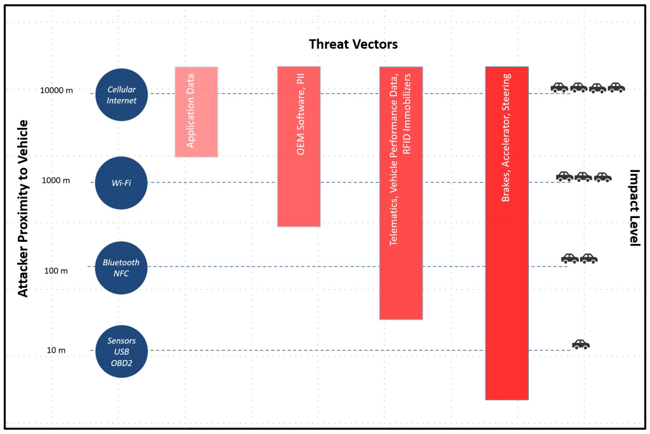

Fig 4: Threats across different interfaces and their impact level

Bluetooth technology is widely available in consumer devices. To provide better user experience car manufacturers are connecting apps on smartphones via Bluetooth, opening a pathway to allow access into the CAN and ECUs. However, architecture in the car needs to be robust enough to avoid becoming a getaway for hackers. One example of a high risk architecture is the 2014 Toyota Prius where the AM/FM/XM radio and Bluetooth are on the same network bus as steering, brakes and tire pressure monitoring system, potentially leaving the gates open for hackers [6].

The cyber risks with fixed Wi-Fi deployments have been well documented and it does not take a lot of imagination to translate some of those risks to a mobile environment. As two security researchers were able to easily hack into a Jeep Cherokee by easily guessing the Wi-Fi password [7]. Researchers were able to control the music player, set the radio station and control volume.

In the summer of 2015, Chrysler ended up recalling 1.4 million vehicles as the same two security researchers in the previous example were able to remotely hack into a Jeep Cherokee [8]. They used the infotainment system as the entry point to dashboard functions, steering, brakes and transmission using a laptop connected to Sprint's cellular network.

The above examples clearly illustrate potential vulnerabilities and threats that are inherent in a connected car ecosystem, where security cannot be an afterthought and a patch work.

Currently there exists aftermarket security devices like plug-in OBD-II devices. These devices scan all traffic in a vehicle's network identifying abnormal transmissions and enabling real-time response to threats. The OBD-II receiver can transmit data through embedded cellular features or via Bluetooth/Wi-Fi interaction using the driver's smartphone. Unless done in a secure manner, the OBD-II receivers 2-way communication with the internet on one hand and with a vehicle's CAN bus network on the other poses a significant security risk, potentially giving the hacker another access point to the car.

While these aftermarket solutions address the growing immediate need to address security concerns of existing connected car owners, however over the long term, what's needed is an integrated, end-to-end security architecture that is robust from both the hardware and software perspective.

IV. SECURITY ARCHITECTURE

Fundamentally, car data needs to be secured when stored and when transmitted throughout all system states: boot-up, idle, run-time and powering-down. When confidential data needs to be shared among entities, the following principal questions should be considered: 1) is the data accessed by only authorized entities? 2) Is the data tamper free? 3) Is the data available when needed?

In the face of the data security challenges, there are proven technologies from other industries that can be leveraged to model the connected car security architecture. Building on the successes from related industries such as Defense, Aerospace and Information Technology (IT), many of the core concepts, procedures, policies and lessons-learned from the threat analysis can be utilized in building a secure, connected car.

The connected car security solution needs to be robust, assisted by hardware and distributed within multiple layers of defense. These layers include hardware based protection for car embedded system, software based defenses for in-car services, security policy enforcement, network monitoring, data privacy and networked security services. The layered model relies on a modular approach of various technologies that is outlined in Figure 5:

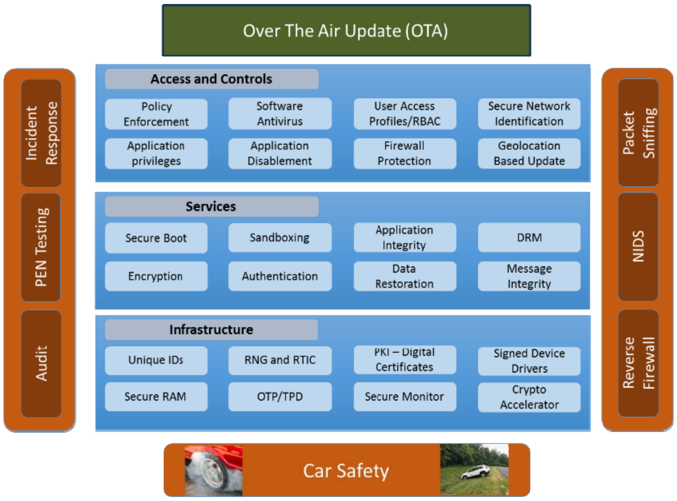

Fig 5. Scalable security architecture for the connected car

The car software architecture needs to incorporate security from the ground up, with special attention given to protecting the integrated car control and steering system. The safety of the car occupants cannot be assured without a well architected security solution that incorporates hardware isolation for critical blocks, OS-level virtualization and sandboxed application execution environment. These need to be designed-in with hardware assisted blocks and tighten integration into embedded system security infrastructure and enablers. Additionally, the modular car software design approach should isolate and limit security-attack damages and allow for quick fixes using OTA.

V. OTA AS AN ENABLER

OTA is about enabling the OEMs to remotely manage and upgrade the software on the car through various over-the-air (or wireless) interfaces such as Cellular, Wi-Fi and Bluetooth. OTA can be used for managing automotive firmware and software, such as core ECUs, navigation maps, infotainment, and telematics, as well as providing OEMs and car dealerships with significant cost savings.

The adoption of OTA in the car industry is growing in all major SW segments, as shown in figure 6. The worldwide total OEM cost savings from OTA software update events is forecasted to grow from $2.7 billion in 2015 (primarily from savings related to updating telematics systems) to more than $35 billion in 2022 (with telematics and infotainment system updates comprising most of the savings)

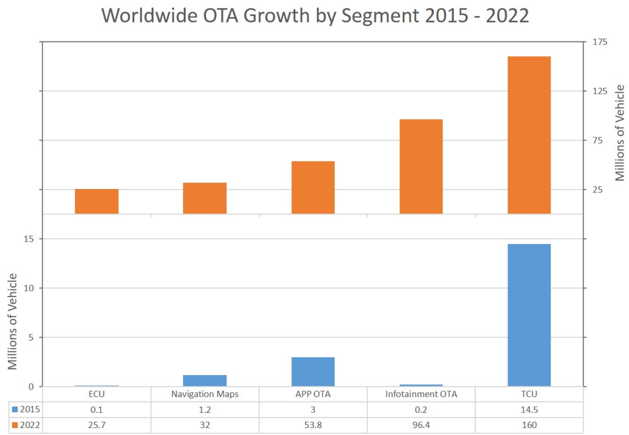

Fig.6 Worldwide OTA Growth by Segment 2015-2022

Looking ahead to predictions for 2016 and beyond [9], there are regulatory requirements outlined in the SPY Car Act of 2015 [10] which direct the National Highway Transportation Safety Board (NHTSB) to work with the Federal Trade Commission, creating cybersecurity guidelines for OEM manufacturers. As new rules and regulations are enacted, OEMs could use efficient, OTA based methods to update software in vehicles that are already in service. In additional several industry groups such as SWRI's Automotive Consortium for Embedded Security, the SAE Vehicle Electrical System Security Committee, the US Council for Automotive Research's (USCAR) Cyber/Physical Systems Task Force, and the Automotive Industry Information Sharing and Analysis Capability (ISAC) are focused are driving awareness and standardization. As the innovation cycle accelerates in areas like information/application sharing among vehicles and software defined vehicles become the platform for autonomous driving, secure OTA delivery mechanisms will become increasingly important to vehicle lifecycles.

One of the fundamental reasons for OEMs to pursue an OTA strategy is to address the growing software driven recalls, which analysts predict is as much as 50% of total recalls. Moreover, a robust OTA platform can fundamentally transform sales and customer retention models by enabling new revenue generation opportunities based on value added security offerings.

With a good OTA platform, OEMs have the flexibility of upgrading the ECU and other components remotely in an unobtrusive fashion. The OTA campaigns can be managed intelligently using rules engine to identify interdependencies and operational requirements e.g. time of day, car state, etc. Some of key considerations of a good OTA platform to support OTA for connected cars include:

- Robust client-server security architecture (beyond OMA-DM) that includes strong authentication, air-tight mechanism for protecting package integrity and authenticity and end-end encryption for data privacy

- Implementation of hardware assisted secure boot and run time tamper detection for core elements of OTA system e.g. OTA Manager and Update Installer

- Security hardened pre-installed, mobile and 3rd party apps by implementing various techniques such as code obfuscation, anti-debug, checksum, etc. to enhance protection against malware and dedicated attacks

- Network Discovery and Authentication: Secure SIM based authentication and seamless handovers between cellular and Wi-Fi networks using Access Network Discovery and Selection Function (ANDSF)

- Ability to update software at component level (e.g. ECU) and provision for strong mechanism for reversion to basic factory software in case of OTA update failure

- Delta generator: Dynamically compare two versions of the firmware and create a delta file to minimize network bandwidth utilization

- OTA Manager: OTA management to accurately track all client revisions on the road to determine the lifecycle of the software versions

- Reliable Transport: Reliably secure data transfer end-to-end with an inbuilt resilience-layer for handling network interruptions, no coverage areas and minimizing data retransmission

However robust a security architecture is, it may be vulnerable to security attacks that can put the car occupant’s life in danger. As the connected car industry matures, the key is to create a proactive system that can monitor for real-time threats and help OEMs mitigate the impact. It is paramount that the OTA system works in harmony with the real time scanning vulnerabilities detector, analytics, cloud and smart SW patch generator as shown in the Figure 7.

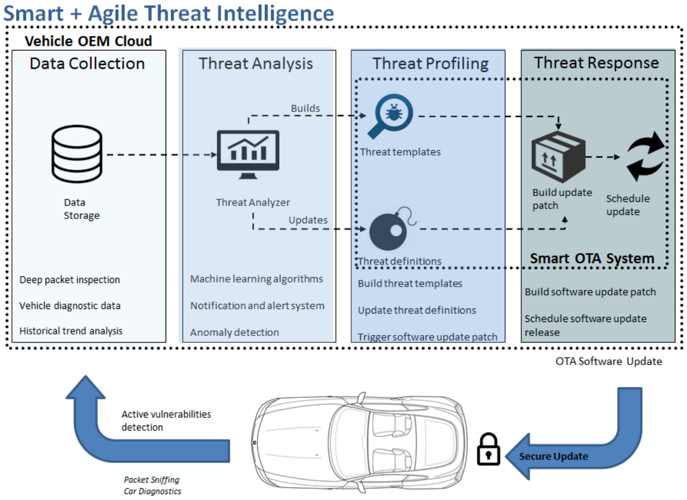

Fig.7 Smart and Agile Threat Intelligence System

The OEM cloud infrastructure should support the ability to perform active threat analysis and profiling using the bidirectional communication channel with the car. For all threats, the backend platform can create the threat definition, update threat templates profiles and a package that needs to be pushed to the car, securely. This smart OTA system works proactively to rapidly push updates to quarantine, isolating the attacked module and providing fixes to close backdoors for future vulnerabilities.

VI. CONCLUSION

The ideal connected driving experience not only parlays infotainment services of other device forms, but also provides occupant safety and convenience through its native digital services. As OEMs adopt the digital economy, it is imperative to re-architect core automotive systems with cyber security built into its safety model to be as critically basic as having good brakes. Most importantly, the industry should collectively progress into the digital world in order to establish an ecosystem that can proactively guard against emerging cyber-attacks. This robust security design needs to include smart OTA capabilities that work collaboratively in an environment with intelligent threat-addressing systems to ensure occupant safety while also providing vehicular serviceability.

REFERENCES

[1] Greenough, John. "THE CONNECTED CAR REPORT: Forecasts, Competing Technologies, and Leading Manufacturers." Business Insider. Business Insider, Inc, 07 Jan. 2016. Web. 29 Apr. 2016. <http://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2015-3>.

[2] Doll, Greg. "The Connected Car: It's All about Integration." Embedded Computing Design. N.p., n.d. Web. 29 Apr. 2016. <http://embedded-computing.com/articles/the-car-its-about-integration/>.

[3] KLEBERGER, PIERRE. "A Structured Approach to Securing the Connected Car." A Structured Approach to Securing the Connected Car (2012): n. pag. Web. 29 Apr. 2016. <http://publications.lib.chalmers.se/records/fulltext/168507/168507.pdf>

[4] "Overview - ECU Consolidation." Redbend. N.p., n.d. Web. 29 Apr. 2016.<http://www.redbend.com/en/solutions/automotive/ecu-consolidation/overview>.

[5] Kelion, Leo. "Nissan Leaf Electric Cars Hack Vulnerability Disclosed." BBC News. N.p., 24 Feb. 2016. Web. 29 Apr. 2016. <http://www.bbc.com/news/technology-35642749>

[6] "How Hackers Could Slam on Your Car's Brakes." CNNMoney. Cable News Network, 1 Aug. 2014. Web. 29 Apr.2016. <http://money.cnn.com/2014/08/01/technology/security/most-hackable-cars/>

[7] "Black Hat USA 2015: The Full Story of How That Jeep Was Hacked." N.p., n.d. Web. 29 Apr. 2016. <https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/>.

[8] Greenberg, Andy. "Hackers Remotely Kill a Jeep on the Highway-With Me in It." Wired.com. Conde Nast Digital, 21 July 2015. Web. 29 Apr. 2016. <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>.

[9] Alam, Mahbubul. "More Algorithms, Vehicle Security to Come in 2016 - CCE Blog." Connected Car Expo RSS. N.p., 04 Jan. 2016. Web. 10 May 2016. <http://connectedcarexpo.com/auto-tech-forecast-2016-vehicle-security-algorithm/>.

[10] S. MDM15C25, 114th Cong., https://www.markey.senate.gov/imo/media/doc/SPY%20Car%20legislation.pdf 1 (2015) (enacted). Print. ‘‘SPY Car Act of 2015’’