CAN Newsletter Online

CAN NEWSLETTER MAGAZINE

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 complete article is published in the March issue of the CAN Newsletter magazine 2022. This is just an excerpt.

(Source: Siemens Digital Industrie Software)

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 auto- motive 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.

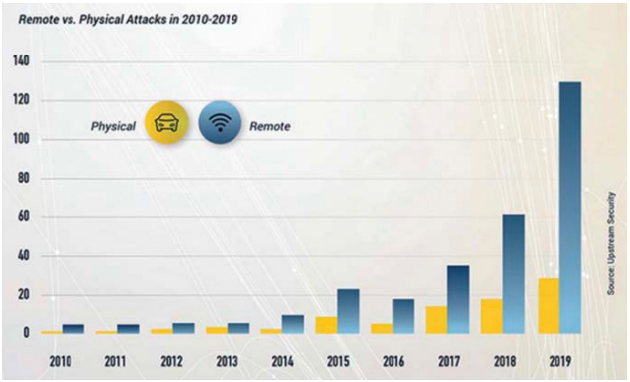

Figure 1: Over the past several years, remote automotive cybersecurity incidents have increased dramatically. As more connected vehicles enter the market, the potential for attacks rises exponentially (Source: Upstream Security)

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.

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.

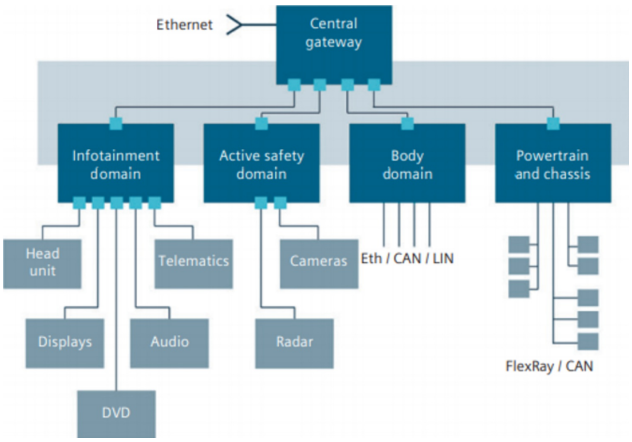

Figure 2: Attack surfaces and corresponding functional units (Source: University of California, San Diego, "Comprehensive experimental analyses of automotive attack surfaces")

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

If you would like to read the full article, you can download it free of charge or you download the entire magazine.

cw