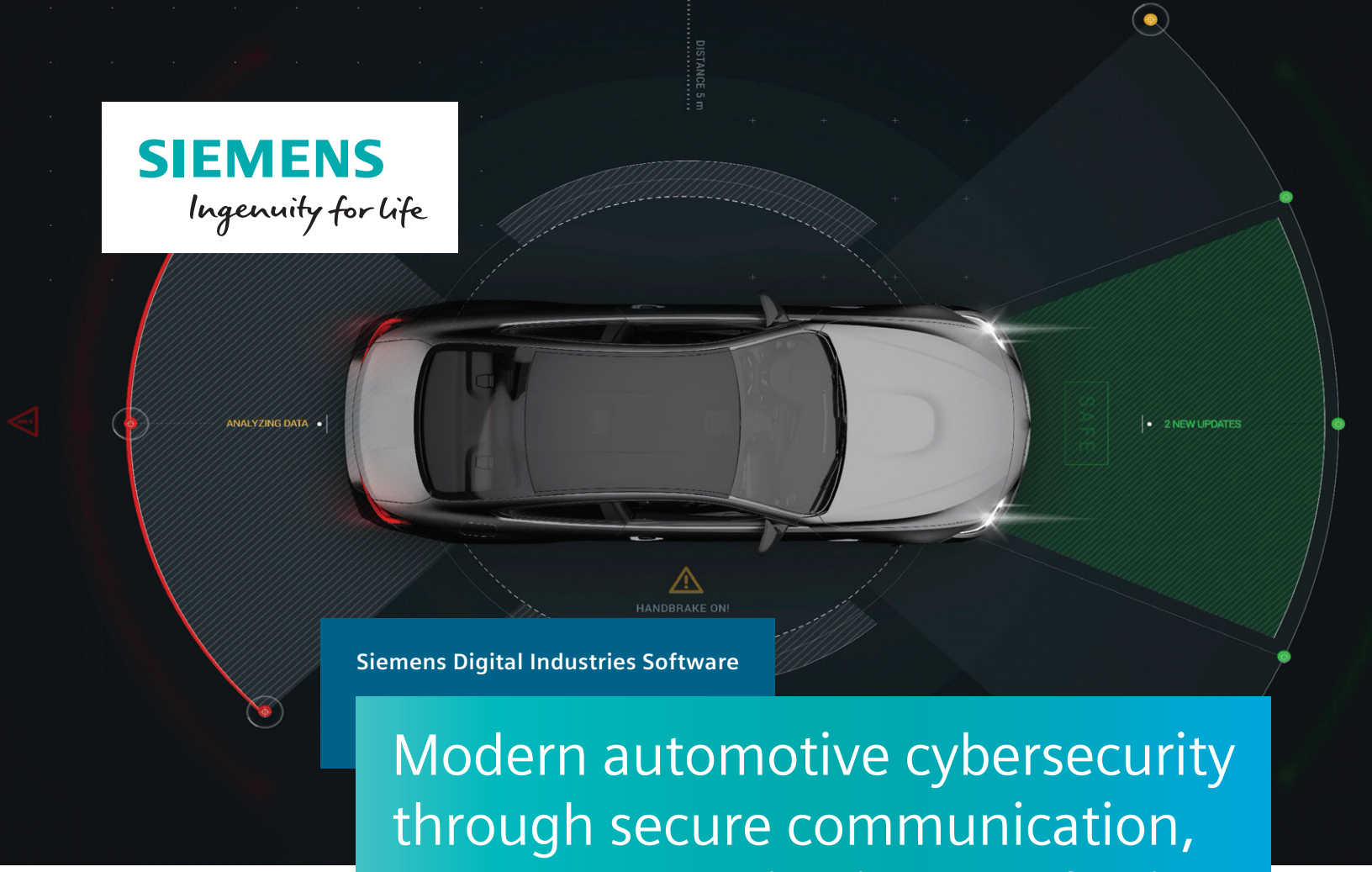


SIEMENS
Ingenuity for life

Siemens Digital Industries Software

Modern automotive cybersecurity through secure communication, strong authentication and flexible firewalls

Executive summary

Continuous security threats on connected automobiles have exposed critical system vulnerabilities. To address these risks, regulatory agencies are now defining cybersecurity requirements by writing new legislation and holding carmakers and their supply chain liable for security and safety breaches.

To adequately address current and future security issues, this white paper discusses a multi-layered approach to connected vehicle security and explains how this security architecture can protect vehicle entry points as well as in-vehicle networks from threats. Several security strategies such as embedded firewalls, authentication, secure communications, encryption and digital certificates will be discussed.

Dr. Ahmed Majeed Khan
Senior Product Manager
Siemens Digital Industries Software

Alan Grau
VP of IoT/Embedded Solutions
Sectigo

Contents

Introduction

The automotive industry is driven by a group of mega-trends called, "Automation, Connectivity, Electrification and Sharing" or what's commonly referred to as ACES.

ACES represents a new opportunity for the industry as it rises up to meet an entirely new set of challenges. One of the challenges is how to deal with the increased use of software in today's modern automobile. In fact, there are more lines of code in the connected car than other more highly sophisticated machines of our time such as the U.S. Air Force F-35 Joint Strike Fighter, Boeing 787 Dreamliner or the U.S. Space Shuttle[1]. Hardware used today is more powerful and as a result, millions of lines of code can be executed when performing a myriad of complex functions. This has created a multitude of systems inside the connected car. Connected cars will soon communicate externally by way of vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, as well as internally among the vehicle subsystems and networks. Safety and security are paramount. All onboard systems must be secure so nothing can affect the vehicle while in motion – or sitting idle.

Dramatic increase in cybersecurity threats

The visual below (figure 1) illustrates the steady climb of automotive cybersecurity attacks from 2010 to 2019. The graph, from the *"2020 Automotive Cybersecurity Report"* from Upstream Security, shows a six-fold increase over this nine-year time period[2]. The numbers have doubled in 2019 when compared to 2018. Moreover, the graph depicts a 94 percent year over year (YoY) growth in cyberattacks since 2016[3].

It's estimated that 57 percent of all automotive liability claims will be paid by the automotive ecosystem[4]. There's no question that new business models will have to evolve as complexity, reliability, risk and liability become primary drivers.

New laws directed specifically at automotive manufacturers

The increased effectiveness and outright proliferation of automotive cyberattacks has created a new urgency in developing security solutions. An unprecedented level of commercial intervention is now underway around the globe, including new regulations by lawmakers to prevent cyberattacks.

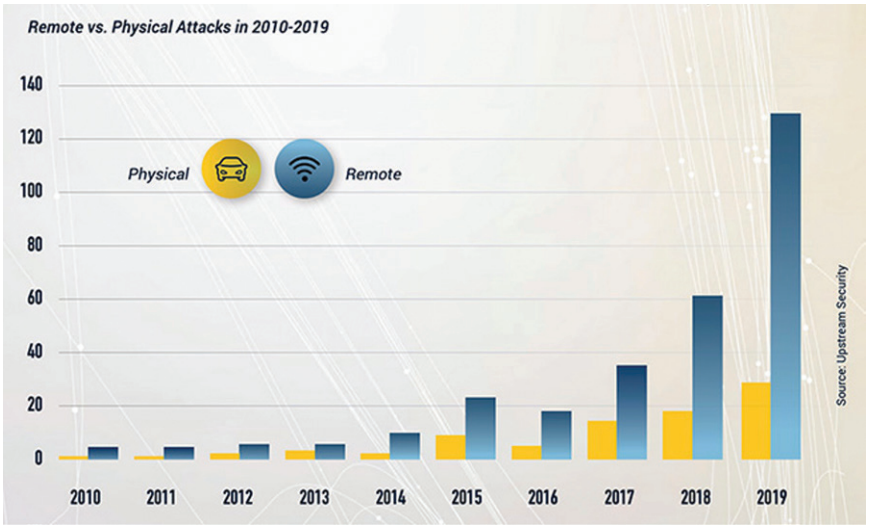


Figure 1. Over the past nine years, remote automotive cybersecurity incidents have increased dramatically. As more connected vehicles hit the road, the potential for damage rises exponentially. Source: Upstream Security.

The U.S. Security and Privacy in Your Car Act[5], or 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.

Similarly, also in 2017, the U.S. House of Representatives passed H.R. 3388[6], "The SELF DRIVE Act", a first-of-its-kind legislation to ensure the safe and innovative development, testing and deployment of the self-driving automobile. This bill strikes a balance between consumer safety while encouraging innovation.

China has established an automotive cybersecurity committee to ensure the safe operation of intelligent, connected and electric cars. The committee will facilitate efforts among researchers and manufacturers to carry out research and work out standards, policies, laws and regulations for cybersecurity in automobiles.

The discussion over "who owns the data" has also been a hot topic for IT companies over the past decade. The debate is not only about who owns the data, but who is responsible for protecting it? This debate applies to the connected automotive industry as well. Data regulations are beginning to emerge. Personal data regulations such as the EU's GDPR[7], Canada's Digital Privacy Law (PIPEDA)[8] and the European Parliament Transport Committee's call for EU regulation on access to car data[9] are a few examples.

Automative network security

NHTSA's Automotive Cybersecurity Research Program takes a threat analysis approach to cybersecurity, breaking down threats into six different categories.

The six threat categories include:

- **Spoofing** – a situation in which a person, program or device conceals itself as something it is not by manipulating data to gain an illegitimate advantage.
- **Tampering** – intentional alteration of data in a way that would make it harmful to the consumer. In the context of connected cars, it could refer to modifications to configuration data, software or hardware used in vehicle control systems.
- **Non-repudiation** – describes a situation where a statement's author cannot successfully dispute its authorship or validity. In other words, the author or the statement cannot later claim to have not made the statement. For example, when the authenticity of a signature is being challenged, the authenticity is being "repudiated."
- **Info disclosure** – can refer to many types of sabotage related to data leakage.
- **Denial of service (DoS)** – refers to a cyberattack in which a machine is flooded with excessive requests from an attacker to an extent that it becomes unavailable for its legitimate users. DoS is typically accomplished by flooding the targeted resource with superfluous requests in an attempt to overload its systems and prevent legitimate requests from being fulfilled.
- **Elevation of privilege** – a situation in which an attacker can abuse a machine and performs unauthorized activities by gaining illegitimate access to resources. Hackers who are successful with elevation of privilege attacks have greater access to systems resources and data, allowing more damaging attacks.

With a basic familiarity of these threats, it is now possible to look at the potential attack surfaces of the connected car. For any type of cyberattack to be fully realized, the first stage is for the hacker to find a way to access the car. The second stage is gaining access to an electronic control unit (ECU) within the vehicle by exploiting a vulnerability or weak cybersecurity controls. And the final phase is exploiting a control feature within the compromised ECU.

To understand more clearly what this means, the connected car has four primary attack surfaces which can be exploited.

Four connected car attack surfaces:

The first attack surface is **direct physical**. This includes access to the on-board diagnostics (OBD) port, charging port, or harness connectors. A car becomes vulnerable when a hacker has direct physical access. This scenario occurs when a car is at the dealer or repair shop for maintenance or repairs, or when a second party has gained access to the vehicle. A skilled hacker working as a valet, for example, could execute a direct physical attack.

The second attack surface is **indirect physical**. Here, a carrier of some sort is needed to execute the attack. The carrier could be a USB stick or CD that compromises the car's firmware. Also, the use of SD cards and firmware updates in modern cars opens up all kinds of attack possibilities.

The third possibility for attack is through **wireless**. Bluetooth and the mobile network are prime possibilities for a wireless attack. Increased connectivity of modern cars has dramatically increased the potential for this type of attack.

The final attack surface is **sensor fooling**. To date, there are no known attacks on a connected car's sensors. However, researchers have shown that these types of attacks are possible, if not achievable, in a laboratory setting. Connected and autonomous cars often use Light Detection and Ranging (LiDAR) sensor technology. These systems can be blinded or fooled with false information that could cause serious harm to 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 as it corresponds to a vehicle's architecture. This figure shows a basic schematic highlighting connectivity within the car, including the use of automotive gateways and multiple vehicle buses. It shows different types of domains including infotainment, active safety (containing cameras and radar) and body. Chassis and powertrain ECUs utilize a Controller Area Network (CAN) bus that can be easily exploited. Also depicted are different types of buses used 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.

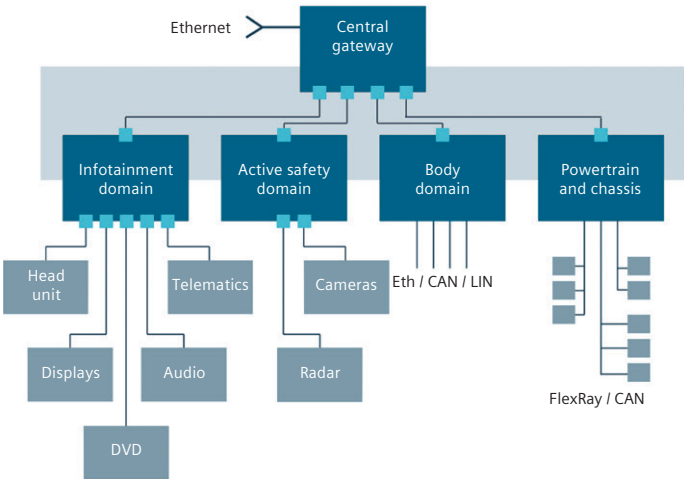


Figure 2. Attack surfaces and corresponding functional units. Source: University of California, San Diego, "Comprehensive Experimental Analyses of Automotive Attack Surfaces."

Figure 3 illustrates how the attack surfaces can be mapped to functional units with the vehicle, such as V2V communication, telematics and on-board diagnostics (OBD). It's becoming more common today for car owners to update their vehicles via software-over-the-air (SOTA). SOTA updates require continuous access and it's during this time, the vehicle is most vulnerable. The diagnostic port OBD-II is also vulnerable to cyberattacks. Several protocols are in use here, including J1850, ISO 15765 CAN, and others. Similarly, many vehicle systems and ECUs are connected via a CAN bus, and this too has shown to be vulnerable to attacks.

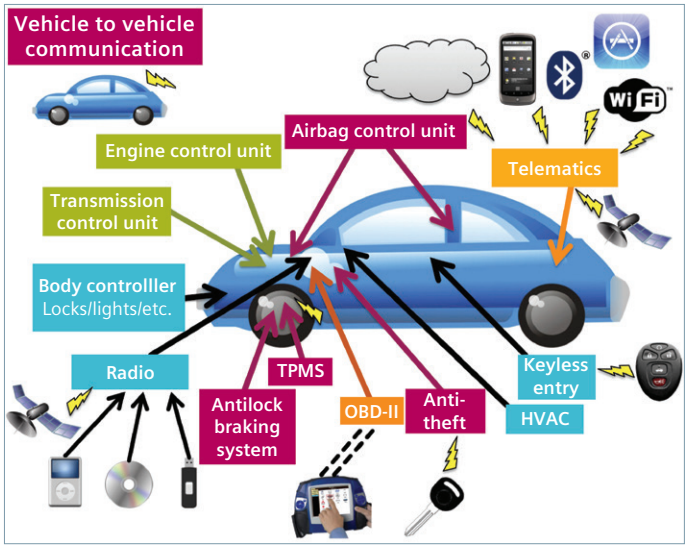


Figure 3. Attack surfaces within a connected car's architecture. Source: University of California, San Diego, "Comprehensive Experimental Analyses of Automotive Attack Surfaces."

Looking at figures 2 and 3 it is quite clear that modern connected cars have multiple entry points. These entry points are seen by hackers as both a challenge and opportunity. To prevent any type of cyberattack, it's imperative for all entry points to maintain an appropriate level of security. To fully understand what it takes to secure a vehicle, it might best to first define "security."

Defining security

Security can be broken down into three aspects. The first aspect includes both 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 from external attacks. This can mean protection against illegitimate access or protection from data leakages, ensuring communication security and finally, avoiding any kinds of harmful software or Trojans from being installed on automobiles.

Finally the last aspect to defining security, which is vitally important, is to detect and report security incidents.

What's required today: A multi-layered security approach

Understanding attack surfaces and what security means to the connected automobile provides the foundation for the proposal of a multi-layered security approach that takes these principles into consideration.

In order for a multilayer security approach to work, the automotive OEM needs to secure all communications; this includes securing all external as well as internal communications.

When discussing a multi-layered security approach, many factors must be considered as these security solutions are built into the connected car. An embedded firewall, or intrusion detection to protect the vehicle from accepting unauthorized traffic, data, or signals sent by a malicious IP address must be part of the mix. Of course, authentication is a key component as well. Utilizing a secure operating system (OS), multicore framework and hypervisor support should also be considered.

This paper explores a few of the more critical components needed to secure a connected car: embedded firewalls, secure communication and authentication.

Embedded firewalls

Building a firewall into a vehicle is a highly specialized process. Understand that this is not a networking firewall running in a router or gateway or on an enterprise device. This is a highly specialized solution tailored exclusively to the automotive environment.

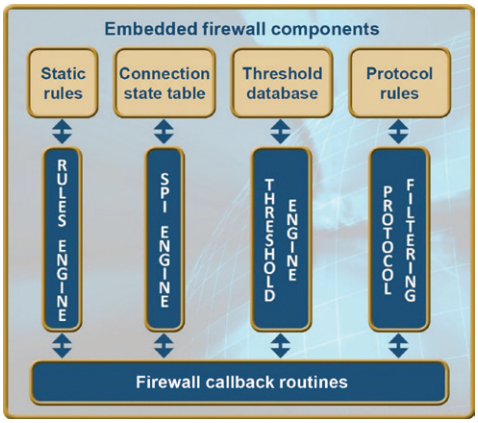
To begin building the firewall, a Software Development Kit (SDK) is needed. The SDK can be integrated directly into the communications stack, whether TCP/IP, CAN, or any other connected solution. The firewall has to meet specialized requirements. It needs to have built-in flexibility to run on any ECU. It should work with a real-time operating system (RTOS) or even in the AUTOSAR environment. Some environments might be resource limited which introduces its own set of challenges. To be successful, the embedded firewall must be a highly configurable, modular solution that works across a range of vehicle ECUs in use today.

When building the firewall, it's recommended to first step back and consider the requirements that must be satisfied. Many cyberattacks begin by sending packets to the connected car, probing for weaknesses. If the firewall can detect this activity early and ensure certain packets are not allowed to be received or forwarded, a potential attack will be thwarted before it even begins. It's important to control what ports and protocols are used to receive messages for the vehicle. If one can control the IP addresses sending data to the vehicle it is possible to protect the vehicle and report suspicious activity.

And why is this important? When studying some of the early cyberattacks, the Miller Vilsack attack on the Jeep Cherokee for example, it wasn't an attack where the hackers started sending a few packets to the car, completed a successful attack and moved on. In the case of the Jeep Cherokee, as with many cyberattacks, the attack started with sending hundreds or even thousands of different messages to the vehicle to probe for weaknesses. What messages can the hacker send to the vehicle? What response does the hacker receive in return from the vehicle? Can the vehicle "sense" when it's being probed and respond in a timely and appropriate manner?

Embedded firewalls for ECUs

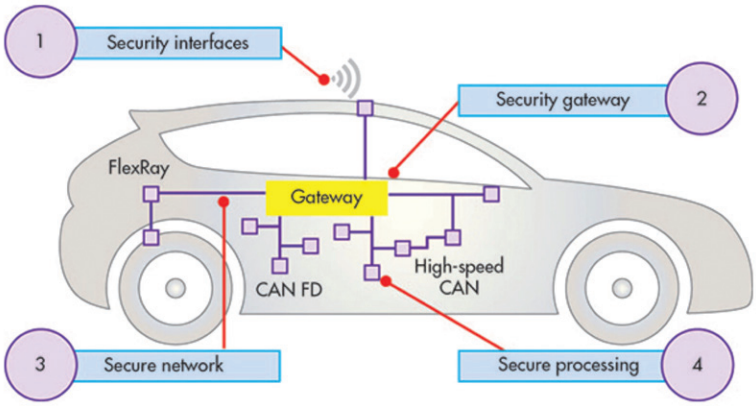
Adding a firewall to a central gateway requires portable source code that can be integrated into the ECU. The firewall must be configurable. For example, citing the Miller Vilsack attack, had there been a firewall in place, suspicious traffic from IP addresses would have been reported calling out the suspicious domains sending the messages. Filtering rules built into the firewall to block specific IP addresses would recognize unwanted activity and respond quickly – a sure way to prevent an attack.



It's critically important that the firewall support different types of filtering capabilities. The ideal firewall should support CAN bus filtering and rules-based filtering. Blocking messages by ports, protocol, IP addresses, etc. is a sure way to stop an attack from ever happening. The firewall must be able to do threshold-based filtering, static or rules-based filtering and stateful packet inspection. These are just a few of modules that need to be built into the firewall. The logging and reporting of attacks enables intrusion detection, which is knowing when something unusual is happening. Reporting this back to some type of a vehicle operations center allows security operations teams to take action based upon that information and shut down the attack before the attackers can complete their attack.

What do you want your firewall to do?

An embedded firewall can operate in different modes. A firewall operating in active mode blocks all outside activity violating firewall rules. A firewall operating in passive mode looks for suspicious or anomalous activity and reports that data back to an operations center. Also, there may be scenarios where a firewall needs to support a learning-mode operation where the firewall learns typical traffic patterns and can later operate in an active mode, recognizing and blocking traffic not matching that pattern.



There are many places to deploy an embedded firewall. One option is deploying the firewall on an **external gateway ECU**. This type of gateway manages the communication with all outside entities. As the focal point for communication, it becomes the bullseye for attack. The firewall on an external gateway ECU enforces filtering rules for all communication coming into the vehicle. Its job is to detect and block attacks before they reach the target ECUs.

It's also possible to deploy the firewall on an **internal gateway ECU**. If there are multiple networks within the car an internal gateway ECU allows communication between different networks. A firewall used in this instance allows for the isolation of safety critical functionality – the more critical internal system are protected from potentially malicious network traffic.

Finally, a firewall can be deployed on an **endpoint ECU**, the actual control ECU that manages critical functionality in the vehicle. Control ECUs are features such as anti-lock brakes, airbags, steering control, etc. In most situations, it's advisable to deploy a firewall on multiple endpoint ECUs. After all, security is about defense in depth and multiple layers of protection. If one aspect of the security solution breaks down, you need to have other security layers to back it up.

Use case

Global tier-one automotive ECU supplier to release new secure gateway
A global leader in cybersecurity solutions, Sectigo, teamed up with the automotive embedded software group at Siemens Digital Industries Software for the development of an embedded firewall solution for a leading global tier-one automotive ECU supplier. The partnership was tasked to build a firewall solution to accommodate the next generation of vehicles with high levels of connectivity. In previous releases, the customer had to rely on an internal automotive gateway ECU for managing external communication. But this proved problematic as the gateway became the focal point for cyberattacks. A new approach to network security was needed.

Sectigo made available an embedded firewall for integration into the external ECU gateway. To speed adoption – and further enhance security capabilities – Siemens integrated the Sectigo Embedded Firewall with its popular AUTOSAR platform, Capital VSTAR. Security capabilities include controlling the packets forwarded to internal networks and blocking traffic based upon both pre-configured filter rules and runtime behavior. In addition, Sectigo's embedded firewall provides the ability to report suspicious activity back to a management system.

Customers have been testing the firewall during successful trials this past year. The Sectigo-enabled AUTOSAR platform is expected to be fully deployed by 2021.

Secure communication

Just as there are multiple use cases for the embedded firewall, so too are there numerous use cases for secure communication. Scenarios include communication between the car and external systems, V2V communication, and communication within the car. V2V communication is more common today and a critical form of communication that must be protected. And again, when discussing secure communication within the car, all of the ECUs must to be protected.

Secure communication is about ensuring that each time a communication session begins, the origin of that communication is known. To ensure secure communication, encryption is recommended. Encrypted communication uses IP protocols such as TLS, DTLS and SSH. If running over a CAN bus, CANcrypt can be used. Ensuring that all data is encrypted using strong cryptography is critical to warding off cyberattacks.

Authentication

Authentication is used when establishing a communication session to verify 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 machine-to-machine communication, certificate-based authentication is frequently used. When discussing authentication, a critical aspect is the role of public key infrastructure (PKI) and how to manage and issue digital certificates. Every ECU has to be identifiable and PKI-based certificates are ideal as they provide strong authentication and can be utilized for machine-to-machine communication. Another aspect of PKI security is code signing which enables secure boot and secure updates for ECUs.

PKI certificates play a central role. Throughout this paper, V2V and V2I communications have been mentioned as critical areas to address in the connected car. With V2I communications, high-speed automated certificate issuance is a must. And having a way to host and manage the entire process in a secure fashion is an essential part of the process. Where is the certificate authority hosted? How is certificate issuance performed? Is it automated? Is it secure? How are private keys protected? These are all extremely important questions that must be taken into consideration.

When looking at a single automotive OEM and their cybersecurity solution, it's common for that manufacturer to have their own internal strategy for the connected car. They are certainly allowed to have their own 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

Building security into the connected car requires a multi-faceted approach (figure 4). It cannot be done as an afterthought. To protect these vehicles, multiple layers of security are required, and all attack surfaces must be taken into consideration. It is safe to assume that at some point in time a connected car will come under a cyberattack. Hackers attempting to penetrate an embedded device using remote attacks probe the device for open ports to find any form of weakness. Blocking all unused ports and protocols limits the attack surface. Logging packets that violate configured filtering rules enable detection of suspicious behavior. And remember, most cyberattacks remain undetected until it's too late, so early detection is a must.

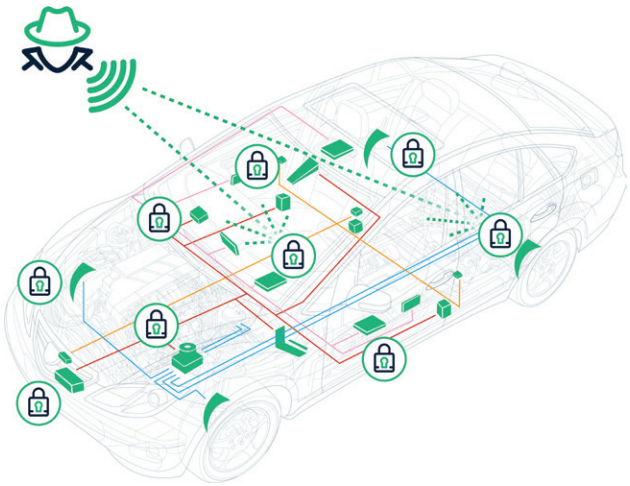


Figure 4. Securing ECUs from cyberattack by employing an embedded firewall and certificate-based authentication. Source: Sectigo.

When two devices communicate within an automotive network, the communication needs to be secure to ensure that nefarious third parties cannot listen in. It's important to verify a program or device in a way that is stringent enough in an intrinsic fashion. Authentication needs to ensure the security of the system by withstanding any attack that system is likely to encounter by verifying the identities of all incoming connections.

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.

Finally, it's up to the automotive community to prove itself trustworthy if people are to trust connected cars. Security should not be made into a competitive differentiating advantage. It needs to be a shared common resource. As this paper points out, embedded firewalls, secure communication and strong authentication techniques are vital elements that constitute a multi-layered security approach.

References

1. Robert N. Charette. "This car runs on code", IEEE Spectrum, February 2009.
2. 2020 Automotive Cybersecurity Report by Upstream Security, December 2019.
3. "Automotive cybersecurity incidents doubled in 2019, up 605% since 2016", Help Net Security, January 2020.
4. "The chaotic middle: the autonomous vehicle and disruption in automobile insurance", KPMG, June 2017, PDF.
5. United States Senate S. 2182 - Spy Car Act of 2017. www.congress.gov/bill/116th-congress/senate-bill/2182/text.
6. United States House H.R 3888 - The Self Drive Act of 2017. www.congress.gov/bill/115th-congress/house-bill/3388/text.
7. General Data Protection Regulation (GDPR) - European Union. https://gdpr.eu.
8. The Personal Information Protection and Electronics Act (PIPEA) - Canada. www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda.
9. "Parliament calls for EU regulation for access to car data." FIA Region 1, February 2018, www.fiaregion1.com/parliament-calls-eu-regulation-access-car-data.

Siemens Digital Industries Software

Headquarters
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

Americas
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

Europe
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

Asia-Pacific
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

siemens.com/software

81953-C6 2/21 H

About Siemens Digital Industries Software

Siemens Digital Industries Software is driving transformation to enable a digital enterprise where engineering, manufacturing and electronics design meet tomorrow. The Xcelerator™ portfolio, the comprehensive and integrated portfolio of software and services from Siemens Digital Industries Software, helps companies of all sizes create and leverage a comprehensive digital twin that provides organizations with new insights, opportunities and levels of automation to drive innovation. For more information on Siemens Digital Industries Software products and services, visit siemens.com/software or follow us on LinkedIn, Twitter, Facebook and Instagram. Siemens Digital Industries Software – Where today meets tomorrow.

About the authors

Dr. Ahmed Majeed Khan is an engineering leader, experienced in working with cross-functional groups to push the envelope of technology implemented in diverse automotive and consumer electronic domains. A silicon-valley veteran with a proficiency to manage onshore and off-shore development of innovative and disruptive products, he has led teams around the globe to produce several high volume, high quality system-level solutions. Currently, he holds a Senior Engineering Management position at Siemens Digital Industries Software, where he assisted in creation of a market-leading automotive-grade product portfolio. Dr. Khan is also Siemens' focal point towards international automotive software consortium, AUTOSAR. He holds a doctorate in Engineering Management from George Washington University, an MS in Electrical Engineering from Michigan State University and has over a decade of experience working with embedded systems.

Alan Grau has 30 years of experience in telecommunications and the embedded software marketplace. He is VP of IoT, Embedded Solutions at Sectigo (formerly Comodo CA), the world's largest commercial Certificate Authority and provider of purpose-built, automated PKI solutions. Alan joined Sectigo in May 2019 as part of the company's acquisition of Icon Labs, a leading provider of security software for IoT and embedded devices, where he was CTO and co-founder, as well as the architect of Icon Labs' award-winning Floodgate Firewall. He is a frequent industry speaker and blogger and holds multiple patents related to telecommunication and security. Prior to founding Icon Labs, he worked for AT&T Bell Labs and Motorola. Alan has an MS in computer science from Northwestern University.