2019 NDIA GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM
GROUND SYSTEMS CYBER ENGINEERING TECHNICAL SESSION
AUGUST 13-15, 2019 - NOVI, MICHIGAN

Secure Connected Vehicle Architecture for Software and Telecommunications

Scott J. McCormick[1],
Elaina Farnsworth[2]

[1]Connected Vehicle Trade Association, Inc. East Lansing, Mi
[2]The Next Education, Pontiac, MI

ABSTRACT

The advent of both new bidirectional communications capabilities and increasing levels of automation to offload driver workload is requiring the vehicle's architecture to evolve substantially. Military vehicles of the US Armed Forces are subject to even greater cybersecurity threats. New vehicle hardware includes many sensors, cameras and other systems to capture road, weather and traffic conditions. These systems will be communicating the data both internally and externally from the vehicle. In addition, the vehicles will send and receive data via multiple communications protocols. Each of these communication protocols have unique capabilities and inherent weaknesses with regard to secure communications. With this vehicle evolution, and with the pervasive cyber threats, the vehicle will have to be architected for holistic vehicle cyber situational awareness. The US Army and US Marine Corps need to be fully versed and trained to recognize threats and effectively deal with them. In addition, satellite, cellular and WiFi systems not only communicate to and from the vehicle, but to the equipment installed for specific military purposes, as well as to the warfighter's nomadic, or carried-in devices such cellphones, tablets, laptops and others.

INTRODUCTION

At this point in time, recognizing the evolving nature of security, there are three primary components of Connected Vehicle Security:

- The CANbus networks that carry all the vehicle operational signals (e.g. braking systems, cruise control, steer by wire) amongst the many computing elements in modern vehicles. This discussion will focus on how these networks and nodes are being secured by OEMs and being enhanced with NHTSA's CYBER Program.
- The In-Vehicle Infotainment (IVI) systems now carry video and voice, and will be the repository of apps, personal data and content, including cellular connectivity via tethered phone apps, and connected services. These IVI systems present a significant security risk if proper firewalls are not designed into the system architecture.
- The Communication Link between the vehicle and the outside world. This discussion largely has focused on how to secure DSRC and other communication protocols, which needs to be closed comprehensively in order to ensure the solution is robust and scales nationwide in a wide variety of traffic conditions. The advent of 5G for vehicle safety messages and autonomy is just now being explored.

Over time we are likely to encounter additional security challenges. For example, as the vehicle electrical architecture evolves, computing might be instituted in distributed nodes as the compute demands of the vehicle increases with advanced driver assist and unmanned vehicle driving capabilities. This re-architecting would bring about additional challenges, but also opportunities to introduce new levels of security and/or distributed storage of personal data that is of sensitive, operational safety or mission critical nature.

1. ADDRESSING SECURITY

Threats exist to identity, confidentiality, data and application integrity, intrusion for malicious intent, and disrupting continuity of service. In-vehicle software can have up to 100 million lines of code which executes on both the primary computer board(s) and 70-100 microprocessor-based electronic control units (ECUs) networked throughout the body of the car. With each level of autonomy the car evolves through, we may add an additional 100 million lines of code. Threats exist from both bad programming and the inability to test all possible software interactions.

A large number of vehicles communicating to each other is essentially an ad-hoc, self-forming network of devices with no server-side security. As vehicle communications are new to automakers, understanding and protecting the systems are a major, ongoing

priority. As with computers, as the vehicle ages, new threats will surface. Opening any communication gateway incurs risk of data corruption, loss and system failure from malicious intent.

There are up to 15 different frequencies and wireless services on today's cars: AM/FM, TV, Digital Audio Broadcasting, Remote Keyless Entry, Tire Pressure Monitoring, cellular phone, WiFi, satellite navigation (GPS) and satellite radio, Bluetooth, DSRC and Radar. These systems operate on many different frequencies: 1 MHz, 100 MHz, 315 –2100 MHz, 1.575 GHz, 2.3 and 2.4 GHZ, 5.9 GHz, 24 and 77 GHz. As more access is provided to wirelessly send and receive road, weather and traffic information, as well as infotainment content, more risk is incurred.

2. AREAS OF SIGNIFICANT RISK FOR CYBERSECURITY BREACH

The four primary cybersecurity breach areas at risk for vehicles are:

- Secure Boot -Works with the hardware to ensure that the loaded software components are valid to provide a root of trust for the rest of the system.
- Hardware Security -Secure boot and software attestation functions: Detects tampering with boot loaders and critical operating system files by checking their digital signatures and product keys.
- Network Security -Message authentication: Verifies that communications are coming from the approved source and defenses to protect authentications from being spoofed or recorded and replayed.
- Cloud Security -Secure authenticated channel to the cloud: Leverages hardware-assisted cryptography for remote monitoring, software updates, and other communications.

3. WARFIGHTER-SPECIFIC COMMUNICATION THREATS

While the vehicles have specific cybersecurity threats, the environment is complicated by the non-embedded components installed into vehicles, as well as the nomadic devices (phones, radios, tablets, laptops, etc.) carried into the vehicle. All elements, the warfighter, the vehicle and the command structure must have a highly secure battlefield network for enhanced communications and situational awareness. Technology advances have revolutionized military communications, vastly increasing connectivity requirements for every vehicle, sensor and soldier, whether on land, sea or air. The macro trend to connect everything is evident even on the battlefield, where every "thing," including soldiers, can be sensors for maneuver command, control, communications and intelligence. Like any

modern communications system, ubiquitous mobile coverage for the military relies on networks, bandwidth, availability and security.

This network-centric approach to make troops smarter and quicker in battlefield situations imposes rigorous security, performance and reliability challenges.

However, wireless communications on the battlefield are becoming safer and more secure, thanks to advances in embedded computing technology.

Modern low power, mid-range density systems, for example, can enable software-defined radio and cryptography in military handheld radios for secure communications, as well as IEEE 1588 support and signal processing.

With regards to satellite communications, Douglas Loverro Former Deputy Assistant Secretary of Defense for Space Policy has stated that *"Cyberattack against a variety of communications networks is a difficult challenge. But the far simpler thing that Russia can do, that North Korea can do, That Iran can do, that Botswana can do, that some guy in the middle of a field with a TV truck can do…is jamming. Jamming is very hard to protect against, unless you have the right equipment."*

Today's commercially-available High Throughput Satellites (HTS) utilize steerable spot beams that provide incredible throughput, but cover smaller areas. Some of these satellites are currently operating in MEO orbits, meaning they combine high throughput with low latency, and are naturally more prolific and harder to jam. By embracing these commercial HTS and MEO satellite constellations, the military can essential get anti-jamming capabilities baked in.

Wireless communications are considered less secure than wired or fiber-based systems because the data is transmitted over the radio channel making it more susceptible to eavesdropping and interception. Thus, security needs special attention. Confidentiality, integrity and availability are the objectives of security solutions. Attacks such as Man-in-the-Middle, replay, and Denial-of-Service can be mitigated or eliminated. Data disclosure to unauthorized people, user identity and location disclosure, impersonation of a valid user, user tracking and subscriber capabilities disclosure are a few of the potential risks that can lead to a mission failure and even cost people's lives. Their security vulnerabilities and the potential attack vectors are analyzed. There are a number of protocols and techniques that address or mitigate the security deficiencies and the way they enforce security.

Aside from the carrier vulnerabilities, smart phone and tablet apps will give troops the ability to perform control, analysis and other sophisticated tasks

anytime, anywhere, while allowing commanders to instantly distribute essential documents directly to troops.

Network and device security concerns have so far hindered widespread smart phone deployment. A new hardened kernel for Android 3.0 devices developed by the National Security Agency (NSA) and George Mason University researchers, currently under certification evaluation by the NSA in 2012 resolved basic concerns on non-classified official networks.

The Joint Tactical Radio System (JTRS) aimed to replace existing radios in the American military with a single set of software-defined radios that could have new frequencies and modes ("waveforms") added via upload, instead of requiring multiple radio types in ground vehicles, and using circuit board swaps in order to upgrade.

Software-defined radio (SDR) is a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/ demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible.

A basic SDR system may consist of a personal computer equipped with a sound card, or other analog-to-digital converter, preceded by some form of RF front end. Significant amounts of signal processing are handed over to the general-purpose processor, rather than being done in special-purpose hardware (electronic circuits). Such a design produces a radio which can receive and transmit widely different radio protocols (sometimes referred to as waveforms) based solely on the software used.

Software radios have significant utility for the military and cell phone services, both of which must serve a wide variety of changing radio protocols in real time.

Ground mobile radios utilize two basic network approaches: the Soldier Radio Waveform (SRW) and the Wideband Networking Waveform. The combined technologies allow secure networked communications among platoon, squad and team-level soldiers, as well as satellite connections back to combat commanders.

The Joint Tactical Radio System (JTRS) evolved from a loosely associated group of radio replacement programs to an integrated effort to network multiple weapon system platforms and forward combat units where it matters most – at the last tactical mile. In 2005, JTRS was restructured under the leadership of a Joint Program Executive Officer (JPEO) headquartered in San Diego, California

A three-year contract was awarded by the National Spectrum Consortium in 2017 to develop a new narrowband mode of the Soldier Radio Waveform (SRW) for the U.S. Department of Defense, and results are expected in 2020.

The new narrowband mode will decrease the amount of spectrum required when deploying an Infantry Brigade Combat Team. This will help extend the warfighter's point-to-point communications range, enabling reliable voice and data communications transmission over varying terrain.

Warfighters today use wideband SRW to transmit higher bandwidth information, such as video and images, over shorter point-to-point distances. The narrowband mode of SRW will extend point-to-point ranges, provide electronic counter-countermeasures, and enhance network scalability. This will allow more users – including other U.S. services and coalition partners – on the network without degrading reliability or performance.

Today's cryptography is very complex, mathematical, and can be virtually unbreakable if implemented properly. This is why the Federal Government and DoD community apply a cryptography standard known as FIPS 140-2 to their IT systems. National Institute of Standards & Technology (NIST) created Federal Information Processing Standard (FIPS) 140-2 – Security Requirements for Cryptographic Modules. FIPS publications are mandatory for Federal Government agencies as required by FISMA law passed in 2002. FIPS 140-2 covers the design, development, and implementation of cryptographic modules, and underlying algorithms, in hardware or software. So what exactly is a cryptographic module? According to FIPS 140-2[a] a crypto module can be hardware, software, firmware, or a combination of the three that implements some form of cryptographic function (encryption, hashing, message authentication, or key management). The Advanced Encryption Standard (AES), also known by its original name Rijndael, is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.

For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES has been adopted by the U.S. government and is now used worldwide.

The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decryption of data. A brute force attack against AES encrypted documents or drives would take years even using numerous super computers.

4. SECURITY STANDARDS

The automotive industry has developed two important bodies of work to address vehicle security. The SAE J3101 standard is Hardware-Protected Security for Ground Vehicle Applications. This standard addresses Secure Boot, Secure Storage, Secure Execution Environment, other hardware capabilities and Over the Air (OTA) authentication, detection, and recovery mechanisms.

SAE J3061 is the Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. This document enumerates all attack surfaces and describes how to conduct threat analysis, reduce attack surfaces, methods to harden hardware and software and Security Testing (Penetration, fuzzing, etc.).

ISO 26262, titled "Road vehicles – Functional safety", is an international standard for functional safety of electrical and/or electronic systems in production automobiles defined by the International Organization for Standardization (ISO) in 2011.

ISO/SAE CD 21434 – Road Vehicles – Cybersecurity Engineering is currently under development

Other notable standards include:

- ISO/SAE AWI 21434 - Road Vehicles -- Cybersecurity engineering (Under development)
- NIST, FIPS, etc.
- CERT (coding standards and more)
- MISRA (coding standard)
- ISO 27000 (wikipedia)
- RTCA/DO-326 (avionics)
- IEC 62443 (primarily automation)
- CMMI (Security by Design with CMMI v1.3, from Siemens)
- Microsoft SDL (Security Development Lifecycle)
- EVITA (research project)
- OpenSAMM (Software Assurance Maturity Model)

5. DEFENSE-IN-DEPTH STRATEGY

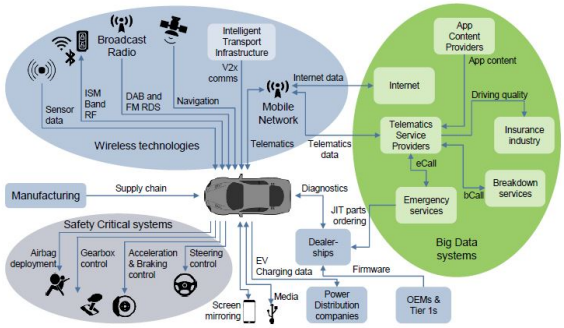
Automakers are developing a defense-in-depth strategy to address the cybersecurity threats to vehicles. The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security. Defense in depth is originally a military strategy that seeks to delay rather than prevent the advance of an attacker by yielding space to buy time.

The four levels of the Defense-In-Depth strategy are:

- Level 1 – Restrict access to the network
- Level 2 – Secure onboard communications
- Level 3 – Apply data usage policies

- Level 4 – Detect anomalies and defend

Attack surfaces can be classified in different groups



Level 1 is accomplished by first limiting the number of electronic control units (ECU) with off-board connections. In level 1, the network is divided into security zones, and traffic is restricted between the zones. Last, unused ports are deactivated and all devices on the network require authentication and authorization.
Level 2, Secure the onboard communications may utilize crypto keys at each node, transport layer security, authentication protocols and other methods appropriate to the system being protected.
Level 3, apply data usage policies protect the system from inappropriately sharing data with other systems, or communicating them externally.
Level 4, detect anomalies and defend and take many forms. Detection can occur at a central device, in a distributed method across ECU's, or at the receiver. A plausibility check based on diverse input data or data sequence or failed integrity checks might trigger defense mechanisms. Defense may include masking or blocking the message from the ECU, enforce bandwidth limitations at switches, or reconfigures (e.g., deactivation of critical functions, initiate hand-over, request change of session key, etc.

With regards to cellular communications, one must consider the risk and enact appropriate measures, such as mobile device management (MDM) systems, to mitigate the risk and bring it to an acceptable level.[b] Cellular infrastructure has evolved into 4G systems and standards and now moving towards 5G. The standards organizations supporting these developments have been the 3rd Generation Partnership Project (3GPP), initially for GSM systems, and the 3rd Generation Partnership Project 2 (3GPP2), initially for CDMA systems. "Long Term Evolution" (LTE) and its 4G evolution, "LTEAdvanced," is defined by 3GPP as the evolution path for wireless networks. The initial release of the standard is currently being deployed commercially and LTEAdvanced is targeted for service in several years. However, in a theatre environment, the communications packet being transmitted has to be encrypted and authentication, unbundling and decryption software must exist at the transceiver in the base station.

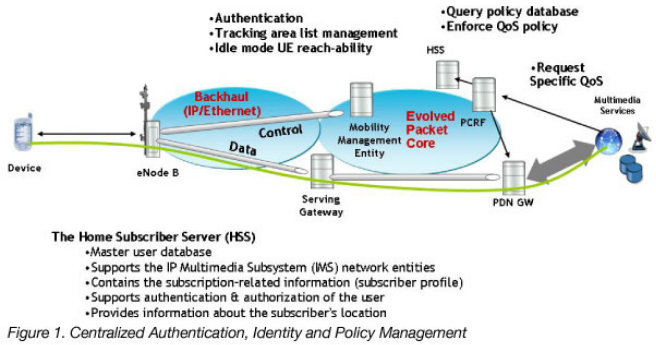


Figure 1. Centralized Authentication, Identity and Policy Management

6. TRAINING IMPLICATIONS

Cybersecurity is today necessary for every engineer. Increasingly systems in the networked vehicle are critical to safety. Functional security cannot be achieved without a comprehensive concept for cybersecurity. With all of these changes and continually evolving threats, people responsible for the design, build, testing and repairing of vehicles need the knowledge and expertise to deploy trusted vehicles. We need assessors who are technical experts of the systems they assess. "Simple" process and document checking won't be enough. Training is required in:

- Cybersecurity foundations for automotive applications
- Cybersecurity for radio and nomadic devices
- Current threats and methodology
- Security Standards (e.g., SAE J3061-2016), legal obligations and governance
- Threat assessment and remediation analysis (TARA)
- Efficient implementation of security in the lifecycle from the security assets to the risk analysis to the consistent implementation throughout the entire lifecycle
- Practical experience and hands-on case studies
- Current trends

7. SUMMARY

Threat surfaces do exist and are now being discovered and addressed. As Military personnel and vehicles of the US Armed Forces become more connected, there will be greater risk of attack, breach and disruption. These attacks will continually evolve. Vehicle cybersecurity efforts will be with us from now on. Standardization for security similar to ISO 26262 is needed, which forms a consensus in the cyber domain.[c] Safety, security, reliability are system aspects that need to be balanced. They are all part of the "quality" of the product.

PRESENTERS

[1] Scott J. McCormick, President, Connected Vehicle Trade Association, Inc.

[2] Elaina Farnsworth, CEO, The Next Education

REFERENCES

[a] See: Information Technology Laboratory, National Institute of Standards and Technology. (2001, May 25). *FIPS PUB 140-2 - FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES.* Retrieved from NIST Computer Security Resource Center: https://csrc.nist.gov/csrc/media/publications/fips/140/2/final/documents/fips1402.pdf

[b] Homeland Security, Industrial Control Systems Cyber Emergency Response Team. (2016, September). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies.* Retrieved from US Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) : https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf

[c] Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., . . . Kohno, T. (2011, August 10). *Comprehensive Experimental Analyses of Automotive Attack Surfaces.* Retrieved from Center for Automotive Embedded Systems Security: http://www.autosec.org/pubs/cars-usenixsec2011.pdf