Managing complexity of automotive software

Most cyberattacks remain undetected until it's too late, so early detection is a must. As the connected car evolves, it is recommended that cybersecurity configuration be performed remotely with an enterprise security management system.

The automotive industry is driven by a group of mega-trends called, "automation, connectivity, electrification, and sharing" commonly referred to as Aces. Aces represents a new opportunity for the automotive industry to meet an entirely new set of challenges. A key challenge is dealing with the increasing software in today's modern automobile. Today, there are more lines of code in the connected car than other more highly sophisticated machines such as the U.S. Air Force F-35 Joint Strike Fighter, Boeing 787 Dreamliner or the U.S. Space Shuttle1. Hardware today is more powerful and, as a result, millions of lines of code can be executed through a multitude of systems to perform complex functions inside the connected car. Soon, these vehicles will communicate externally by way of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Safety and security are paramount concerns, so all onboard systems must be secure while the vehicle is in motion – or sitting idle.

Cybersecurity threats are ever increasing

The "2020 automotive cybersecurity report" (Figure 1) from Upstream Security depicts a six-fold increase over a nine-year time period with numbers doubled from 2018 to 2019. The graph depicts a 94 percent year-over-year (YoY) growth in cyberattacks since 2016. New business models will have to evolve as complexity, reliability, risk, and liability become primary drivers.

The increased effectiveness and proliferation of automotive cyberattacks has created a new urgency for security solutions, driving new regulations by lawmakers to prevent cyberattacks globally. The U.S. Security and Privacy in Your Car Act, or also called the "Spy Car Act of 2017", defines requirements for protection against unauthorized data access and reporting. The bill directs the National Highway Traffic Safety Administration (NHSTA) to issue vehicle cybersecurity guidelines that require motor vehicles manufactured for sale in the United States to build in protection against unauthorized access to electronic controls and driving data.

Also in 2017, the U.S. House of Representatives passed H.R. 33886, "The Self Drive Act", a first-of-its kind legislation to ensure the safe and innovative development, testing, and deployment of self-driving automobiles. China established an automotive cybersecurity committee to ensure the safe operation of intelligent, connected, and electric cars, including research, standards, policies, laws, and regulations. Other data regulations are beginning to emerge, such as the EU's GDPR (general data protection regulation), Canada's Digital Privacy Law (Pipeda), and the European Parliament Transport Committee's call for EU regulation on access to car data.

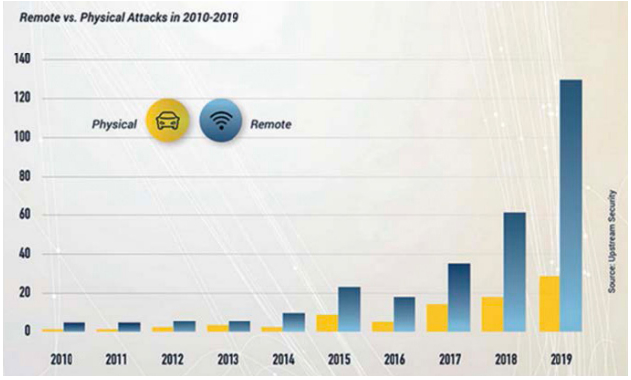


Figure 1: Over the past several years, remote automotive cybersecurity incidents have increased dramatically. As more connected vehicles enter the market, the potential for attacks rises exponentially (Source: Upstream Security)

NHTSA's automotive cybersecurity research program takes a threat analysis approach to cybersecurity, placing threats into six different categories:

- Spoofing – where a person, program, or device conceals itself as something it is not by manipulating data to gain an illegitimate advantage.
- Tampering – intentional data alteration to harm the consumer. For connected cars, this includes modifications to configuration data, software, or hardware used in vehicle control systems.
- Non-repudiation – where a statement's author cannot successfully dispute validity or authorship.
- Info disclosure – refers to many types of sabotage related to data leakage.
- Denial of service (DoS) – refers to a cyberattack where a machine is flooded with excessive requests from an attacker forcing it to become unavailable for legitimate users by overloading its systems and preventing legitimate requests from being fulfilled.
- Elevation of privilege – where an attacker can abuse a machine and perform unauthorized activities by gaining illegitimate access to systems resources and data, causing more damaging attacks.

Connected car attack surfaces

By understanding these threats, OEMs (original equipment manufacturers) can look at four potential attack surfaces of the connected car:

- The first attack surface is direct physical, including access to the on-board diagnostics (OBD) port, charging port, or harness connectors. A car becomes vulnerable when a hacker has direct physical access, such as at the dealer or repair shop for maintenance or repairs, or when a second party has gained access to the vehicle, like a parking valet who could execute a direct physical attack.
- The second attack surface is indirect physical. Here, a carrier is needed to execute the attack, such as a USB stick or CD that compromises the car's firmware, or SD cards and firmware updates which open up all kinds of attack possibilities.
- The third possibility for attack is through wireless. Bluetooth and the mobile network are prone for wireless attacks and increased automotive systems connectivity has dramatically increased the potential for attack.
- The final attack surface is sensor fooling. Researchers have shown that these types of attacks are possible in a laboratory setting. Connected and autonomous cars often use light detection and ranging (Lidar) sensor technology, causing systems to be blinded or fooled with false information to harm the vehicle operator and occupants. GPS is another technology with vulnerabilities that could be exploited.

Mapping attack surfaces to a vehicle's architecture (Figure 2) depicts attack surfaces corresponding to a vehicle's architecture. This basic schematic highlights

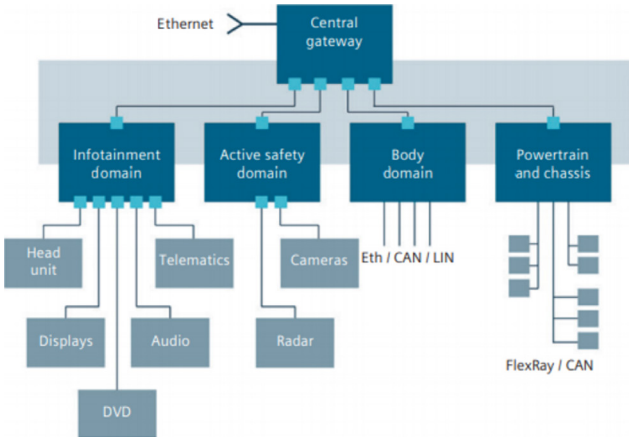


Figure 2: Attack surfaces and corresponding functional units (Source: University of California, San Diego, "Comprehensive experimental analyses of automotive attack surfaces")

connectivity within the car, including the use of automotive gateways and multiple vehicle networks, and different types of domains: infotainment, active safety (containing cameras and radar), and body. Chassis and powertrain ECUs (electronic control unit) utilize a CAN network that can be easily exploited. Also shown are a variety of networks to communicate data within the central gateway. The central gateway ECU is a focal point of attack because of its direct exposure to the outside world.

It is quite clear that modern connected cars have multiple entry points, which hackers view as both a challenge and opportunity. To prevent any type of cyberattack, all entry points must maintain an appropriate level of security.

Security can be broken down into three aspects. The first aspect includes authentication and access control. Authentication means who is allowed to do things inside a vehicle. Access control is what the individual or system is allowed to do once inside. The second aspect to security is protection against illegitimate access, data leakages, or harmful software or Trojans from being installed. The final aspect to defining security is to detect and report security incidents.

A multi-layered security approach is needed

Knowing the attack surfaces within the connected automobile provides the foundation for a multi-layered security approach. Automotive OEMs must secure all internal and external communications. An embedded firewall to protect the vehicle from accepting unauthorized traffic, data, or signals sent by a malicious IP address must be part of the mix. The following are critical components to secure a connected car:

Embedded firewalls: Building a firewall into a vehicle is a highly-specialized process tailored exclusively to the automotive environment. To build the firewall, a software development kit (SDK) is integrated directly into the communications stack, whether CAN, TCP/IP, or other connected solution. The embedded firewall must be highly configurable with built-in flexibility, operate across a range of vehicle ECUs, and work with a real-time operating system (RTOS) or even in the Autosar environment. Many cyberattacks begin by sending packets to the connected car, seeking weaknesses, so if the firewall can detect this ▷

CANcrypt for secure communication

As already mentioned, CANcrypt from Esacademy's (Emsa) can be used to secure communication. Commonly used security methods for authentication and encryption/decryption on the Internet cannot be easily applied to CAN/CANopen. Emsa's solution is a combination of scalable security features for CAN. The in-depth description of CANcrypt is available as book: "Implementing scalable CAN security with CANcrypt, authentication and encryption for CANopen, J1939, and other Controller Area Network or CAN FD protocols".

CAN Newsletter Online

The CAN Newsletter Online as well as the magazine, already reported several times about ways of cybersecurity and CAN, provided by Emsa.

Security column

Updates and outlook on securing CAN

Over the past years, Olaf Pfeiffer and Christian Keydel from Embedded Systems Academy (Emsa) have published several security-related CAN articles in the CAN Newsletter magazine. It's now time for an up-to-date summary, review, and outlook.

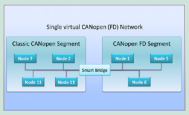
Read on

CAN Newsletter magazine

Classical CAN/CAN FD security threats

The authors of this article already have introduced various technical solutions for distinct security threats. This time, they want to take a step back to look at the bigger picture of CAN security.

Read on



CAN Newsletter magazine

Smart-bridging CANopen and CANopen FD

This article gives an description on how to smart-bridge classic CANopen and CANopen FD networks.

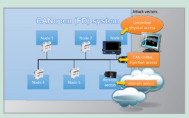
Read on

CAN Newsletter magazine

CAN security: how small can we go?

What kind of CAN security can still be added to a deployed CAN system if the processors have only medium performance and only adding a few kilobytes of extra code is possible?

Read on



CAN Newsletter magazine

CANopen FD multi-level security demonstrator

Many CAN-based networks open multiple attack vectors for hackers, especially after they have gained access to the system either remotely through a gateway or even physically.

Read on

activity early and ensure certain packets are not allowed to be received or forwarded, a potential attack will be thwarted before it even begins. Controlling what ports and protocols used to receive messages for the vehicle is crucial to protect and report suspicious activity.

Embedded firewalls for ECUs: Adding a firewall to a central gateway requires portable source code that can be integrated and configured into the ECU. Filtering rules built into the firewall block specific IP addresses and recognize unwanted activity with quick response to prevent an attack – firewall support of different types of filtering capabilities (CAN network, rules-based, threshold-based, static) is critical, including stateful packet inspection. Logging and reporting attacks enable intrusion detection, which is knowing when something unusual is happening. The connected vehicle must be able to report nefarious activity back to a vehicle operations center allowing security operations teams to take the necessary action and share that information across the security network.

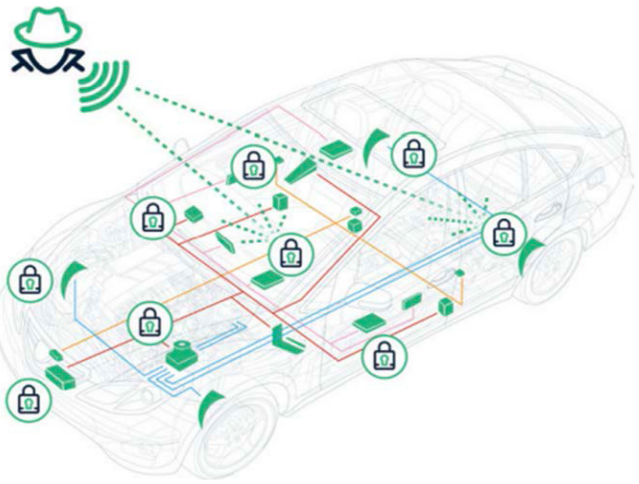


Figure 3: Securing ECUs from cyberattacks by employing an embedded firewall and certificate-based authentication (Source: Sectigo)

A firewall on an external gateway ECU manages communication with all outside entities, serving as the bullseye for attack by enabling filtering rules for all vehicle communications. Its job is to detect and block attacks before they reach the target ECUs. A firewall on an internal gateway ECU is another option. With multiple networks within the car, an internal gateway ECU allows communication between different networks to isolate safety critical functionality – the more critical internal systems are protected from potentially malicious network traffic. Finally, a firewall can be on an endpoint ECU, the actual control ECU that manages critical functionality in the vehicle. Control ECUs include anti-lock brakes, airbags, steering control, etc., so it is advisable to deploy a firewall on multiple endpoint ECUs.

Secure communication: There are numerous use cases for secure communication, including communication between the car and external systems, V2V communication, and communication within the car. V2V communication is more common and critical today, so it must be protected. To achieve secure communication within the car, all ECUs must be protected. As a communication session begins, the origin of that communication is known, so encryption is recommended. Encrypted communication uses IP protocols such as TLS, DTLS, and SSH. If running over a CAN network, CANcrypt can be used. All data encrypted using strong cryptography is required to ward off cyberattacks.

Authentication: During a communication session (Figure 3), authentication verifies that who you are communicating with is actually who they say they are, i.e., is the other device or process really who it claims to be? For authentication, a public key infrastructure (PKI) to manage and issue digital certificates is crucial. Every ECU must be identifiable and PKI-based certificates provide strong authentication for machine-to-machine communication. Another aspect of PKI security is code signing to enable secure boot and secure updates. With V2I communications, high-speed automated certificate issuance is mandatory since hosting and managing the entire process securely is essential. Where is the certificate authority hosted? How is certificate issuance performed? Is it automated? Is it secure? How are private keys protected?

Finally, an OEM may have its own internal strategy for securing the connected car with a proprietary safety ecosystem. But when considering V2I or V2V communications, where vehicles from multiple OEMs travel the same road, vehicle manufacturers must construct a shared ecosystem with the same requirements for security, management capabilities, and other safety-related capabilities to ensure interoperability among all vehicles on the road.

Conclusion

To protect today's connected cars, multiple layers of security are required, and all attack surfaces must be taken into consideration. Most cyberattacks remain undetected until it's too late, so early detection is a must. As the connected car evolves, it is recommended that cybersecurity configuration be performed remotely with an enterprise security management system. This integration provides centralized management of security policies, situational awareness, and device data monitoring, event management, and log file analysis for data analytics. Security needs to be a shared common resource. Embedded firewalls, secure communication, and strong authentication techniques are vital elements that constitute a multi-layered security approach. ◀

Reference

[1] Robert N. Charette. "This car runs on code", IEEE Spectrum, February 2009.

Author

Dr. Ahmed Majeed Khan
Siemens Digital Industrie Software
info@siemens.com
www.siemens.com