2017 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
VEHICLE ELECTRONICS AND ARCHITECTURE (VEA) TECHNICAL SESSION
AUGUST 8-10, 2017 - NOVI, MICHIGAN

SMART VEHICLES, AUTOMOTIVE CYBER SECURITY & SOFTWARE SAFETY APPLIED TO LEADER-FOLLOWER (LF) AND AUTONOMOUS CONVOY OPERATIONS (ACO)

Sumeet Chhawri
FEV North America
Auburn Hills, MI

Stephan Tarnutzer
FEV North America
Auburn Hills, MI

Thomas Tasky,
FEV North America
Auburn Hills, MI

Gerald R. Lane
Great Lakes Systems & Technology LLC
Chesterfield Twp., MI

ABSTRACT

FEV North America will discuss application of advanced automotive cybersecurity to smart vehicle projects, - software safety - software architecture and how it applies to similar features and capabilities across the fleet of DoD combat and tactical vehicles. The analogous system architectures of automotive and military vehicles with advanced architectures, distributed electronic control units, connectivity to networks, user interfaces and maintenance networks and interface points clearly open an opportunity for DoD to leverage the technology techniques, hardware, software, management and human resources to drive implementation costs down while implementing fleet modifications, infrastructure methodology and many of the features of the automotive cyber security spectrum.

Two of the primary automotive and DoD subsystems most relevant to Cyber Security threat and protection are the automotive connected vehicles analogous to the DoD Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) systems; and the extensive employed automotive CanBus parallels the DoD GV electrical power; intra-vehicle networks; data processing; and electrical components. These DoD subsystems can gain many Cyber benefits to achieve at minimum cost and schedule to desired examples of Cross-domain guards, Security Infrastructure, Security applications, Vehicle authentication and authorization, Secure networks, and Vehicle cyber security threats.

INTRODUCTION

Information and Communication Technology (ICT) is a key driver for the advancements and enabler of connectivity and Autonomy in vehicles. This has led to the development of connected vehicles utilizing cellular, Wi-Fi, and Bluetooth as transport mediums and platforms such as Android Auto, proprietary automotive platforms such as Sync (from Ford), UConnect (from FCA) and OnStar (from GM) to name a few. This also leads to security vulnerabilities as showcased by researchers. Vulnerabilities in Subaru were revealed recently (1), similarly vulnerabilities in Tesla and Jeep were presented in reference (2), and (3) respectively. The publication from Miller and Valasek (4) describes the landscape attack vectors and demonstrates attack on an unaltered vehicle from a cellular interface. Vulnerabilities such as these are evidence that security has to become a de-facto standard integrated within the development of automotive systems. In the following sections we proceed to elaborate on the cyber security landscape of modern and future automotive technologies identifying challenges, attack vectors

and vehicle architecture. Then we discuss in detail the approaches taken by FEV to address these challenges.

CYBER SECURITY LANDSCAPE

A modern vehicle with connectivity and advanced safety functionalities has more than 50 attack surfaces. The following figure (Figure 1) shows the interfaces of a modern vehicle.

Security and safety concerns become evident with enablers of connectivity and autonomy. Security should support enablement of these platforms within automotive and hence our approach provides a comprehensive security solution by strengthening security through the complete product life-cycle. FEV provides engineering services through-out the product development life-cycle as shown in figure (Figure-2). The attack surface originated from connectivity can be categorized in broad vectors of low range (Bluetooth, Wi-Fi etc.), long range (4G LTE, 5G, DSRC – Dedicated Short Range Communication) and physical access (OBD II – Updated On-Board Diagnostics standard effective in cars sold in the US after 1-1-96, ECUs – Electronic Control Units, USB etc.). The approach to secure the complex intricacies of communication, hardware and software to enable connectivity and autonomy are discussed in the following sections.

CYBER SECURITY APPROACH

Our approach comprises of three primary verticals. These are as follows:

a. Risk and Threat Assessment
b. Hardware and Software security and
c. Cyber security testing.

Risk and threat assessment is the first step towards identifying high risk threats to the system under investigation. Non-automotive industry standards

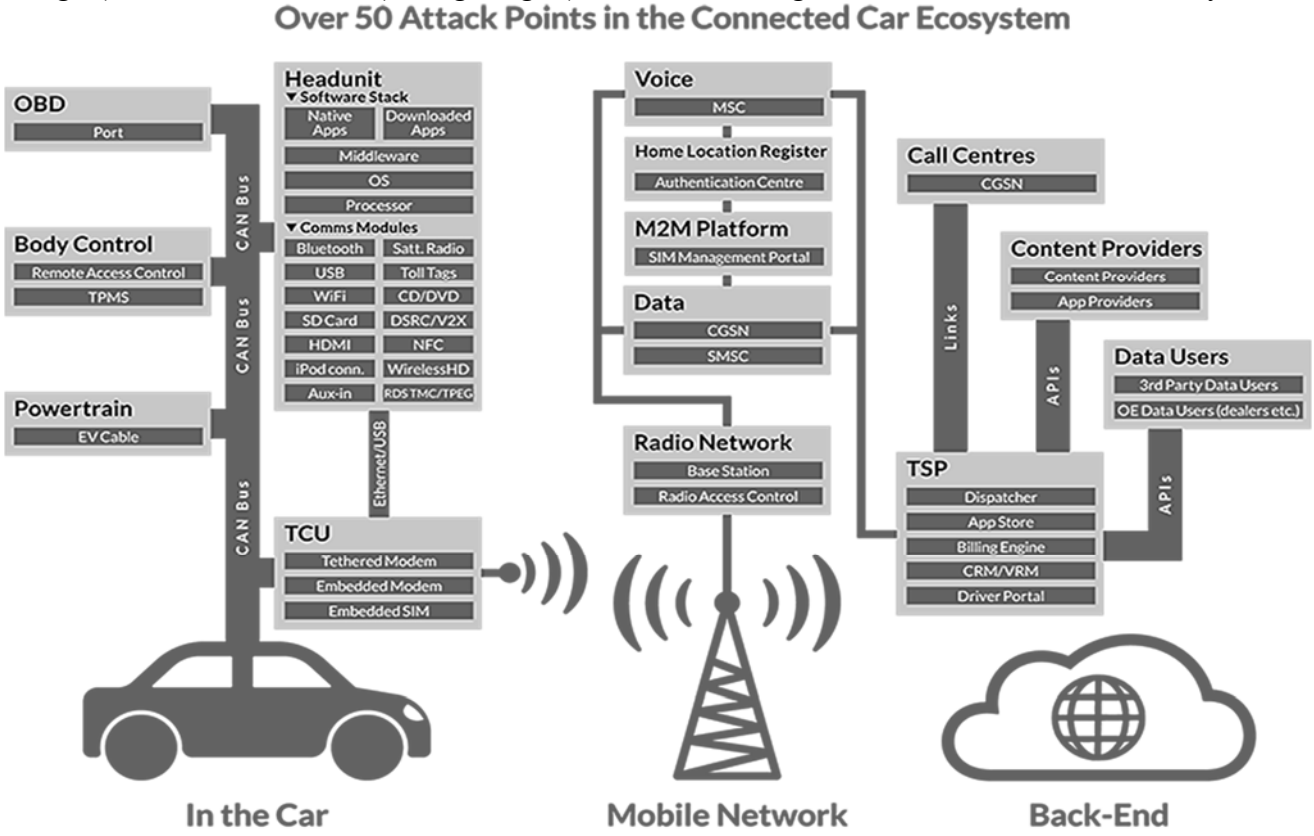

Figure 1: Attack vectors of modern automotive eco-system

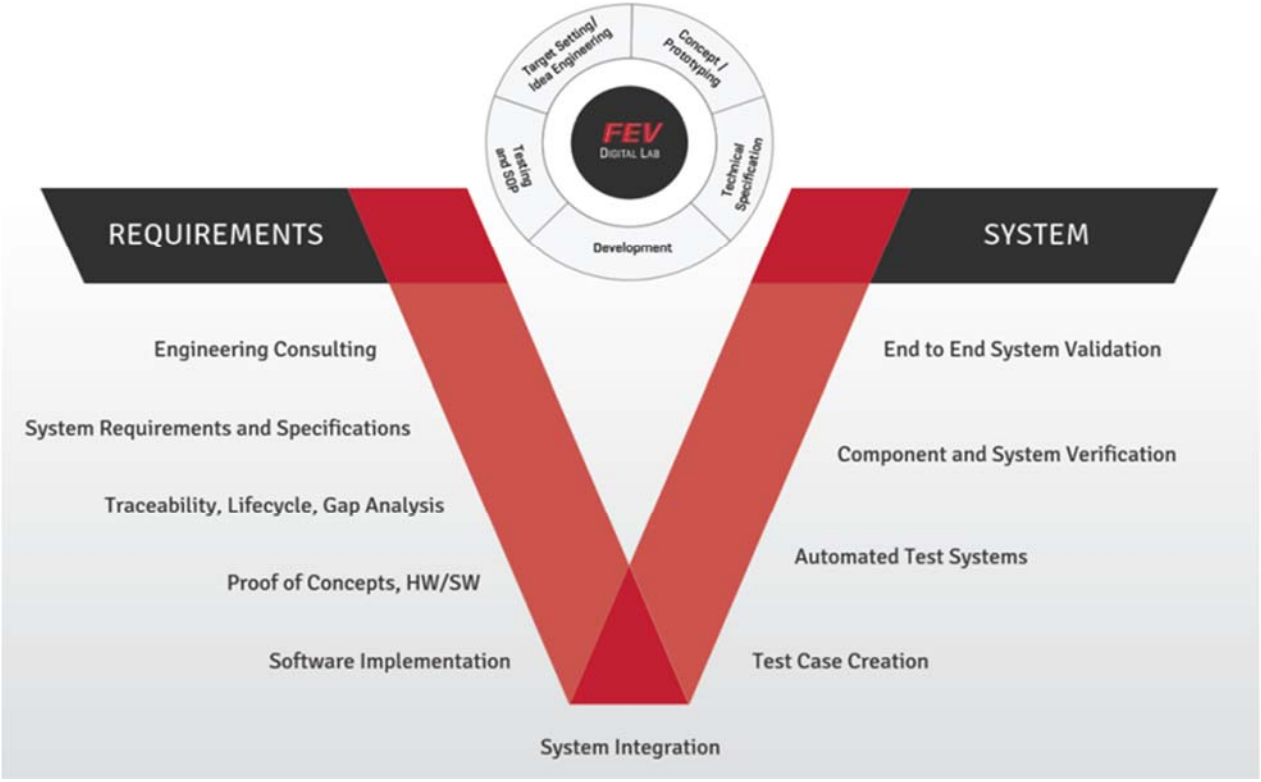

Figure 2: Development Life-Cycle

for Risk and Threat Assessment can be leveraged to provide a hybrid approach to streamline the vast number of threats emerging from the connected and autonomous automotive eco-system. These include and not limited to NIST RMF (5), and ICS-CERT (6). The automotive industry published the SAE J3061 (7) guidelines which provides an overview of the cyber security landscape within the automotive domain. EVITA (8) and HEAVENS provide a direction towards performing risk and threat assessment. NHTSA incorporated the NIST RMF in the automotive use-case and published the results (5).

From the above mentioned standards and guidelines FEV has developed a risk and threat assessment approach to address the requirements of the automotive industry and incorporating non-automotive best practices.

This approach includes assessment of the vehicle architecture analyzing individual components and functioning at a system level. Developing attack scenarios constituting worst case scenarios or dark side scenarios to assess motivation, attack vectors, and capabilities of attackers. This includes assessment of key attributes such as types of tools available, expertise level of attacker, financial support that might be available to a certain group of attack actors. From a system standpoint, we also analyze the capability of the system itself to withstand such attacks. This includes analysis of attributes of for e.g. access to system (physical or remote), expertise level and resources required to penetrate the system.

Attack actors are systematically categorized into “Organized and well financed attackers”, “Individual attackers”, “Amateurs” and “Insiders”. Organized and well financed attackers include Nation states actors from governments, defense and intelligence organizations, industrial organizations and companies, Hacktivists (non-state) with

Figure 1: Active attack vectors on modern vehicles

political targets of opportunity, and mass disruption. Individual hackers including white hat and black hat hackers with varied motivations of financial, privacy, theft etc. Amateurs, also termed as script kiddies may use existing tools to perform attacks on privacy or financial related. Insiders which include disgruntled employees, or event unintended attacks. An attack actor category is leveraged based on specific domain requirements.

With this analysis our approach provides us with a custom requirements based risk matrix that represents Impact and Likelihood of an attack scenario described above (including the attack vector).

AUTOMOTIVE LEVELS AND SECURITY LAYERS

FEV provides security at various levels of the automotive eco-system. A depiction of the levels of automotive architecture is shown in figure (Figure 3). The architecture is a general overview of the communication, hardware and software components of an automotive system. Level 1 defines the security solutions required at the external interfaces of the automotive eco-system. This includes connectivity enablers such as cellular, WiFi, Bluetooth, and V2X (Vehicle to X, where X can be Vehicle or Infrastructure or Pedestrian) communication which requires security in the form of firewall, secure communication, and the host controllers which integrate these technologies to have secure elements at both hardware and software components.

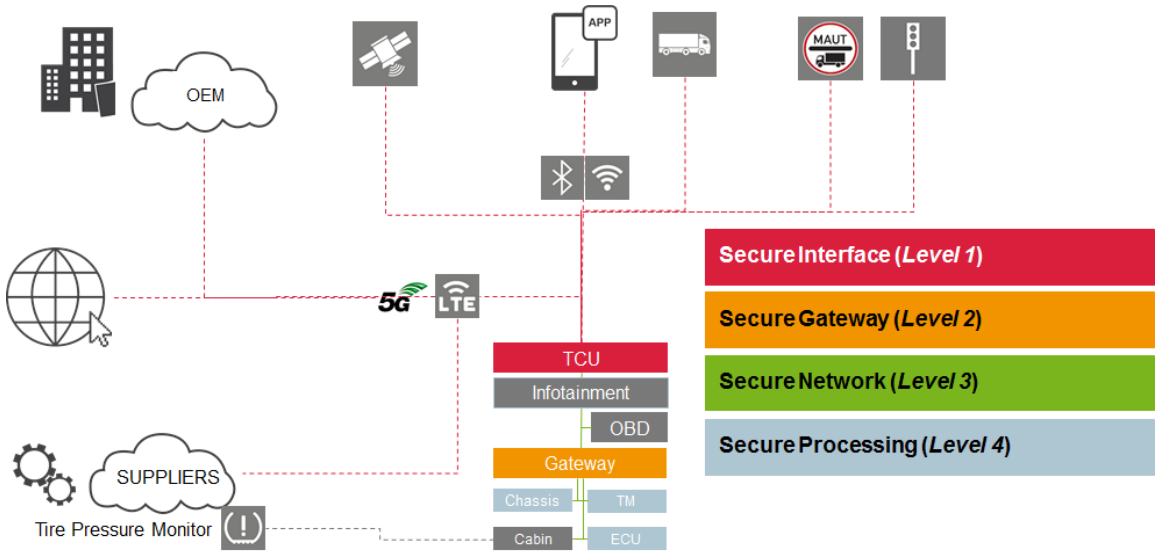

Figure 3: Layered security solution based on automotive levels

Level 2 defines the security solutions recommended at the interface between the external environment and the vehicle internal in-vehicle network system. We provide a solution that enables a secure architecture through the utilization of a Security Gateway that enables a CAN based firewall, Intrusion Detection System (IDS), and a traditional vehicle gateway. The firewall provides security to the safety functions that reside within the in-vehicle network and are not allowed to penetrate from the external domain.

Level 3 provides security to the in-vehicle communication mechanism which can be securing communication over CAN, CAN-FD or automotive Ethernet.

Level 4 requires an integration of hardware supported secure execution environment for each ECU participating in the vehicle functioning. These

hardware supported secure execution elements include Hardware Security Modules (HSM), or Trusted Platform Modules (TPMs) to name a few. Level 4 also includes providing integrity to the software running on the ECU. This is supported by our partner Karamba Security where we have integrated this software solution to provide ECU Integrity.

DESIGN AND DEVELOPMENT

The layers of security solutions for communication, hardware and software mentioned above with regards to automotive architecture levels are described in further detail in this section.

Gateway:

- The security gateway at level 2 is an interface security solution functioning to prohibit unauthorized communication CAN (controller area network) bus from the direction of level 1 i.e. communication from level 1 interfaces towards ascending levels must be authorized and secure and vice-versa.
- FEV's security gateway prohibits unauthorized CAN messages from penetrating the system from unintended communication directions. This is accomplished by developing state-full packet analyzers, access control (read and write capability), and attack profile based algorithms (replay, Denial of Service etc.).
- The security gateway is designed as a hardware software module with a versatile architecture integration. The gateway can be integrated as a standalone hardware software module between the OBD II and in-vehicle network or can be integrated between the infotainment (TCU in this case) and the in-vehicle network. It can also be modularized to be integrated as a software only solution as part of existing gateway systems.

Secure elements:

- Secure elements are hardware supported secure execution environments that allow system designers to segregate critical security parameters such as private keys, unique identification in separate hardware modules. This minimizes the risk of software based attacks to retrieve security keys.
- Trusted Platform Modules (TPM), is a secure execution environment specification published by Trusted Computing Group and the main specification can be reference here: (9).
- Similarly HSM (EVITA standards) and SHE (Secure Hardware Execution) based standards for secure execution are published by respective organization/groups.
- These modules are to be integrated at different levels of the automotive system. Such as the high performance TPM's can be integrated at the infotainment/TCU level. Whereas the dedicated secure elements such as HSM (different profiles) and SHE can be integrated at automotive ECU levels.
- FEV has integrated TPM's with FEV modules which provide the following security functions:
    - Root of trust
    - Secure remote attestations
    - Secure boot, verified and measured boot.
    - And secure device identity.

Software Solutions:

A. Secure software development:

- Best practices for secure software development needs to be adhered to towards developing automotive systems.
- Secure coding standards from CERT C (10) and MISRA C Secure (11) must be followed.
- Multiple tools are available both open source and commercial to addressing adherence to

the above standards. For e.g. PRQA, LDRA etc.

B. Software security solutions:

One of the solutions that FEV has demonstrated with collaboration with Karamba Security is to provide ECU integrity solutions by:

- Automatic Policy Generation, Factory settings based policy (Automatic hashing of all binaries and Automatic creation – part of build server.
- This will provide security from altered payloads and tampering of existing binaries on ECUs.

- Detect and Prevent -Any foreign code:
  - Prevent In-Memory Attacks, Factory settings based policy (Automatically generated functions' calling graph & Return address mapping).
  - This will protect ECU firmware from zero-day vulnerabilities that may exist on already installed applications.

Security Testing:

- The lack of standards in the domain of automotive security testing places challenges in the development of a comprehensive test process.
- FEV has leveraged knowledge from FEV's connected vehicle and testing practice to develop risk and functional security test systems for automotive systems which allow us to automate security related testing.
- Based on the risk assessment and threat modeling process described above, test cases are developed.
- These test cases are then evaluated and automated using LabView.

CONCLUSION

Department of Defense (DoD) applications requiring on a higher threshold of security will benefit by adopting the processes and solutions mentioned in the article.

- An architecture review of levels will provide initiation of risk assessment.
- Leveraging the results of risk assessment will allow the stakeholders to set a baseline security threshold goals.
- These goals will define the solutions required to be integrated into components at various levels of the target system.
- Automated testing will provide a recursive testing methodology to automate already identified vulnerabilities.

The above process will meet a comprehensive end-to-end security approach to strengthen the safety and security of the target systems.

REFERENCES

1. **Abel, Robert.** SC Network Security. *scmagazine.* [Online] https://www.scmagazine.com/researcher-hacks-subaru-wrx-sti-starlink/article/666460/.

2. **Peterson, Andrea.** The Washington Post. *washingtonpost.com.* [Online] https://www.washingtonpost.com/news/the-switch/wp/2016/09/20/researchers-remotely-hack-tesla-model-s/?utm_term=.3b939c6cc8f7.

3. **Greenberg, Andy.** wired. *wired.com.* [Online] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

4. **Miller, Dr. Charlie and Valasek, Chris.** illmatics. *illmatics.com.* [Online] http://illmatics.com/Remote%20Car%20Hacking.pdf.

5. **McCarthy, C., Harnett, K., & Carter, A.** *Characterization of potential security threats in modern automobiles: A composite modeling approach.* Washington, DC : National Highway Traffic Safety Administration, 2014.

6. **ICS-CERT. *ics-cert.us-cert.gov.* [Online] https://ics-cert.us-cert.gov/.**

7. SAE J3061 Surface Vehicle Recommended Practice. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.* s.l. : SAE International, 2016.

8. Ruddle, Alastair and Ward, David. *EVITA Project Deliverable D2.3: "Security requirements for automotive on-board networks based on dark-side scenarios".* 2009.

9. Group, Trusted Computing. TPM Main Specification. *trustedcomputinggroup.org.* [Online]

https://trustedcomputinggroup.org/tpm-main-specification/.

10. SEI CERT. SEI CERT C Coding Standard. ***www.securecoding.cert.org.*** **[Online] https://www.securecoding.cert.org/confluence/display/c/SEI+CERT+C+Coding+Standard.**

11. MISRA C. ***MISRA C:2012 – Addendum 2 Coverage of MISRA C:2012 against ISO/IEC TS 17961:2013 "C Secure".*** **2016.**

12. SAE International. ***Surface vehicle recommended practice Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.*** **s.l. : SAE International, 2016.**

13. D2.1, EVITA deliverable. ***Specification and evaluation of e-security relevant use cases.*** **2009.**

14. Ruddle, Alastair, et al. ***Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios.*** **2009.**

15. Alastair Ruddle, David Ward, Benjamin Weyl, Sabir Idrees, Yves Roudier, Michael Friedewald, Timo Leimb, Andreas Fuchs, Sigrid Gürgens, Olaf Henniger, Roland Rieke, Matthias Ritscher, Henrik Broberg, Ludovic Apvrille, Renaud Pacalet, Gabriel Pedroza. ***Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios.*** **s.l. : EVITA, 2009.**

16. Microsoft Corporation. The STRIDE Threat Model. ***microsoft.*** **[Online] 2005. [Cited: 09 29, 2016.] https://msdn.microsoft.com/library/ms954176.aspx.**

.