Positioning Automotive Cybersecurity for the Future

Software-defined vehicles open up tremendous possibilities, allowing end customers to enjoy many of the very latest safety, comfort and convenience features available on the market through software updates, even as their vehicle models age. Protecting that software throughout deployment and operation is critical.

Well-structured cybersecurity management must go hand in hand with the development of software-defined vehicles. Developers must bake security into every layer, making no assumptions about the safety of a particular application or any of the supporting software.

In short, developers must manage risk, draw lessons from other industries, and push forward with comprehensive cybersecurity management systems that provide a framework for handling whatever risks come next. Working with our customers, suppliers and peers through industry organizations, Aptiv is actively helping to raise the bar.

THE SECURITY CHALLENGE

Cybersecurity is a relatively new concern for the automotive industry. As automobile manufacturers began to include electronically controlled steering and brakes in their vehicles, the risk increased, but connectivity opened the door to much more risk.

Observers often point to vehicles' direct connections to the internet as a source of risk, but they tend to overlook indirect connections, such as through a cellphone via USB or Bluetooth. Even a vehicle that otherwise does not appear to have any connectivity could have a wireless tire pressure monitoring system or an onboard diagnostic module that allows access to vehicle information.

Connectivity without robust enough security led to a widely publicized incident in 2015 in which researchers were able to remotely control certain functions of a vehicle. Despite being a painful experience for many, the incident forced the automotive industry to more deeply consider what a systematic approach to vehicle cybersecurity might look like.

Of course, other industries have had similar journeys, so security management practices from a variety of industries have helped shape the framework for automotive cybersecurity. While one might think of business IT and its high-profile ongoing defense against malware, there is a closer analog: the aerospace industry.

That industry has long supported the idea of having very sensitive code running next to less sensitive code. In fact, it classifies software by Design Assurance Level, or DAL, a risk classification system that is similar to the automotive industry's Automotive Safety Integrity Level, or ASIL.

Other industries' experience with cybersecurity provided the basis for new regulations that specify how to create a comprehensive cybersecurity management system in automotive, such as Regulation 155 (R155) from the United Nations Economic Commission for Europe (UNECE). The demand for hardware-backed security has created economies of scale in specialized microprocessors from which the automotive industry benefits. And defense-in-depth strategies developed for other industries provide a clear path for ensuring security at multiple layers throughout a vehicle.

SECURITY AT EVERY LAYER

A cybersecurity management system represents a systematic approach to defining processes and governance with security in mind — from the start of development through the maintenance of the software over time — and it allows an organization to apply that approach at every layer of the automotive system. Here are some of the key areas of focus in automotive.

Secure updates

To ensure that consumers have the most capable features and functions available, today's vehicles download software updates over the air from the cloud, and those updates must be secure.

Most people are familiar with the lock icon in their web browsers indicating that an encrypted connection has been established with a server that has been authenticated. The cryptographic verification of the code being downloaded to a vehicle follows similar principles.

Public key infrastructure (PKI) is the mechanism that allows manufacturers to digitally sign their software in such a way that the receiving system can verify its authenticity. Using a secret digital key, the manufacturer encrypts the software before making it available. When a vehicle downloads the software, it uses a different, publicly available digital key to validate the content. A complex algorithm ensures that only content signed with the secret key can be validated with the public key.

Secure boot

Even with secure update mechanisms like PKI in place, manufacturers should not assume that all software on the vehicle is harmless, because some might have gotten there by other means.

That is why manufacturers must also provide for secure boot. When a vehicle starts up, the system should verify the authenticity and integrity of software before it starts running. That is, the system must ensure that the code was made by the manufacturer rather than by an attacker.

Secure vehicle networking

As vehicles become more software-defined and complex, the many software applications running on them will use the same processors and the same networks to transfer data among various processing nodes. For example, some infotainment applications might require vehicle speed and navigational data, while other applications might need information on battery management.

Having a network within the vehicle — and a connection out to the cloud network through cellular and Wi-Fi — requires that vehicles secure those connections at multiple levels.

The lowest layer is Media Access Control Security (MACsec), which establishes a bidirectional encrypted link between two directly connected devices. MACsec can work extremely quickly, encrypting and decrypting information at line rate using specialized hardware.

The next higher layer is Internet Protocol Security (IPsec), which works at the network layer to authenticate and encrypt packets of data between network nodes with IP addresses. Using the IPsec mechanism can help protect data as it flows throughout a network — through a router, up to a cloud and so on — and not just on a physical link between two points.

Moving up the stack, manufacturers can use Transport Layer Security (TLS), which operates at the level of the network where processes communicate without being tied to IP addresses, so the security mechanism is more flexible. TLS is used pervasively in internet-based communication today, and vehicles are likely to use TLS when communicating with the cloud.

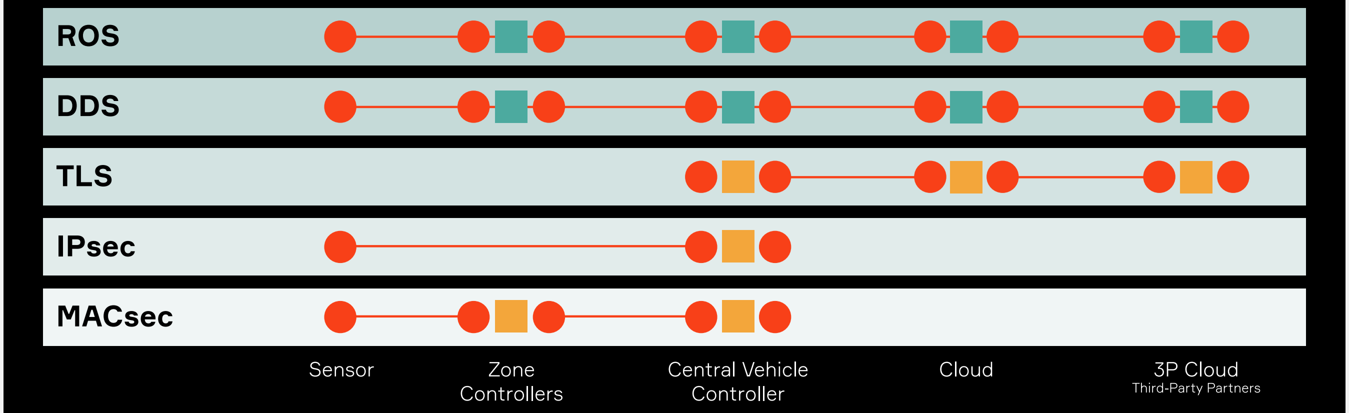
While Aptiv has implemented MACsec, IPsec and TLS in our products, we are also exploring message integrity protection — such as that found in some Data Distribution Service

LAYERS OF SECURITY

Having multiple layers of encryption in place protects data as it moves throughout a vehicle and up into the cloud.

🟩 Message authentication keeps protecting data even in storage and caching

🟧 Connection encryption lacks integrity protection in storage and caching



ROS: Robot Operating System
DDS: Data Distribution Service
TLS: Transport Layer Security
IPsec: Internet Protocol Security

implementations and in Secure Robot Operating System 2 (SROS2) — to actually bind the protection to the information. This protection can hold even as the information is cached and stored between TLS connections, and even for relays spanning many TLS connections within a vehicle and between the vehicle and clouds and smartphones.

Advanced communications

As autonomous driving becomes more common, implementing security at even higher layers for encrypting messages could become increasingly important. For example, a consumer may send a message to a vehicle requesting that it pick her up at a certain address. That message should be signed cryptographically and delivered securely. New protocols can help with this, even across multiple clouds, if necessary.

In addition, as automotive companies start to bring in more developers to build different features in software, it is becoming important to ensure noninterference among the applications by using hypervisors, containers and other technologies to keep the software separate, even on shared hardware.

A STRUCTURED APPROACH

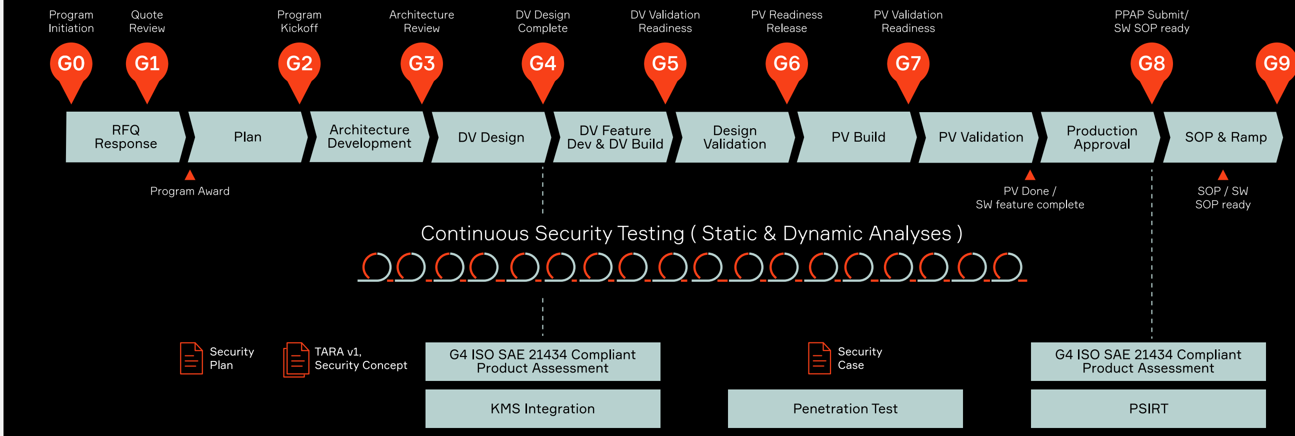
Getting all of these cybersecurity technologies in place in the right way requires structure, which can come from best practices, automated testing, audits or regulations.

The United Nations has established regulations that provide guidance for cybersecurity in the automotive industry. One is UNECE R156, which drives all of the requirements for secure update, secure boot and other technologies. The other is UNECE R155, which calls for cybersecurity management systems governing how security is engineered into vehicles and provides a framework for thinking systematically about risk to a vehicle, through a threat analysis and risk analysis.

UNECE R155 cites the international standard ISO/SAE 21434, which, among many other valuable contributions, helps set guidelines for gauging risk that are based on the feasibility of

CONTINUOUS TESTING

Security testing should be continuous throughout the development process.



Program Initiation G0
Quote Review G1
Program Kickoff G2
Architecture Review G3
DV Design Complete G4
DV Validation Readiness G5
PV Readiness Release G6
PV Validation Readiness G7
PPAP Submit/ SW SOP ready G8
G9

RFQ Response → Plan → Architecture Development → DV Design → DV Feature Dev & DV Build → Design Validation → PV Build → PV Validation → Production Approval → SOP & Ramp

Program Award
PV Done / SW feature complete
SOP / SW SOP ready

Continuous Security Testing (Static & Dynamic Analyses)

Security Plan
TARA v1, Security Concept
G4 ISO SAE 21434 Compliant Product Assessment
KMS Integration
Security Case
Penetration Test
G4 ISO SAE 21434 Compliant Product Assessment
PSIRT

an attack occurring and the potential impact if a threat were realized. The standard also introduces the concept of the cybersecurity assurance level (CAL), which can convey how critically a system must be protected from attacks.

An organization can scale its cybersecurity activities — that is, it can use more or less rigor — based on the CAL.

Automotive companies are currently preparing for the UNECE regulations to become mandatory in the European Union in mid-2024 by auditing their engineering processes to ensure that they are in compliance. Once the regulations are in effect, regular audits can ensure ongoing compliance.

Compliance is not enough, of course. Automated testing is also essential to maintaining a high level of security resilience. Aptiv has already built continuous security testing into our continuous integration and continuous deployment (CI/CD) infrastructure and is adding more forms of testing.

Aptiv uses several ways to test code as it moves through development. Static application security testing (SAST) inspects source code for flaws, and dynamic application security testing (DAST) runs simulated attacks. Going beyond SAST and DAST, fuzz testing or "fuzzing" tools can help security-test code as it matures throughout software development, instead of waiting until the end of the process when time is short on deadlines. Fuzzing covers a very wide range of potentially unexpected inputs; it generates inputs automatically and in large numbers, quickly giving developers the feedback they need, sometimes nightly, to harden their code against everything from malformed packets to random data.

NEXT STEPS

Many of the risks in automotive are not unique to one company but rather are shared by the entire industry. As automotive cybersecurity evolves, automakers and suppliers will need to speak openly about risks and work together to develop best practices to address them. They will have to share information about what is happening in the threat landscape and collaborate to recognize when threat actors might be targeting automotive. Much of that collaboration can happen through existing bodies, such as the Automotive Information Sharing & Analysis Center (Auto-ISAC).

Aptiv is proud to be very active in Auto-ISAC, and we will continue to work closely with our customers, partners and industry colleagues as we all strive to create cybersecurity management systems that enable the next generation of software-defined vehicle innovation.

ABOUT THE AUTHOR

Brian Witten
Vice President & Chief Product Security Officer

With more than 20 years of cybersecurity experience ranging from consumer electronics to military aerospace systems, Brian Witten has global responsibility for product cybersecurity at Aptiv. He oversees cybersecurity policies and processes, planning and leading the development of diverse tools and infrastructure for the company. Prior to joining Aptiv, Brian held engineering and research leadership roles at the Defense Advanced Research Projects Agency (DARPA), Symantec, United Technologies Corporation (UTC) and Raytheon Technologies, and served in the U.S. Air Force. Over the years, Brian has helped build security into millions of cars and billions of devices.