White Paper

Automotive Security Best Practices

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

intel Security

Contributors:
David A Brown
Geoffrey Cooper
Ian Gilvarry
Anand Rajan
Alan Tatourian
Ramnath Venugopalan
David Wheeler
Meiyuan Zhao

Table of Contents

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 examples of the increased threat. Computer attacks are now a clear and present danger for car users, dealers, manufacturers, and suppliers. Computer security joins reliability and safety as a cornerstone for consumer confidence and continued success in the automotive industry.

Intel 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 computers as Internet security emerged, Intel is a long-established participant in security, standards, and threat mitigation. Intel 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.

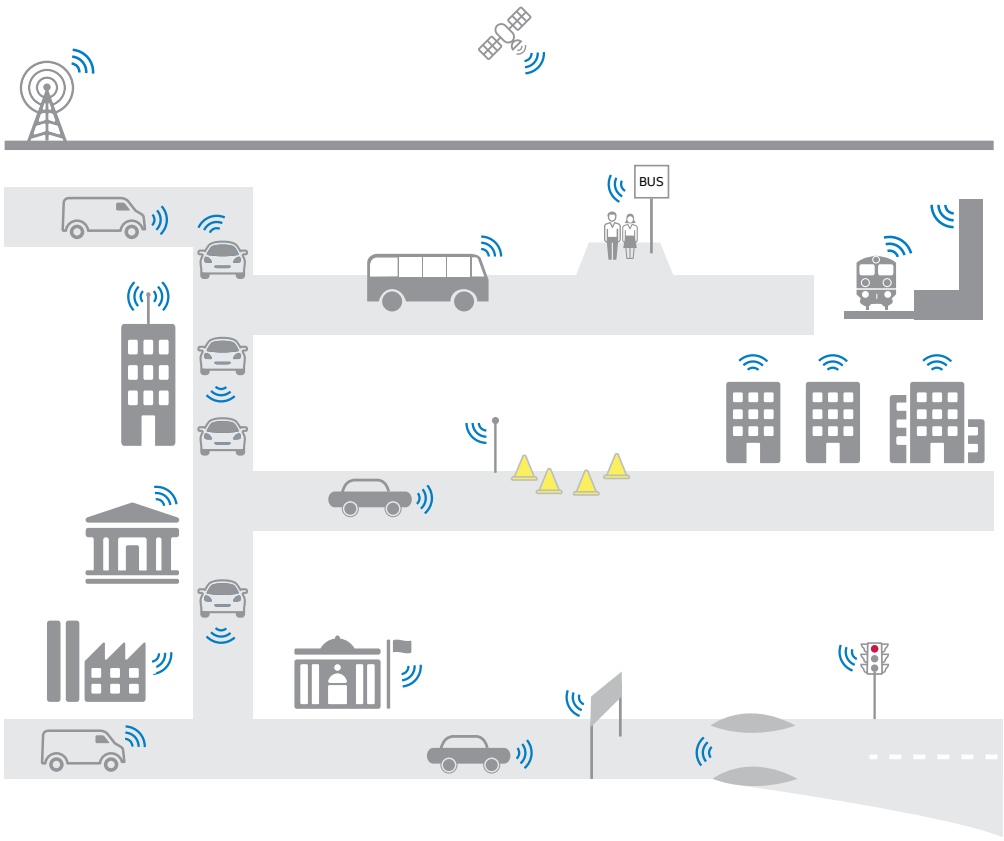

Figure 1. Ecosystem and infrastructure of the next-generation car.

Computers have made significant contributions to vehicle safety, value, and functionality—from stability control to electronic fuel injection, navigation, and theft prevention. Since these systems increasingly rely on shared information and in-vehicle communication, they are at risk from cyberattacks. They have also increased connectivity, adding many functions common to smartphones, such as cellular data and voice functionality, web browsers, online games, and entertainment. This increase in connections opens up new attack surfaces, further underscoring the need for robust security solutions, especially as connected and even driverless cars emerge and evolve. Each electronic control unit (ECU) 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. As vehicles start to connect beyond the bumper, the risk increases exponentially, and the core challenge will be establishing and maintaining trust and consumer confidence.

Emerging next-generation car usages

By introducing networking to cars, the industry has enabled exciting new usages. Some preliminary versions are already in new models. These new usages are often referred to as cyberphysical features, since almost all of them require collection of data from physical environment and cybersystems, making automotive operation decisions, and executing on such decisions with physical consequences. Some example usages include:

- **Advanced driver assistant systems (ADAS)**: Smart lighting control, adaptive cruise control, lane departure warning, and parking assist.
- **Advanced fleet management**: Real-time telematics, driver fatigue detection, and package tracking.
- **Smart transportation**: Vehicle-to-infrastructure communications, such as smart intersection, traffic light control, collision avoidance, and traffic management. This type of usage often involves frequent interactions between vehicles and transportation infrastructure.
- **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.

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

Automotive security 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 by accident. Many security vulnerabilities now extend to vehicles, such as malware, Trojans, buffer overflow exploits, and privilege escalation. With cars sporting 100 or more ECUs, the 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 this is also a collaborative effort, using a holistic approach with the involvement and contribution of the supply chain and the broader ecosystem, not by separately dealing with individual components, threats, or attack points. Unlike traditional computer systems, initiation and consequences in both the cyberworld and the physical realm are possible over vehicle attack surfaces, making it more challenging to protect the vehicle's systems.

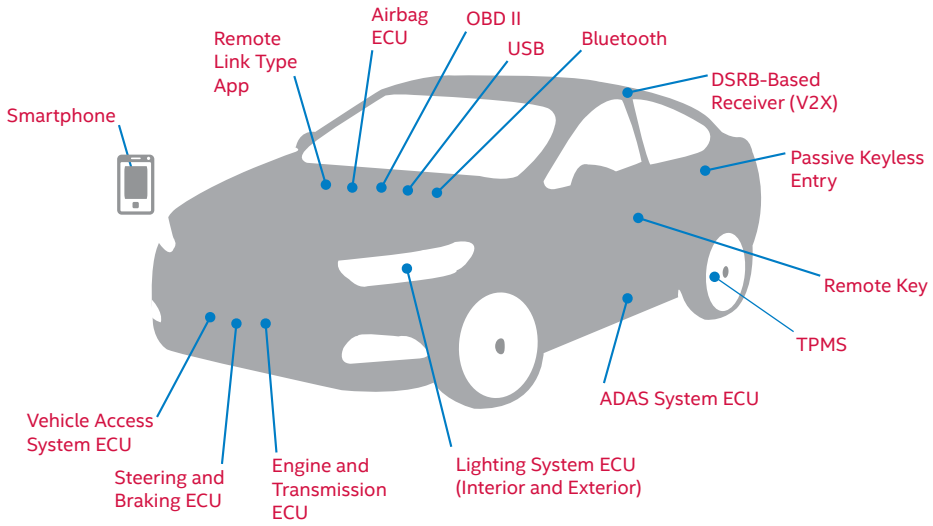

Figure 2. Fifteen of the most hackable and exposed attack surfaces on a next-generation car.

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 on 20 recent models (2014 to 2015) from multiple different car manufacturers. Furthermore, the more advanced cyberphysical features a car has, the more likely it is to be attacked. The same authors demonstrated realistic hacking scenarios on a Jeep Cherokee.[2]

Designing Automotive Product Security

While vehicle security may be distinct from vehicle safety, in some ways, vehicle security is essential to delivering vehicle safety. The organizational disciplines that lead to safe and reliable cars also apply to security. In particular, safety, reliability, and security must all start at the outset of the design phase. To ensure a secure design, a threat model is created for the vehicle that anticipates 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.

There is a substantial legacy of control and bus systems on a car, with each system historically dedicated and independent. It was once felt that the complexity of automotive systems would inhibit hacking. But, as in the general computer industry, this is now understood to be insufficient. Current automotive systems are vulnerable. Applying best known practices and lessons learned earlier in the computer industry will be helpful as vehicles become increasingly connected. Hackers are more sophisticated and often 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.

Expanding on experience from related industries such as defense, aerospace, and industrial machines, many of the foundational principles, lessons learned, and processes developed over the past decades in cybersecurity can be utilized: a distributed security architecture, exhibiting defense-in-depth, analogous to the layers of protection analysis (LOPA) methodology used for safety and risk reduction; and securing systems from the hardware to the cloud, with identified best practices and technologies for each discrete building block. 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 authentication, network encryption, data privacy, behavioral monitoring, anomaly detection, supply chain risk management, 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

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 intrusion detection and protection services (IDPS), firewalls, whitelists/blacklists, malware detection, cryptographic services, biometrics, over-the-air updates, and other capabilities.

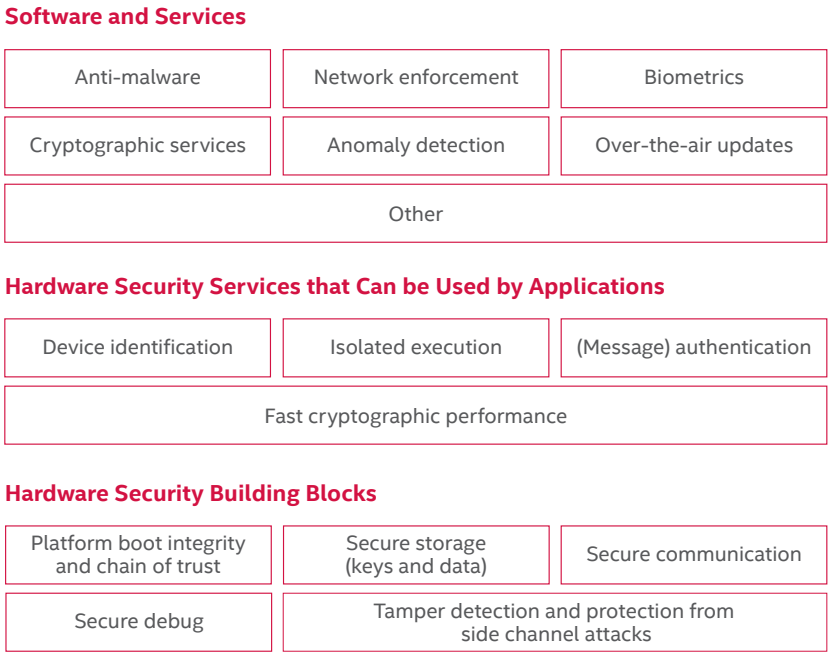

Figure 3. Defense-in-depth building blocks.

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 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 overrun and 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. This technology, built into the chip, can also encrypt the identity to preserve anonymity.

Software security

Automotive networks and control units have historically been protected by careful isolation within the hardware architecture, making their attack surface hard to reach. A determined attacker with time and money can still break into these systems, even on new vehicles. 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 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 cooperating 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.
- **Virtualization**: A commonly used software and hardware combination that makes it possible to create a defensive barrier on a single ECU that separates externally facing functions from those that drive the vehicles, reducing the complexity of consolidating multiple systems onto a single ECU.
- **Software containers**: Used to isolate individual systems and applications, making it possible to update or replace individual functions without affecting overall operation or mirroring functions for 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 behaviour**: Required instead of isolation, for networked systems. 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.

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), automotive Ethernet, Bluetooth, or Wi-Fi—and newly proposed protocols, like dedicated short-range communications (DSRC)—amplify the threat, as they increase the number of nodes that are vulnerable to an external attack. Replacing unsecured legacy protocols with common protocols makes it possible to leverage good security techniques that have been developed in the computer industry, but it also makes it easier for computer hackers to attack cars. Security-enhanced ECUs can interact with security-enhanced networking protocols (in-vehicle or external) to enhance authenticity, reliability, integrity, and timeliness of the transmitted data. Hardware-assisted technologies to secure networks without significantly impeding performance, latency, or real-time response include:

- **Message authentication**: Verifies that communications are coming from the approved source and defenses to protect 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.
- **Firewalls**: 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.

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**: Collaborate among vehicles, dealers, manufacturers, and even government agencies to quickly propagate zero-day exploit and malware warnings 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.

Supply chain risk management

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**: Includes a long-term parts availability policy.

Data privacy and anonymity

Personally identifiable information (PII) is now leaving the confines of the vehicle, requiring appropriate privacy controls and anonymization of data. Data privacy has two aspects: confidentiality of personal data and leaking of data outside the consumer's control. For 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 telemetry. For data leakage, there is a need for new methodologies to justify what data is stored, securely store data, destroy data upon consumption, and protect against unauthorized access.

Discussion on Security Best Practices

Automotive and cybersecurity ecosystems need to engage in discussion and development of best practices for designing, developing, and deploying security solutions.

Automotive safety is a probabilistic science where risks are identified and measured, and components are built accordingly. Best practices for production processes, in line with industry standards, ensure that the design components for vehicle security are correctly implemented and their implementation is linked back to the properties in the secure design, giving customers confidence that the platform is secure. Computer security is not probabilistic, as vulnerabilities in software cannot be easily predicted, many threats are intentional and malicious, and security can be a winner-take-all scenario. As a result, software security aims to prevent or contain all material threats, intentional or accidental, at all layers, throughout the deployed lifetime.

Security development lifecycle

As long as a car is in operation, it needs to be protected from intentional and accidental threats, which can happen at any time and at any layer. Like product safety processes that have been practiced for decades, product security processes have been developed and standardized through decades of experience with vulnerabilities, attacks, and their aftermath. This includes testing, validating, and documenting hardware and software implementations against security goals, and feeding results and lessons learned back into the design process for continuous learning.

A security development lifecycle (SDL) that integrates security and privacy tasks into each stage of development as part of a seamless process is a best practice designed to deliver software with security built into it, not on or around it. The security practices within the SDL are used to establish and maintain trust in products, services, and platforms throughout their lifecycle. During the design phase, the focus is on mitigation of trust issues. A security architect assesses the design proposal for security and privacy implications and creates threat models to identify any areas of concern based on the applicable security policies and then modifies the design to address or mitigate the threats.

During the development stages, the focus is on detection and removal of trust issues prior to product release. Security coding standards and best practices, such as Motor Industry Software Reliability Association C (MISRA C) and Computer Emergency Response Team (CERT C), or the Joint Strike Fighter (JSF) C/C++ coding standard, are rigorously followed, and the product security architect reviews all designs and coded implementations to ensure that the security requirements are being met. All code goes through manual code reviews with the appropriate peers or subject matter experts, and many tools are available to assist these reviews. Detection includes validation focused on the security design elements identified during the prevention phase to ensure security mitigations were implemented successfully. Functional and integration verification plans must include component- and system-level penetration tests, including third-party testing.

Throughout the process there is continuous review and validation of security assumptions, as well as maintenance and upgrade plans. Privacy reviews cover the whole lifecycle of customer data and extend beyond the product to include front-end and back-end systems and intermediate infrastructure. The final phase of the SDL is survival following a trust issue in a released product. No single process can remove every single security vulnerability with total assurance; therefore, it is essential to be able to react to discovered security issues quickly in order to survive the threat and protect customers. Survival requires prior planning to identify the threat; subject matter experts needed to solve the issues; design teams, tools, and processes to create the security fixes; and appropriate secure channels to distribute solutions to customers and affected parties. "Prevent-Detect-Survive" is a cradle-to-grave security process that covers more than just the development and release cycles; it also includes detailed support for products in the field.

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 and requiring detection and correction processes. Supplier quality engineers are a common role in the automotive industry, and supplier security engineers may soon join their ranks, while cost of security will likely join cost of quality in the decision-making process. Suppliers should follow similar secure development processes, and these 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.

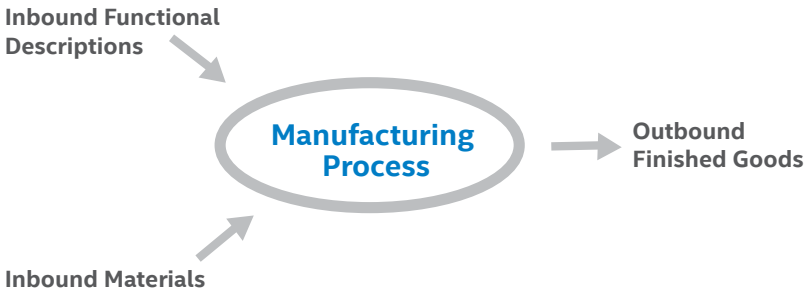

Figure 4. Supply chain risk management.

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. If yield or performance is not impacted, then the security risk is low. 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. The only practical way to modify the function is to replace the mask set, so protecting the mask set safeguards against insertion of malicious functions.

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.

Standards

There is a range of coding, product security, and process standards available or in development from various industry groups. Secure coding standards from the MISRA C and CERT C are common practice.

For vendors selling products into multiple industry sectors, competing security standards cannot be avoided, so people who work on standardization focus on integrating or abstracting conflicting requirements into established frameworks, such as ISO or IEEE. While this may delay standardization efforts in the short term, using a framework yields better and more flexible requirements in the long term. For example, ISO 26262, the functional safety standard for road vehicles, is considering adding security to its specification.

Other industry 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, where components are protected against tampering and sensitive data protected against compromise.
- **Trusted Platform Module (TPM)**: Written by a consortium called Trusted Computing Group (TCG) and standardized as ISO/IEC 11889, it is designed for dedicated microprocessors that integrate cryptographic keys into devices. TCG also recently released a TPM profile for secure automobile data and operations.
- **Secure Hardware Extensions (SHE)**: From the German OEM consortium Hersteller Initiative Software (HIS), these are on-chip extensions that provide a set of cryptographic services to the application layer and isolate the keys.
- **ISO/IEC FDIS 20243 Information Technology and Open Trusted Technology Provider Standard (O-TTPS)**: These aim to mitigate maliciously tainted and counterfeit products and will soon become an international standard for auditing supply chains to confirm that security practices exist and are followed.

The automotive industry is also examining security efforts, best practices, and standards from other industries, such as military, aerospace, and aviation. The US Federal Aviation Administration (FAA) has developed an advisory circular that advises airlines on how to implement a cybersecurity program to manage and support their e-enabled aircraft. The FAA recently distributed a public draft of the Aircraft Network Security Program for review and comment.

SAE International is working on the following security standards which are in draft form:

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

In addition, there are several more that cover different aspects and properties of the vehicle and its production.

Other areas of transportation security research include vehicle cybersecurity and privacy, automated vehicle cybersecurity, transportation privacy, automotive security applications, and vehicle security risk assessment.

Operating Securely for the Full Lifecycle

While robust vehicle security starts at the beginning of the design phase, updates are a critical activity over the lifecycle of the vehicle. Vehicle software is at risk as long as it is on the road and has to be protected over the full lifecycle from potential hardware vulnerabilities, software vulnerabilities, intentional and accidental owner actions, and malicious attacks. As computing capacity and performance increase over time, and new attack methodologies are developed, attacks that were previously impossible become possible. Identifying and understanding potential criminal business models helps to prioritize threats, articulate their associated risks, and determine necessary countermeasures. Detailed incident response plans in the event of a newly discovered vulnerability or security breach guide immediate actions and provide confidence to the consumer and manufacturer. Consumer trust and confidence need to be maintained through multiple owners and transactions with new and pre-owned car dealers and repair shops. These operational measures require secure chains of trust that are designed into the vehicle and meant to last for its deployed lifetime.

Securing the chains of trust includes building and sustaining a source of trusted spare parts for ongoing maintenance of the vehicle. Threat analysis and risk assessment also continue throughout the life of the car, as old vulnerabilities are patched and new ones come to light, and the risk of attack can even increase over time. The lifetime of a vehicle is now approaching 15 years, much longer than the lifecycle of most software and even computer hardware. For example, support and security updates for Microsoft Windows XP were discontinued 12 and a half years after it was released, after more than 100 updates, or an average of about one per month. Techniques such as over-the-air software or firmware patches and updates are necessary to quickly close vulnerabilities and significantly reduce recall costs. Being able to leverage and deploy countermeasures to known threats in short order is essential. Policies to sustain trusted supply are also critical. Best practices continuously review and renew obsolete parts supply chains for unexpected events such as floods or earthquakes that destroy stocks.

Cybersecurity business models

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. 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 to pranksters to owners to criminals to nation-states.

Researchers and hobbyists

Researchers and hobbyists, sometimes funded by universities, 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, and 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 and hactivists typically represent the dark side of the hobbyist group. They take the opportunity to demonstrate their skills or promote their cause, 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 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 too 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 become a real and significant threat actor in the cybersecurity space, and there is no reason to expect that its presence will be significantly different in automotive security. The main motivation for this group is financial gain. 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 be 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.

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. It is not clear if this threat is emanating from organized crime or nation-state groups. What is clear is that establishing supply chain transparency, meaning credible information about where parts were sourced from and evidence that secure supply chain practices were followed, is a best practice to mitigate the risk of cloned parts infiltrating the vehicle.

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. Others 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.

System behavior

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? 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 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, which may be automatic or may require explicit interaction by the owner and manufacturer.

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. 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 do deal with unpatched systems. Memory monitoring and anomaly warning solutions are possible that model the normal operation of the vehicle and create a unique fingerprint. 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 hacks from prohibited 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 create some increased risk.

Aftermarket

App stores, aftermarket components, and service shops are a large component of the auto industry, as they are for many other 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 FOTA 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 appeared in 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 extensive 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.

Open Questions

This paper has just scratched the surface of 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," but an "Update Software" light may well be a future reality. Intel has established technology leadership in all these areas and is actively engaging with standards organization and ecosystems to address unique challenges for next-generation vehicles. This paper is a call for action to move the automotive industry to the vision of cutting the number of road casualties in half by 2020 and eliminating fatalities by 2050.

Best practices for automotive security are an evolution and amalgamation of both product safety and computer security. Intel, Intel Security, and Wind River together supply many of the key ingredients to the automotive industry and are leaders in the computer security 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.

Intel Resources

Intel 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 Intel, see:

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

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security combines the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

1. *Charlie Miller and Chris Valasek, "A Survey of Remote Automotive Attack Surfaces," DEF CON 2014.*
2. *Wired, July 21, 2015, "Hackers Remotely Kill a Jeep on the Highway—With Me in It"*

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com