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

PREPARED BY:
Muzaffar Khurram, Hemanth Kumar, Adi Chandak,
Varun Sarwade, Nitu Arora, Tony Quach
IBB Consulting Group
Philadelphia, August 22, 2016

Executive Summary:

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 prevailing long product lifecycles. 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 open1, 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. The imperative is to redevelop quickly through expert adoption and mature collaboratively. OEMs could leverage from other industries that are mature in its data security infrastructure and design security into the vehicle software architecture from the ground-up. The criticality is to protect the data path between access points and control units that can ultimately lead to a car’s physical manipulation. Additionally, connected cars should be re-architected with hardware-assisted hardened execution environments; modularized software and control units with privileged access-control; and proactive measures for software updates and rapid fixes using a ‘smart’ over-the-air (OTA) system.

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

Conclusion

The ideal connected driving experience not only parleys 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


The authors appreciate your review of the executive summary. We look forward to your comments, views and further ideas on the IBB LinkedIn forum, on the security and OTA framework for connected car to evolve the solution to push its wider adoption.

The full white paper is accepted for publication by “The 5th International Conference on Connected Vehicles & Expo (ICCVE 2016)” to be held in Seattle WA, from Sept. 12-16 2016. For further details please contact:

Muzaffar Khurram mkhurram@ibbconsulting.com