WHITE PAPER

McAfee
Together is power.

Automotive Security Best Practices

Recommendations for security and privacy in the era of the next-generation car

Table of Contents

Industry Contributors:

David Clare,
Automotive Technical Lead,
NCC Group

Shane Fry,
Security Researcher,
Star Lab Corporation

Helena Handschuh,
Technical Director, Cryptography
Research Division of Rambus

Harsh Patil,
IoT Security Engineer, LG Electronics

Chris Poulin,
Research Strategist, IBM X-Force

Dr. Armin Wasicek,
Researcher,
University of California at Berkeley

Rob Wood,
Global Hardware Lead, NCC Group

McAfee Contributors:

David A Brown
Geoffrey Cooper
Ian Gilvarry
David Grawrock
Anand Rajan
Alan Tatourian
Ramnath Venugopalan
Claire Vishik
David Wheeler
Meiyuan Zhao

Automotive Security Best Practices

Recommendations for security and privacy in the era of the next-generation car

Introduction

"Remember to lock your car" is no longer sufficient advice to protect your vehicle. United States Senator Edward Markey's Tracking & Hacking report on gaps in automotive security and privacy, as well as successful recent attacks on car computer systems from different manufacturers, are just two reminders of the increased threat to vehicle safety. Computer attacks are now a clear and present danger for car drivers, owners, dealers, manufacturers, and suppliers. Increased automation, vehicle-to-vehicle and vehicle-to-infrastructure communications, and advances in autonomous driving add computer security and data privacy to reliability and safety as cornerstones for consumer confidence and continued success in the automotive industry.

This paper is intended as an informative backgrounder and starting point for continued discussion and collaboration. The primary goal is to present the current state of automotive security, the main concerns, some use cases, and potential solutions. This is by no means an exhaustive review. This is the second version, incorporating comments from a variety of automotive and security researchers. Further comments are welcome, and the intent is an ongoing working paper as part of the Automotive Security Review Board (ASRB).

The ASRB will conduct research and collaborate on ways to improve automotive security products and technology, bringing together top security industry talent from around the world. ASRB researchers will perform security tests and audits intended to codify best practices and design recommendations for advanced cybersecurity solutions and products to benefit the automobile industry and drivers.

McAfee is part of a large and vibrant ecosystem delivering components to the automotive industry, including hardware, software, and security processes from chip to cloud and from design to driveway. A key player in the evolution of Internet security, McAfee is a long-established participant in security, standards, and threat mitigation. McAfee considers itself fortunate to be in a unique position to collaborate with the technology, security, and automotive industries to advance the analytics, research, standards, and best practices on secure driving experiences.

Computers have made significant contributions to vehicle safety, value, and functionality—from stability control to electronic fuel injection, navigation, and theft prevention. They have also increased connectivity, adding many functions common to smartphones, such as cellular data and voice functionality, web browsers, online games, and entertainment. But increases in use of

shared information and in-vehicle communication have made cars vulnerable to cyberattacks. Each electronic control unit (ECU) and the increasing array of sensors they work with must be secured in some shape or form, whether it is via cooperating or co-processors, code verification, protection of data at rest and in transit, or other capabilities that have become common in Internet security. With vehicles already connecting beyond the bumper, the risk has increased, and the core challenges will be establishing and maintaining trust, consumer confidence, and vehicle safety.

Innovation in next-generation cars

By advancing network connectivity in cars, the industry has enabled innovative functions, some of which are already available. These new functions are often referred to as "cyberphysical" features, since almost all of them require collecting data from the physical environment and cybersystems, making automotive operation decisions, and executing on such decisions with physical consequences. Some of these innovations include:

- **Advanced driver assistant systems (ADAS):** Smart lighting control, adaptive cruise control, collision avoidance, driver fatigue detection, lane departure warning, and parking assist
- **Advanced fleet management:** Usage and behavior monitoring, warranty restrictions by zone, real-time telematics, and package tracking
- **Smart transportation:** Traffic congestion, vehicle sharing, and fuel efficiency are influencing existing operating modes and creating new ones. Vehicle-to-infrastructure and vehicle-to-vehicle communications, such as smart intersections, traffic light control, road trains, and traffic management, are key contributors to smart city operations.
- **Autonomous driving:** The ultimate goal of the next generation of vehicles is that driverless cars become a reality to achieve zero fatalities and/or collisions, improved traffic flow, and other benefits, with early examples already visible from Daimler, Ford, Google, Tesla, and others.

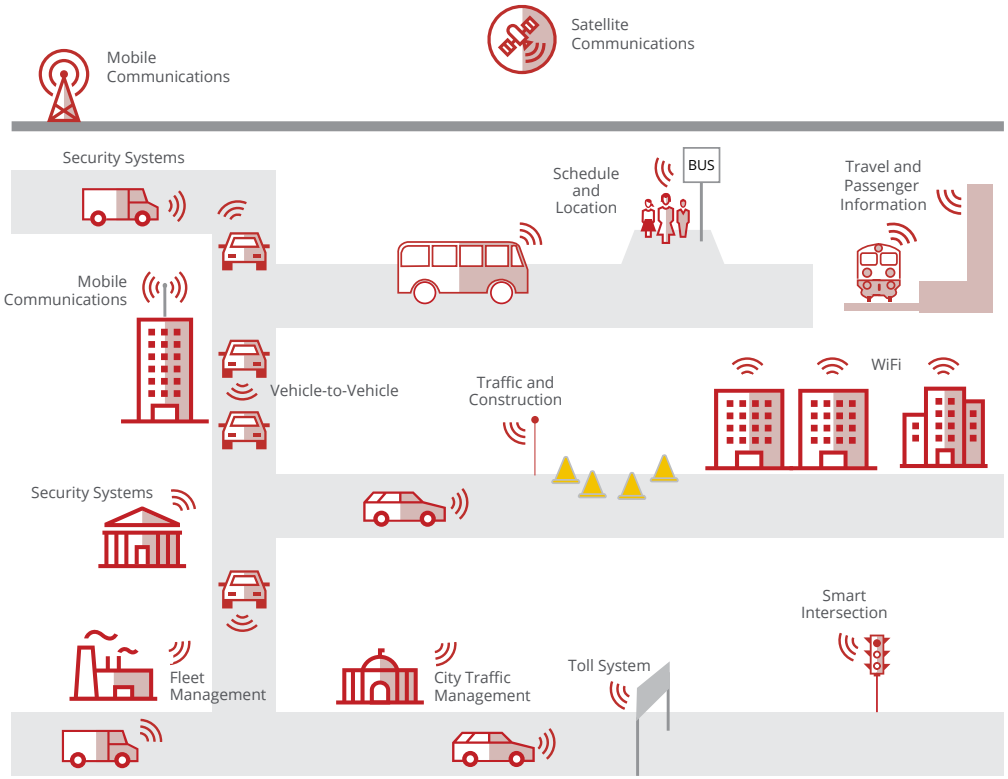

Figure 1. Ecosystem and infrastructure of the next-generation car.

Automotive innovation is driving the need for built-in security solutions and architectural design to mitigate emerging threats. The goal for automotive security products is to ensure that the new vehicle paradigm is protected and can operate to its full potential, even in a malicious operating environment.

Automotive Security: Privacy Risks and Vulnerabilities

Whenever something new connects to the Internet, it is exposed to the full force of malicious activity. When something as complex as a modern car or truck is connected, assessing the scope of threats is an immense job, and an attack surface may be left unprotected unintentionally. Many security risks now extend to vehicles—malware, Trojans, buffer overflow exploits, and privilege escalation. Let's look at a few use cases to illustrate potential threats, describe the attackers, and explore general approaches to mitigation.

With cars incorporating up to 100 ECUs, they are approaching the upper boundaries of the wiring harness, which is one reason the industry is moving towards greater integration and virtualization, reducing the total number of ECUs but increasing the number of functions and complexity of the software. The resulting attack surface is broad, touching most in-vehicle systems and an increasingly wide range of external networks, from Wi-Fi, cellular networks, and the Internet to service garages, toll roads, drive-through windows, gas stations, and a rapidly growing list of automotive and aftermarket applications.

Security for complex systems like these is a collaborative effort, requiring a holistic approach, with the involvement and contribution of the supply chain and the broader ecosystem. Effective security cannot be achieved by dealing with individual components, threats, or attack points. Unlike traditional computer systems, initiation and consequences in both the cyberworld and the physical world are possible over vehicle attack surfaces, making it more challenging to protect the vehicle's systems.

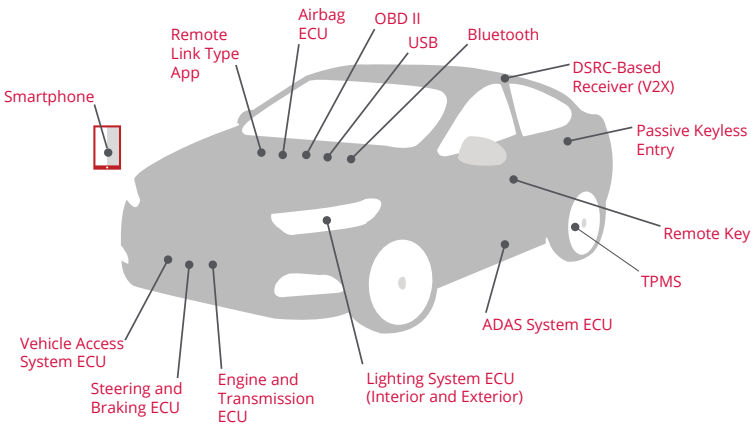

Figure 2. Fifteen of the most hackable and exposed attack surfaces on a next-generation car.

As pointed out by Miller and Valasek,[1] the success of hacking cars depends on three major categories: remote attack surfaces, cyberphysical features, and in-vehicle network architectures. They identified more than seven major categories of remote attack surfaces, based on their study of 20 recent models (2014 to 2015) from multiple different car manufacturers. Some, such as the

CAN bus and on-board diagnostics, are designed to be robust and readily available; you just have to open the hood and connect to read what is there. Furthermore, the more advanced systems features a car has, the more potential attack vectors.

Cybersecurity threat agents, models, and motivations

One of the most important steps in improving security posture, whether for a physical location or a computer system, is understanding the motivations, objectives, and actions of potential attackers or threat agents. Stronger motivations or more valuable objectives often translate to greater attack capabilities and higher risks. There is a typical progression of these actors in a newly Internet-connected market—from researchers and pranksters to owners, criminals, and nation-states. In connected systems, threats can infiltrate from outside the immediate device—in this case, from attacks, misbehavior, or failure of transportation infrastructure. Threat agents are quite diverse, but knowing who they are and modeling their behavior can help in planning the most effective mitigation strategies.

Threat information has historically been fragmented and sensationalized with a lack of standard agent definitions, which makes it difficult to quickly and consistently assess risks from specific agents. The McAfee® IT Threat Assessment Group developed a Threat Agent Library[2] and Threat Agent Risk Assessment usage model[3] to drive a standardized reference to human agents that pose threats to computer systems and other information assets.

Researchers and hobbyists

Researchers and hobbyists, sometimes funded by universities, government labs, Defense Advanced Research Projects Agency (DARPA), or the target industry, are typically the first hackers to attempt to attack a new market or device. Their motivations are usually positive, and they have considerable time and access to conduct their research. Research objectives are often meant to highlight vulnerabilities and exploits before the market hits critical mass or to demonstrate their hacking skills. The results are usually freely shared with others online and via conferences. While sharing may appear to open the door to pranksters and criminals, the benefits of open product security information and corrective action outweigh the risks. This group also has the important function of keeping the public informed about security risks in products and infrastructure and will look for any and all openings they can think of, but total coverage is restricted by their numbers and funding.

Pranksters and hacktivists

Pranksters, hacktivists, and vandals typically represent the dark side of the hobbyist group. They take the opportunity to demonstrate their skills or promote their causes, but with negative outcomes for the product owner or manufacturer. In the automotive market, the complexity of the product and requirement for special tools or skills may constrain the number of pranksters and hacktivists able to actually uncover and exploit vulnerabilities, at least until the exploits are developed and made available by criminals or nation-states with greater resources.

Owners and operators

Many car hacking tools already exist for owners, as they do for smartphones and other consumer electronics. These individuals are not criminals, but they may want to hack their own vehicles for repairs and maintenance in order to improve performance, remove restrictions imposed by the manufacturer or government regulator, or disable components to obfuscate their actions for private or fraudulent reasons. Since some automotive systems are safety-critical, tampering or modifications can also be constrained or controlled with appropriate security functions, even by owners, ensuring that the vehicle operates as intended so that the manufacturer is not subject to additional liability.

Organized crime

Organized crime has always been a threat to vehicles, and is now a significant threat actor in the cybersecurity space, and possibly ahead of researchers in their technical capability. The main motivation for this group is financial gain, so these malicious actors will be looking for ways to steal cars more easily, or otherwise separate drivers and owners from some cash. Cyberthreats often follow an evolutionary pattern, beginning with denial-of-service (DoS), followed by malware, ransomware, and attacks targeted at specific entities. In this case, DoS or disabling vehicle functions could be aimed at specific models, geographic regions, rental car companies, or other corporate fleets. Malware may follow a similar pattern, searching for valuable data to sell or use or tampering with mileage and maintenance data. Ransomware in this case could involve holding individual cars for ransom (or even an entire model or fleet) or disrupting traffic to create havoc for financial or political gain. In cybersecurity, these tools then became available to others on a Cybercrime-as-a-Service model, potentially opening up the automotive market to precise attacks against individuals, competitors, and politicians, among others.

Nation-states

The motives of nation-states are not often easy to determine. The obvious ones are industrial espionage, surveillance, and economic or physical warfare. Other motives may be intervention to assist a national manufacturer against foreign competitors. If cars are softer targets than corporate or government facilities, they could enable tracking and audio monitoring of high-value subjects. As cybercrime matures and code is shared, sophisticated code developed by well-funded nation-states finds its way into the hands of criminals and pranksters, increasing the threats.

Transportation infrastructure

Next-generation cars are not just communicating with the Internet, they are also talking to each other and to multiple parts of the transportation infrastructure. In addition to attacking the vehicle, security and safety issues can occur through attacks or misbehavior of the surrounding infrastructure. For example, traffic lights that are accidentally or intentionally set to be green in both directions, road trains that allow the cars to be too close together, or message floods that prevent delivery of vehicle-to-vehicle data in time to avoid a collision. Smart vehicles need to be able to safely manage through these and other scenarios with appropriate preemptive actions.

Example use cases

What do you do when a security issue is detected and is highly dependent on the potential short- and long-term impact to driver and passenger safety, safety of pedestrians, safety of others sharing the road, and the vehicle value? Design for safe failure and incident response plans covering all stakeholders are a critical component of successful security operations. There are multiple stakeholders interested and involved in the security issue and its outcome, including the driver, owner, manufacturer, aftermarket providers, emergency agencies, and security vendors. There is also no clear answer as to the locus of responsibility for monitoring the vehicle for security. Does it belong with the manufacturer, owner, government agency, or an aftermarket security company?

Driver

The safety of the driver, passengers, and bystanders is obviously the most important consideration when a vehicle security incident is detected. Determining when and how a vehicle will fail, deciding when and whether to update code, and determining which features to disable for a failsafe mode so that the vehicle and occupants are protected and can safely get home or to a safe stop are paramount. Once that is completed, the next step in incident response is to remediate or correct the situation: this may be automatic or may require explicit interaction by the owner and manufacturer. It is important to remember that vehicles have multiple drivers, who may not be related or even know each other in situations like car sharing or rentals.

Owner

Owners of computers are painfully familiar with security patches and software update processes. Interrupting a drive for a weekly security scan or urgent update is not realistic, especially since the owner may or may not be drivers of the vehicle. Forcing a patch at the wrong time may be dangerous to the vehicle occupants. Processes will need to be developed to determine when and how to inform the owner that an update is required, how and when to enforce the update, and how to deal with unpatched systems. Memory monitoring and anomaly warning solutions that model the normal operation of the vehicle and create a unique fingerprint are possible. Significant deviation from the model can trigger alerts and even a safe mode with sufficient but diminished functions to enable the car to get home.

Manufacturer

The vehicle manufacturer needs to gather information on all security events but can be overwhelmed by the sheer volume of alerts and the complexity of multiple tiers of suppliers. Automotive security operations will need special tools to deal with this volume and correlate real threats from noise and distinguish legitimate owner or driver hacks from warranty-voiding ones. Like other large-scale software update processes, the automobile maker's servers will need to be protected from tampering and disruption, connections must be secured from the cloud to the vehicle endpoint, and updates need to be signed, validated, and re-verified after installation. Over-the-air updates, after appropriate testing and experience, could improve security response

times and significantly reduce update or recall costs, but they can also introduce some increased risk.

Aftermarket

App stores, aftermarket components, and service shops are a major source of revenue for the auto industry, as they are for many consumer electronics. Security is affected by decisions regarding if, when, and how to allow these groups to interface with the electronic vehicle systems. Closed or walled garden systems are increasing in popularity by computer vendors as they increase control and reduce risk, but at the risk of consumer backlash. On the other hand, aftermarket companies may be the first to identify vulnerabilities or security breaches, and sharing information throughout the ecosystem has proven to be an important part of effective incident response and recovery.

Dealer

Dealers are often the main interface between the manufacturer, the aftermarket, and the owners. Before over-the-air systems are ubiquitous, dealers will provide essential software patching functions on behalf of manufacturers. Dealers may also be the interface to some types of aftermarket software products, as they are today for roof racks, backup cameras, and other add-ons. If vehicle security moves towards third-party security vendors, similar to the way antivirus companies provide PC security, dealers might have an important part to play in education, sales, and provisioning of these products.

Emergency agency

As manufacturers of safety-critical systems, the automotive industry is subject to regulation and oversight by various levels of government. When and how to inform the appropriate agencies of a security breach or exploit may be regulated or self-imposed, but, either way, it is an important part of incident response. Increasing information sharing with national and international agencies is becoming more common, as the Internet and threat vectors are largely independent of national borders.

Security vendor

Security vendors play an interesting role in the ecosystem of secure computing products. In addition to supplying components, the leaders have labs and research teams, working to uncover and protect against new attacks and vulnerabilities before they become a significant threat. Sharing threat intelligence with these companies helps reduce the attack surface, improve incident response, and contain the spread of a cyberattack or infection as security vendors rapidly redistribute the information to other potentially affected organizations.

Data privacy and anonymity

Personally identifiable information (PII), such as location data, address books, and credit card numbers, is now entering and leaving the confines of the vehicle, requiring appropriate privacy controls and anonymization of data. As automakers and third-parties

create a seamless experience and increase the level of vehicle personalization, cars are becoming an extension of, or adjunct to, smartphones, home automation systems, entertainment libraries, and other components of the digital life, syncing and storing user data.

Data privacy has two aspects: confidentiality of personal data and leaking of data outside the consumer's control. To maintain confidentiality, data needs to be protected by encryption inside and outside the vehicle while it is stored, while it is transmitted, and by memory protection extensions while it is being processed. Cybercriminals have been known to attack and steal data in all three locations. This includes not only stored personal information, such as address books or credit cards, but also style of driving, current location, previous destinations, and other metadata. For data leakage, there is a need to justify what data is stored, secure storage of data, destruction of data upon consumption, and protection against unauthorized access to ensure compliance with information privacy laws.

There are a few steps to improve data privacy. The first is to minimize the amount of personal data that is stored, erring on the side of storing too little rather than too much. The next step is to be transparent about what is collected, how it is used, and what is stored. Only data that can be reasonably assumed to be necessary for the service should be collected without a specific opt-in function. Finally, drivers and owners should have a clear way to securely delete any stored personal data or ensure that it is not saved. This is especially important in an era of increased vehicle sharing, as well as rentals, loaners, and other temporary usage scenarios.

Designing Secure Automotive Systems

Now that we have reviewed some potential threats and vulnerabilities, the next issue is designing secure automotive systems. While the automotive security field is relatively recent, there are strong technologies and expertise in adjacent industries to be leveraged and adapted. Developers can take advantage of existing secure development processes to incorporate security and privacy into their new vehicles by design.

There is a strong relationship between cybersecurity for automotive safety. SAE has captured this very well in their J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems.[4] To paraphrase, system safety is concerned with protecting against harm to life, property, or the environment. System cybersecurity aims to prevent financial, operational, privacy, or safety losses. So all safety critical systems are security critical, but there may be systems, such as entertainment systems, that are security critical but not safety critical.

The organizational disciplines that lead to safe and reliable cars also apply to security. In particular, safety, reliability, security, and privacy must all start at the outset of the design phase. To ensure a secure design, a threat model for the vehicle should anticipate different kinds of threats and seeks to mitigate them. While the safety designer is adding in crumple zones, airbags, proximity detection, and automatic braking systems, the security designer is also building in layers of protection, seeking to isolate a threat before it can affect vehicle operations. The vehicle security architect has a collection of security tools to choose from—

ranging from encryption of critical or private data to isolation of software components by function—and can combine hardware and software functions as needed to meet cost and performance goals. Perhaps the most important safeguard, which is different from commercial computers, is the ability of systems to protect vehicle operations, as well as data and processes.

Software engineering approaches and cycles in the auto industry have typically been different from corporate and PC processes, with longer time scales and little or no update or patching capability. There is a substantial legacy of control systems and networks on a car, with each system historically dedicated and independent. At one time, the complexity of automotive systems might have been a barrier to entry for hackers, but that is no longer the case. Hackers are more sophisticated and may be part of criminal or nation-state groups with significant skills and funding. In addition, specifications for most chips and operating systems are readily available on the Internet due to increased technology standardization and proliferation. As a result, as vehicle systems consolidate and interconnect, security design has to be intentional and proactive. Applying best known practices and lessons learned in the computer industry will be helpful as vehicles become increasingly connected.

Other industries and market segments, such as defense, aerospace, and industrial machines, provide opportunities to adapt and cross-pollinate many of the foundational principles, lessons learned, and processes developed over the past decades in cybersecurity. For example, auto manufacturers could implement a distributed security architecture, exhibiting defense-in-depth, analogous to the layers of protection analysis (LOPA) methodology used for safety and risk reduction. Securing systems from the hardware to the cloud, with identified best practices and technologies for each discrete building block, would provide comprehensive, end-to-end protection.

Realizing these protections in actual vehicle systems requires coordinated design of multiple security technologies, such as isolation of safety critical systems, secure boot, trusted execution environments, tamper protection, message and device authentication, data encryption, data anonymization, behavioral monitoring, anomaly detection, and shared threat intelligence.

Distributed security architecture

Automotive computer security is a collaborative approach of defenses to detect, protect, and correct identifiable or avoidable threats and to protect from previously unknown or unavoidable ones. With next-generation cars, these layers include hardware-based protection in and around the ECUs, software-based in-vehicle defenses, network monitoring and enforcement inside and outside the vehicle, cloud security services, and appropriate data privacy and anonymity for bumper-to-cloud protection. The key tenets of data privacy and anonymity must be safeguarded while ensuring the security of the automobile. Users must also be educated about secure usage of the systems and potential threats. For example, if they sync their phones to a rental or shared vehicle, which may copy all of their contacts and location data, they must remember to disconnect and delete the data when they return their cars.

Security defense-in-depth consists of three layers: hardware security modules, hardware services, and software security services. Hardware security protects the ECU as a security enabler and enforcer. Its primary responsibilities are: secure boot to bring the environment to the initial trusted state, secure storage of keys, and a trusted execution environment.

Hardware security services build on top of hardware security and provide fast cryptographic performance, immutable device identification, message authentication, and execution isolation.

Software security services enhance security capabilities on top of the hardware with network enforcement, whitelists/blacklists, anomaly detection, cryptographic services, biometrics, secure over-the-air updates, and upgrade capabilities, all delivered over the life of the car.

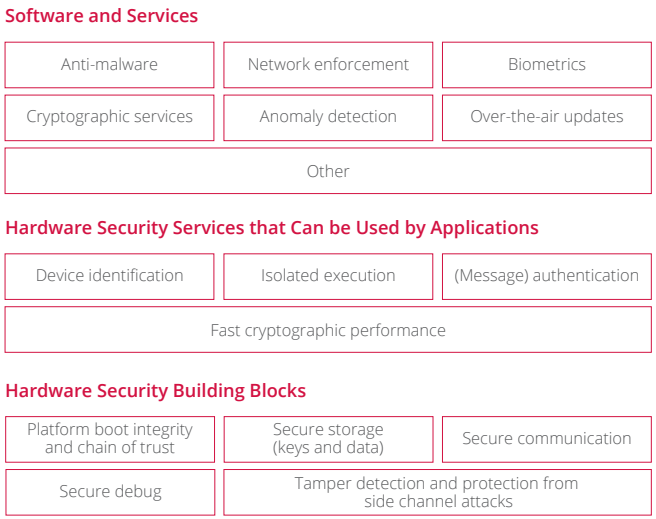

Figure 3. Defense-in-depth building blocks.

Hardware security

Hardware security systems are like the physical protection systems on a car—the engine firewall, seatbelts, and airbags. They are there to protect the operating components from intentional or accidental damage. There is a wide range of hardware security building blocks available from the computer security industry that help secure the ECUs and buses. These include:

- **Secure boot and software attestation functions:** Detects tampering with boot loaders and critical operating system files by checking their digital signatures and product keys. Invalid files are blocked from running before they can attack or infect the system, giving an ECU its trust foundation when operating.
- **Trusted execution technology, such as the trusted processor module:** Uses cryptographic techniques to create a unique identifier for each approved component, enabling an accurate comparison of the elements of a startup environment against a known good source and arresting the launch of code that does not match.
- **Tamper protection:** Encrypts encryption keys, intellectual property, account credentials, and other valuable information at compile time and decrypts only during a small execution window, protecting the information from reverse engineering and monitoring for tampering attempts.

- **Cryptographic acceleration:** Offloads encryption workloads to optimized hardware, improving cryptographic performance and making it easier to broadly incorporate symmetric or public key encryption into applications and communications processes.
- **Active memory protection:** Reduces code vulnerabilities by embedding pointer-checking functionality into hardware to prevent buffer overflow conditions that may be exploited by malicious code.
- **Device identity directly on the device:** Enables manufacturers to know the unique identity of every device, enabling secure identification and preventing unapproved devices from accessing the manufacturer's network or systems. Technologies such as Intel EPID (Enhanced Privacy ID), which may be built into processors from Intel and others, also protects anonymity by allowing devices to be verified as part of a group instead of by their unique identity.

Software security

Automotive networks and control units used to be difficult for hackers to reach, only accessible by direct physical contact inside the car.[5] Now, a determined attacker with time and money can break into these systems with little or no physical access. If automotive attackers evolve towards larger and more sophisticated organizations, as Internet attackers have, this may become the norm.

In addition, the proliferation of ECUs linked by common protocols has increased the attack surface and has made vehicles more accessible to attackers. There are many ECUs with different capabilities in a vehicle. It is difficult or impossible to add hardware security capabilities to some of them, so co-operating processors and software-based security are also needed. Architectural techniques and software technologies that can defend the vehicle include:

- **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.
- **Partitioned operating systems:** A commonly used software and hardware combination that isolates different processes or functions, such as externally facing functions from those that drive the vehicle, reducing the complexity of consolidating multiple systems onto a single ECU. Techniques, including virtualization and software containers, make it possible to update or replace individual functions without affecting overall operation, or mirror functions for redundancy and fast fail-over.
- **Authentication:** Authentication by a physical key for unlocking doors and starting the engine is no longer sufficient and is being augmented by software, as cars offer personalized services across multiple functions and profiles. Electronic keys, passwords, and biometrics need to be managed and authorized to access personal information, such as identity, telemetry, locations, and financial transactions. Similarly, the various ECUs in a vehicle need to authenticate communication to prevent an attacker from faking messages or commands.

- **Enforcement of approved and appropriate behavior:** It is very common for cyberattacks to try to jump from one system to another or send messages from a compromised component to an uncompromised one. Preventing this network activity is a key to detecting and correcting accidental or malicious threats. These functions can also prevent multicar attacks on an entire series of cars or snowball effects from cascading error propagation.

Network security

With in-vehicle networks carrying a mix of operational and personally identifiable information—such as location, navigation history, call history, microphone recordings—protecting messages and data over the communication bus is critical for operational security, privacy, and consumer trust. Common protocols, such as controller area network (CAN), local interconnect network (LIN), media-oriented systems transport (MOST), FlexRay, automotive Ethernet, Bluetooth, Wi-Fi, and mobile 5G—and newly proposed protocols, like dedicated short-range communications (DSRC)—amplify the threat, as they increase attack vectors. Replacing unsecured legacy protocols with common protocols makes it possible to leverage good security techniques that have been developed in the computer industry. Security-enhanced ECUs can interact with security-enhanced networking protocols (in-vehicle or external) to enhance authenticity, reliability, and integrity of the transmitted data. Hardware-assisted technologies that help to secure networks without significantly impeding performance, latency, or real-time response include:

- **Message and device authentication:** Verifies that communications are coming from an approved source and protects authentications from being spoofed or recorded and replayed.
- **Enforcement of predictably holistic behavior of all systems:** Restricts network communications to predefined normal behavior and constrains abnormal types or volumes of messages so that they do not impair the vehicle's functions.
- **Access controls:** Explicitly permit communications and messages only between pre-approved systems and sensors, block unapproved and inappropriate messages, and alert security systems about any invalid attempts. Manufacturers, maintenance organizations, owners, drivers, and even police and insurance companies will have different access rights to the car's information systems that need to be authorized and controlled.

Cloud security services

While embedded vehicle security is essential, some additional security services require real-time intelligence and updates, so the systems need to be able to connect to cloud-based security services in order to detect and correct threats before they get to the car. These include:

- **Secure authenticated channel to the cloud:** Leverages hardware-assisted cryptography for remote monitoring, software updates, and other communications. Data protection technology secures data throughout the transaction.

- **Remote monitoring of vehicle activity**: Includes appropriate privacy constraints to help detect anomalous behavior and misbehaving vehicles and filter out and remove malware.
- **Threat intelligence exchanges**: Collaboration among dealers, manufacturers, and government agencies to quickly propagate warnings and remediation of zero-day exploits and new malware to the vehicle, containing the spread of an attack and retroactively identifying and correcting previously infected ones.
- **Over-the-air updates:** Used for firmware (FOTA) and software (SOTA) updates and work well for smartphones and other consumer and business electronics. With appropriate user controls and safety precautions, these are vital to get systems updated quickly when a breach or vulnerability is discovered and substantially reduce the cost of recalls.
- **Credential management:** The online component of vehicle, owner, and driver authentication, providing easy and secure management of user profiles and account information, federated identities, and associated cryptographic keys and services. Security of credentials is critical to data privacy.

Taking Advantage of Security Standards and Best Practices

Standards and industry best practices, developed in automotive and related fields, can contribute to more secure automotive environments. Automotive and cybersecurity ecosystems need to engage in discussion and development of best practices for designing, developing, and deploying security solutions. The two systems need to understand the difference between safety and security. Automotive safety is a probabilistic science with measured and identified risks and components built to mitigate those risks. Production practices and repair practices give customers confidence that the safety mechanisms are in place and operating correctly. Computer security is not probabilistic. Threats come from a variety of sources, including intentionally malicious and unintentionally malignant. The goal of security therefore is to mitigate threats both before they occur and after they happen. The security landscape has to mitigate these threats over the entire lifecycle of the product, from early design decisions through manufacturing to operation and decommissioning.

Security development lifecycle

A security development lifecycle (SDL) is a framework that allows the product developer to deal with the identification of appropriate threats, use mechanisms to mitigate the threats, implement processes to manufacture the product, understand how to handle exploits in the field, and fold in learnings for future products. Vehicle development is no different, and hence the use of a defined SDL can greatly enhance the threats mitigated and ability to inform users and customers of the product security goals. SDL frameworks, such as ISO/IEC 27034, define the control points that help ensure that development, testing, manufacturing, delivery, and operation all properly combine to mitigate the identified threats.

The SDL focuses on two main issues: identification of product threats and assurance of proper product creation. If the product developer is unable to prove a

negative, which affirms that there is nothing "bad" in the product, the developer must point to adherence to their SDL process to provide confidence that the product delivered follows the product design. These processes include architectural reviews, coding standards, code reviews, internal and external functional validation, internal and external security testing, and component and system-level penetration testing. The exact mix of all of these processes will be product specific and in line with the identified threats. The SDL process should include various checkpoints, where the assumptions and threats undergo a review to ensure that the product is still meeting the needs of a changing environment.

One definition of a secure product is that the product does exactly what the design says, no more and no less. Testing for doing less is functional testing: the product performs the identified function, or it does not. Testing for doing more is security testing. When there is additional functionality that is not in the design, it may or may not work correctly. At the very least, additional functionality represents an attack surface that malicious entities may take advantage of. The security validation strategy, therefore, is an attempt to find those additional functionalities. The strategy will involve reviews, defined tests, and penetration testing.

Known vulnerabilities represent threats successfully exploited in the past. Known vulnerabilities include such items as buffer overflows, side channel analysis, and a host of others. Developers should include in their testing strategies tools that help identify the presence of known vulnerabilities. These tools include fuzzing and glitching, along with various compiler options. Vehicle-specific vulnerabilities, along with attack behaviors, are the focus of SAE J3061, which a developer must take into account. Product-specific vulnerabilities discovered by the team or from experiences with shipping products should help drive the testing strategies for the next or related versions of the product.

Most SDL frameworks include privacy considerations. The SDL process, with its identification of assets, is a natural process to deal with potential privacy issues. The privacy reviews, therefore, become an integral component of the full SDL process.

The SDL depends on an accurate reflection of the current threat landscape. Failure to mitigate known threats leaves the product vulnerable the minute it ships. The coordination of known vulnerabilities is a process globally coordinated by the Computer Emergency Response Teams (CERT) on both national and industry boundaries. As the products in use by the vehicle are likely generic, knowledge of the complete threat landscape is critical for the vehicle developer. The Alliance of Automobile Manufacturers, in collaboration with global automakers, established the Information Sharing and Analysis Center (ISAC) to serve as a central hub for intelligence and analysis. By providing timely sharing of cyberthreat information relative to vehicle electronics and software, the ISAC will assist developers in responding to the changing threat landscape.

Supply chain security

No electronic product today is created by a single company. Hardware and software components, development tools, manufacturing, product assembly, and verification testing may all be provided by one or more suppliers. Counterfeiting of electronic parts and components is a big problem in the automotive industry, with significant product security implications. Supplier quality engineers are a common role in the automotive industry, and supplier security engineers may soon join their ranks. Cost of security will likely join cost of quality in the decision-making process.

Detecting and avoiding infiltration of tainted or counterfeit parts is necessary to maintain the trust and integrity of the security architecture. More specifically, it is necessary to prevent well-funded criminal or nation-state groups from gaining physical access to hardware used in the car. Known best practices to protect supply chains include:

- **Authorized distribution channels:** Used for procurement of all hardware and software used to build and maintain the car.
- **Track and trace:** Detects critical components and parts involved with security and safety systems.
- **Continuity of supply:** Plans for spares and maintenance parts, and includes a long-term parts availability policy.

Suppliers should follow secure development processes or have SDL details mandated in their contracts that need to be audited and verified at appropriate intervals.

Supply chain risk management encompasses both the inbound and outbound supply chains. The four distinct operations include:

- **Inbound functional descriptions:** The logical design process
- **Inbound materials:** The physical ingredients and functions used to make the ICs
- **Manufacturing processes:** Risks arising during the manufacturing process
- **Outbound finished goods:** Outbound risks, including freight theft, tampering, false description, product substitution, and counterfeiting

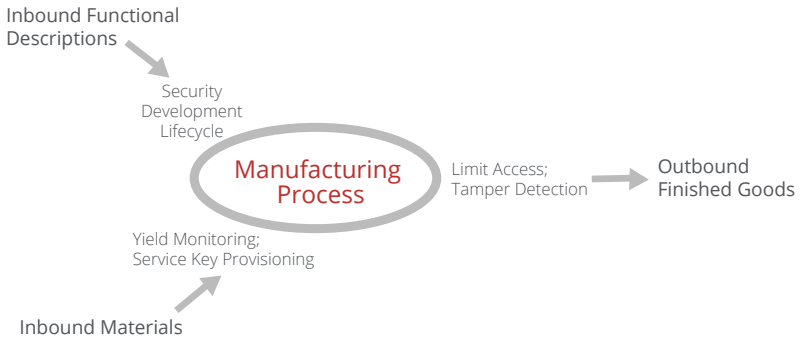

Figure 4. Supply chain risk management.

From a cybersecurity point of view, each operational area has different priorities with distinct risk mitigation controls. The primary inbound threat of tainted or counterfeit materials is mitigated by rigorous tracking of when and where each batch of material is consumed during manufacturing. Correlating yield

and performance measurements with batch identity will detect unauthorized substitution of ingredients that impact yield. Inbound functional descriptions are protected as part of the security development lifecycle.

Manufacturing processes for integrated circuits are protected by the combination of yield and performance monitoring, and the conversion of functional descriptions into wafer mask sets. Attacks through the manufacturing process are difficult, prompting adversaries to look for the weakest links, which may be the software development tools and provisioning of encryption keys. In the development stage, the lower level the tool, the more access it typically has, and many tools hold all of the necessary passwords in the software to make work faster and easier for engineers. If you can get ahold of the lowest level tool, you can break into almost anything. Key provisioning is another vulnerability; if you can capture the keys, you have privileged access without affecting the product in a detectable way. These keys must be protected and inserted securely, with appropriate key hierarchies, delegation of appropriate rights to different groups, and two-step key provisioning, one at the fabrication location and one at the assembly plant.

Cloning of integrated circuits (ICs) is an emerging attack that was reported in detail at the 2015 "Surface Mount Technology Association/Center for Advanced Life Cycle Engineering" workshop on mitigating risk of counterfeit electronic parts. Cloned ICs enable injection of malicious functions into an apparently trustworthy part. Cloned parts are difficult to detect using only visual and electrical testing. If the incoming inspection is only looking for expected and documented functions, a cloned IC that implements more than the expected functions will not be detected.

Outbound finished goods are also at risk of theft and counterfeiting. Protocols that limit unauthorized physical access to finished goods and technologies that detect tampering or modification of device identity are the dominant outbound risk mitigation controls.

Each operational area should do ongoing risk assessments independently from the others and implement controls appropriate to local operations. However, it is recommended that each area also invite peer reviews by representatives from other operations to enable coordination among functions and to promote sharing of best practices.

Leveraging standards

The point of standardization is for the developer to show compliance to the standard. The belief is that when a product follows the standard, particular properties are present. Security, and vehicle security in particular, is no different from any other industry—there are many standards from a wide range of providers. A very incomplete list would include International Standards Organization (ISO), International Electrotechnical Commission (IEC), Institute of Electrical and Electronics Engineers (IEEE), Internet Engineering Task Force (IETF), Trusted Computing Group (TCG), Society of Automotive Engineers International (SAE), MISRA C, and CERT C. In addition to the global standards, there are numerous country-specific standards and regulations. Not surprisingly, with so many different organizations

creating standards, some of the standards overlap. The overlaps sometimes are complementary, and sometimes they are in conflict. A vehicle developer will need to make conscious decisions as to what standards they will prioritize over others when conflicts are present.

While vehicle development forces a merger of security and safety, many of the standards cross industry and device boundaries. For instance, the standards that relate to the SDL are applicable to all industries and not just vehicle development. To illustrate the gamut of standards, the following lists show the depth and breadth of available standards.

The partial list of ISO/IEC standards includes:

- **ISO/IEC 9797-1:** Security techniques – Message Authentication Codes
- **ISO/IEC 11889:** Trusted Platform Module
- **ISO 12207:** Systems and software engineering – Software life cycle processes
- **ISO 15408**: Evaluation criteria for IT security
- **ISO 26262:** Functional safety for road vehicles
- **ISO 27001:** Information Security Management System
- **ISO 27002:** Code of Practice – Security
- **ISO 27018:** Code of Practice – Handling PII / SPI (Privacy)
- **ISO 27034:** Application security techniques
- **ISO 29101:** Privacy architecture framework
- **ISO 29119:** Software testing standard
- **IEC 62443:** Industrial Network and System Security

Some of the standards that SAE International is working on or has published include:

- **J2945:** Dedicated Short Range Communication (DSRC) Minimum Performance Requirements
- **J3061:** Cybersecurity Guidebook for Cyber-Physical Vehicle Systems
- **J3101:** Requirements for Hardware-Protected Security for Ground Vehicle Applications

Examples of other industry and government security initiatives include:

- **E-safety Vehicle Intrusion Protected Applications (EVITA):** Co-funded by the European Commission, it is an architecture for secure on-board automotive networks, with a focus on protecting components from compromise due to tampering or other faults.
- **Trusted Platform Module (TPM):** Written by the TCG and standardized as ISO/IEC 11889, it defines roots of trust that enable many of the key attestation activities that are mandatory on a vehicle. The TCG recently released a TPM specification focusing on secure automotive data and operations.
- **Global Platform:** A member-driven association, this group defines and develops specifications for secure deployment and management of secure chip technology.
- **Secure Hardware Extensions (SHE):** From the German OEM consortium Hersteller Initiative Software (HIS), these on-chip extensions provide a set of cryptographic services to the application layer and isolate the keys.

While the previous list is quite large, it barely covers the range of available standards and specifications. Additional industries, while not directly related to automotive, are also creating standards and specifications that can assist the vehicle developer. These industries include military, aerospace, aviation, and critical infrastructure. One example is the US Federal Aviation Administration (FAA), which recently developed an advisory circular that provides advice for airlines implementing cybersecurity for their e-enabled aircraft.

Given the wide variety of these standards and regulations, it is impossible to choose a single canonical set that meets the needs of every product. The developer needs to identify the target market and determine the prioritization of the standards in that market. After determining the prioritization, the developer will then have to rationalize any conflicting requirements.

Operating securely for the full lifecycle

While robust vehicle security starts at the beginning of the design phase, the entire vehicle lifecycle requires security thought and actions. Design, implementation, manufacturing, distribution, operation, maintenance, recovery, and retirement all require attention to security issues. Attackers can and will attempt to modify vehicle hardware and software at every phase of this lifecycle. The security of the system must also anticipate that owners, maintainers, and users may all perform operations that were unanticipated in the original security design. Resilience on the security operations and the ability to recover from loss of hardware or software integrity are crucial aspects of the vehicle design.

It is likely, due to Right to Repair acts and other types of legislation and industry activities, that the methods in use to secure vehicle hardware and software will be widely known. It is a long-held security principle that the attacker knows your mechanism. In light of this, it is imperative that vehicle security depends on cryptography with appropriate key sizes. The provisioning of the key material must be a supply chain consideration, along with potential recovery mechanisms in the event of key material compromise.

Cryptographic key strength in light of the expected 15-year vehicle lifetime will require deep security analysis. The expectation that the key material will remain confidential over the 15-year period, with multiple vehicle owners and numerous trips for maintenance, is a driver for a conservative approach to key size.

It is inevitable that over a 15-year lifetime there will be a need to recover from an attack or other loss of integrity with the vehicle software and hardware. The recovery mechanisms must engender customer trust and confidence such that recovery is possible in any lifecycle phase. The vehicle provider anticipation includes the creation of detailed incident response plans in the event of a loss of vehicle integrity. It is critical to note that loss of vehicle integrity is not just a result of active malicious activity, but can also occur through natural disasters, mistakes in the supply chain, errors in hardware and software, and an unlimited number of other sources. It

is not possible that the security analysis done today will anticipate new types of attacks and techniques that will be possible in 15 years. Therefore, the vehicle recovery mechanisms must be inherent in the vehicle design and not added on just prior to shipment.

Another inevitability over the 15-year lifetime is the need to replace vehicle parts. The ability to maintain a security boundary, when adding new parts is a crucial aspect of the recovery mechanism. Not all parts will directly affect the security functionality, but the customer has to have confidence that changing brake pads will not affect the security of the vehicle. Maintaining the software, both functional and security focused, is a new lifecycle challenge. One of longest supported software products was Microsoft Windows XP with support ending after 12 and half years. In that period there were more than 100 updates, or, on average, about one per month. This update frequency is vastly different from most car maintenance interactions. The ability to update the software, through some public network, further drives the need for secure maintenance and recovery mechanisms. It is likely that the incident response plans will require mechanisms to respond, potentially in a matter of hours or days, to an active threat.

Also inherent in the security mechanisms will be the security policies to deal with jail breaking, removal of tamper protections, forcing upgrades, preventing downgrades, and controlling or limiting owner and driver modifications. The security mechanisms must have the ability to enforce the policies along with provisions to update securely the policies.

Open Questions

This paper has some of the security and privacy issues in the next-generation car and has demonstrated that a potential recipe for success includes:

- Protecting every ECU, even for tiny sensors
- Protecting functions that require multi-ECU interactions and data exchange
- Protecting data in/out of vehicular systems
- Protecting privacy of personal information
- Integrating safety, security, and usability goals
- Dealing with the full lifecycle of vehicular and transportation systems

There are many open questions in this field. In the future, cars may not get a “Check Security” light or “Hack Test Rating.” An “Update Software” light may well be a future reality. McAfee has established technology leadership in all these areas and is actively engaging with standards organizations and ecosystems to address unique challenges for next-generation vehicles.

Best practices for automotive security are an evolution and amalgamation of both product safety and computer security. Together, industry leaders McAfee and Wind River supply many of the key security ingredients for the automotive industry. This puts the companies in an excellent position to collaborate with all parties to research, develop, and enhance products, services, and best practices for a more secure driving experience. Together, the goals of trusted vehicles, secure cars, and a confident user experience are achievable.

Comments on this document and related issues are welcome and encouraged and will be incorporated into future versions.

McAfee Resources

McAfee is involved in the development and implementation of computing and consumer electronics standards and works with more than 250 standards and industry groups worldwide to pursue the latest technological advances, including industry alliances, regional standards organizations, international industry standards groups and formal international standards bodies.

For additional information on standards activities at McAfee, see:

- Enabling a Global Infrastructure for Products and Services
- McAfee Standards—Computing and Consumer Electronics Standards
- Technology Standards—McAfee National and International Standards

1. C. Miller and C. Valasek. A survey of remote automotive attack surfaces. In *BlackHat USA*, 2014.
2. Casey, T. Threat agent library helps identify security risks. https://communities.intel.com/servlet/JiveServlet/downloadBody/1151-102-1-1111/Threat Agent Library_07-2202w.pdf. Intel Corp. 2007
3. Rosenquist, M. Prioritizing Information Security Risks with Threat Agent Risk Assessment. https://communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf. Intel Corp. 2009
4. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. http://standards.sae.org/j3061_201601/. SAE International. 2016
5. S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno. 2011. Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association, Berkeley, CA, USA, 6-6.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com