Accelerating security

Winning the race to vehicle integrity and data privacy

IBM Institute for Business Value

How IBM can help

Today's vehicles are evolving from a mode of transport to also serve as a new kind of moving data center with onboard sensors and computers that capture information about the vehicle. Using such real-time data, IBM helps auto executives provide new services that the connected consumer needs and expects from the vehicle experience. Our combined strength in manufacturing and depth of global automotive expertise can address consumer concerns about safety and quality. Innovative technologies such as Watson for analytic capabilities can meet OEM and supplier needs, including products and services that are more secure and reliable to enable higher brand loyalty and customer satisfaction. Please visit **ibm.com**/industries/automotive.

Preventing, detecting and responding

In 2014, IBM published a point of view on automotive security, "Driving security: Cyber assurance for next-generation vehicles," which introduced the "Design, Build, Drive" approach for the automotive security lifecycle.[1] It's time to dig deeper. While it's logical to tackle each phase in the lifecycle, starting with Design, most conversations around vehicle security quickly turn to the threat to in-service vehicles and data privacy, both of which are aspects of the Drive phase. Consequently, we'll focus on this phase, the one consumers can most readily identify with, and evaluate ways in which automakers can engineer technology to prevent exploits, detect suspicious behavior and respond by recovering gracefully and safely.

Executive summary

Consumers drove the genesis of the connected vehicle. We've always wanted music to accompany our road trips, and that journey has taken us from the back roads of 8-track players to an age in which our mobile phones can store thousands of songs, which of course we want to stream through the vehicle's speakers.

While that may sound simple, there's complexity involved whenever a vehicle has to connect to external devices. If the vehicle can provide Bluetooth services, why can't it also serve as a WiFi hotspot for all passengers? In our recent study, "A new relationship — people and cars," we found that 49 percent of consumers we surveyed expect the vehicle to be a securely integrated device in the Internet of Things (IoT) within the next 10 years.[2]

Modern travelers will want to switch seamlessly between modes of transportation, all the while retaining a consistent and personalized digital experience. With many technologies sharing information about the traveler, and each participant in an intermodal experience independent from each other, governance and privacy are major concerns. When the traveler leaves one mode for another, there must be guarantees that personal data is wiped from the vehicle and that persistent data captured during the travel transaction is properly protected, encrypted and retained for the minimum period of use before it is finally deleted.

The good news is that connected functionalities aren't being actively exploited by threat actors — yet. While researcher antics have dominated recent news — demonstrating that it is possible to take control of a vehicle — there hasn't been widespread exploitation of vehicle vulnerabilities.[3] Currently, general purpose computing platforms such as desktops, laptops and even mobile phones and tablets are easier targets for malware and ransomware; however, as security controls make it more difficult for attackers to compromise those targets, they'll move on to the IoT, including connected vehicles.[4]

56% of consumers say security and privacy will be key differentiators in their future vehicle purchasing decisions

In the age of connected vehicles, the **vehicle is not completely safe until it is secure**

Security must be part of the DNA of the enterprise and manifest itself throughout the full lifecycle of the vehicle

It's not just the consumer's safety and privacy that are at risk; the automaker and other participants in the mobility ecosystem (such as telecommunications and insurance companies) assume great liability in the connected vehicle era. It's impossible to stop attackers and researchers from probing for vulnerabilities. Automakers need to do their best to produce vulnerability-free products, test them thoroughly and continuously and remain prepared to acknowledge, fix and publicly respond to researchers' findings and incidents. As the vehicle continues to evolve into a "datacenter on wheels," an interdisciplinary approach is needed that involves traditional and non-traditional players and capabilities to tackle cybersecurity and data privacy challenges.

Automakers must also be publically transparent about efforts to evolve the safety, security and privacy of connected vehicles. Fifty-six percent of consumers we surveyed said security and privacy would be key differentiators in their future vehicle purchasing decisions.[5] While consumers demand the latest technology, they also expect it to be wrapped into a neat package with three bows: safety, security and data privacy.

Building a foundation for success

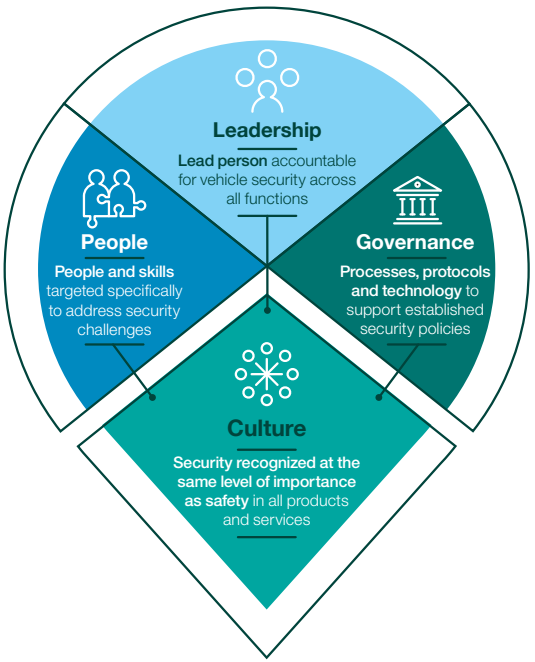
Automakers will have the greatest success in engineering effective security solutions when they are operating from a solid foundation of preparedness. Two key aspects of this foundation are ensuring that security is infused into the DNA of the organization and having a robust data model that comprehends all aspects of data usage, privacy and ownership — both for the automaker and, most importantly, the consumer. Only then can automakers truly implement the phases of the Design, Build, Drive security approach — specifically the Drive phase — to prevent, detect and respond to threats.

Infusing security into the DNA of the organization

Security for connected vehicles begins at the organizational level and should pervade an automaker's culture, from its leadership down to its people and throughout its governance (see Figure 1). The Design, Build, Drive security approach requires a new perspective — one where security rises to the same level of importance as safety, as there is no safety without security in the age of IoT and, consequently, connected vehicles. Security is not an inherent concern for most employees, including those in leadership positions; they must learn to prioritize it. Automakers, in particular, need to institutionalize security into every process, and through repetition this approach will become reflexive for employees.

Figure 1

When an automaker embraces security and promotes it throughout its culture, vehicle security becomes as important as safety



Including non-traditional industry participants

The automotive industry unquestionably understands its technology and safety models, but information security researchers better understand the cybersecurity landscape and the threat actors. In a recent IBM Institute for Business Value report, "Automotive 2025: Industry without borders," we found the digital experiences that most resonated with consumers were those designed by outside partners, not the automakers.[6] This is because the interfaces are based on consumer devices, such as mobile phones, which have a far more intimate user engagement experience. The moral: Include non-traditional industry participants with deep expertise in multiple disciplines to design the best solution.

Because designing, building and managing vehicles throughout their lifespan is a complex undertaking involving many distinct organizational entities, there must be one body that defines the security strategy and practice and governs the implementation and coordination of activities among the entities. The leader of this body is commonly referred to as the "cybersecurity tsar," but under whatever moniker, this position must have the authority to work with all organizational entities, including design, production and service. This body must work to ensure cross-communication between the entities to encourage everyone to consider the security concerns and threat models, both in creating scenarios and managing them throughout the Design, Build and Drive phases.

Auto companies must also hire employees, from outside the industry, with security expertise in a variety of key positions. Such experts can be expected to identify security practice flaws and drive improvements, as well as impart a security philosophy to those around them.

The industry is expanding its frontiers beyond technology specific to automobiles and into areas where automakers may lack deep expertise. The solution is for companies to collaborate with experts in IoT technology and security, including software and firmware analysts, communications and networking engineers, cloud architects, mobile device developers, threat analysts and data scientists. Automakers must also collaborate within the industry to share threat intelligence, and they must collaborate across industries to detect general threats, such as nation-state espionage, as early as possible.

Collaboration also means inviting researchers to test automotive products and share their findings with automakers first. Researchers are motivated by recognition and money: Bug bounty programs are an effective way to enlist them to uncover more real-world attack scenarios than an internal quality assurance team might find.

Finally, consumers need to know that automakers are actively taking steps to address and improve the security, and therefore the safety and privacy, of connected vehicles. Transparency means listing specifics, such as the details of vulnerabilities, and giving consumers the tools to validate that their vehicle is up-to-date. Collaborating with researchers and connecting with consumers is key to building trust and maintaining brand loyalty.

Evaluating data usage and ownership

Having robust data usage and ownership models are important when evaluating security and privacy requirements. This includes the data that is generated and where and how is it collected, transmitted and stored. Also, automakers must categorize and classify data. Does it belong to the occupants or to the automaker? Based on that information, how should it be protected?

Automakers struggle with who ultimately owns the data. Information such as weather and maps clearly belong to the automaker. Phone contacts, call logs and text messages clearly belong to the consumer. But who owns telemetry from in-vehicle sensors? Unless legally specified, automakers should assume the data belongs to the occupants of the vehicle and that they may only transmit, store and use it if the consumer consents via some opt-in mechanism.[7]

Data that is clearly sensitive and considered personally identifiable information may fall into this "digital persona" category. For example:

- The vehicle may come to "know" how you feel by your driving style and respond accordingly. If your driving becomes aggressive, the vehicle might switch from the heavy metal station to a smooth jazz station to calm you.
- The vehicle may come equipped with a heartrate monitor in the steering wheel. If the monitor detects a serious anomaly in your heart rhythm, it may switch to fully autonomous mode and alert emergency services.

Personal data in today's vehicles

Personal data runs throughout today's vehicles. For example, a navigation system may gather data about a vehicle's location coordinates and send it to an automaker's backend systems to perform analytics on driving patterns and to feed navigation apps. The vehicle must anonymize this data to remove personal information about the owner or occupants. When a consumer pairs a phone to the vehicle and syncs contacts, call logs and text, the vehicle must encrypt this data. When the occupant exits the vehicle and the pairing is out of range, the vehicle must wipe the data so that subsequent occupants cannot gain access to it.

- The vehicle may have access to your medical records and transmit them to emergency personnel only if you're in an accident or have an emergency health condition.

For automakers, this is an area that will only grow in complexity. Consumers will not truly realize the benefits that connected vehicles can deliver until they are confident their data is protected.

Embracing the Design, Build, Drive security approach

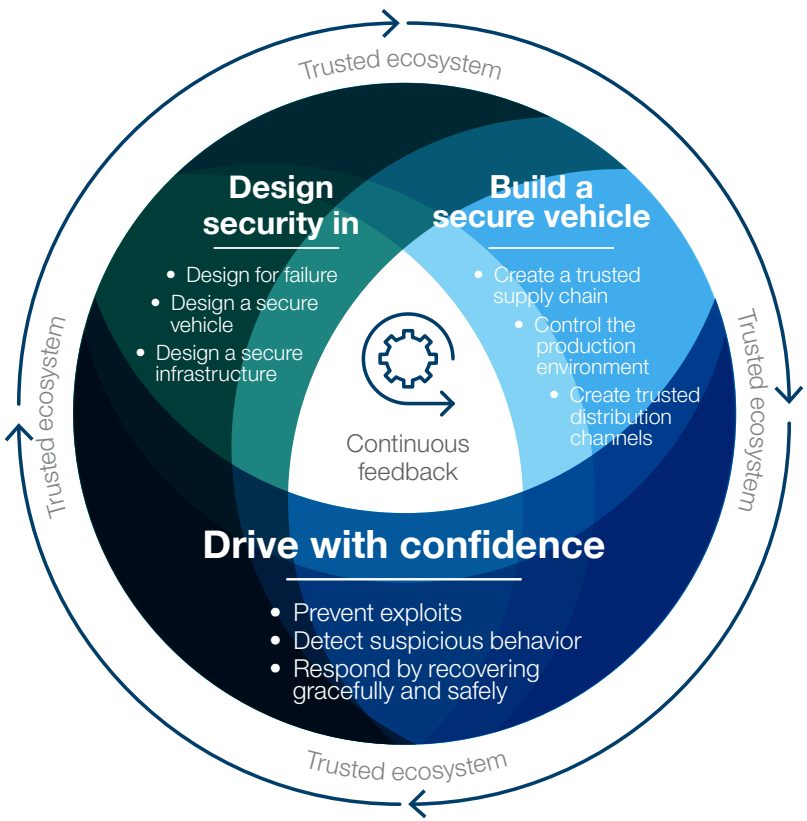
While the focus of this paper is to delve deeper into the Drive phase, it is important to briefly recap the key components of the first two phases because all three work together to support a trusted ecosystem (see Figure 2).

Designing security in refers to planning for attacks, not only in the vehicle but also in the interaction between vehicles and infrastructure. A guiding principle for achieving this security is to assume the worst and design for failure. For example, every interaction on the bus systems could be compromised, and so Electronic Control Units (ECUs) should not blindly act on every control message.

When designing a secure vehicle, the design process must have a security focus from the onset. This includes defining the means and methods of testing the range of threats that may be exposed during the use of the vehicle. This threat model should be available to the entire design team. Next, designing a secure infrastructure requires taking into account not only the vehicle but all the infrastructure components the vehicle will communicate with. Traffic lights, toll lanes and other vehicles are just some of the devices that cars will interact with. Designing a guarantee of integrity between all elements is crucial.

Figure 2

A comprehensive approach to security is required to address the needs of today's connected vehicles



Building a secure vehicle requires attention to not only the supply chain and production environment, but also the distribution channels all the way to the consumer. Creating a trusted supply chain requires integrity — this means preventing counterfeit or malicious components from entering the vehicle parts supply chain and ensuring that a part has not been tampered with from the time it is shipped from the factory to the time it is installed in the vehicle.

Controlling the production environment entails establishing the integrity of the IT and production systems. Understanding functions, applications, interfaces and protocols for each system and having a security policy with access and security controls in place will help secure the production environment. Creating trusted distribution channels is similar to the supply side process but focuses on the time when the vehicle is traveling between production, the dealer and, ultimately, the consumer. Controls to prevent vehicle tampering as the vehicle is handled by third-party providers such as logistics companies need to be in place.

It should be clear at this point that security encompasses more than just the vehicle and automaker. It also includes dealers and service centers, as well as third-party providers, to name a few. The industry must instrument and monitor the entirety to create a **trusted ecosystem.** The result: an end-to-end approach to security that meets today's needs and is elastic to accommodate the future. Consequently, each area within the ecosystem requires a trusted environment that includes security controls for strong authentication and access rules, system hardening and key management.

While automakers have control over the vehicle, many parties want to connect to it. The connection points provide an open platform, but also create what security experts call a "broad threat surface." Automakers must consider the implications of each connection technology and choose those that are compatible with the greatest number of potential third parties that provide strong security.

Drive with confidence

When an automaker has embraced the foundational considerations we have presented thus far, it will have greater success in improving security in the third phase of the Design, Build, Drive approach. During the Drive phase, when the vehicle is on the road, a driver expects technology and services to prevent exploits, detect suspicious behavior and respond by recovering gracefully and safely (see Figure 3). To the extent possible, the vehicle, automaker and third parties involved in managing the vehicle must execute this comprehensive approach without burdening the owner — unless the owner asks to be involved. Only in extreme situations should the driver be expected to make decisions about safety, security and privacy.

Prevent exploits

Authenticating entities

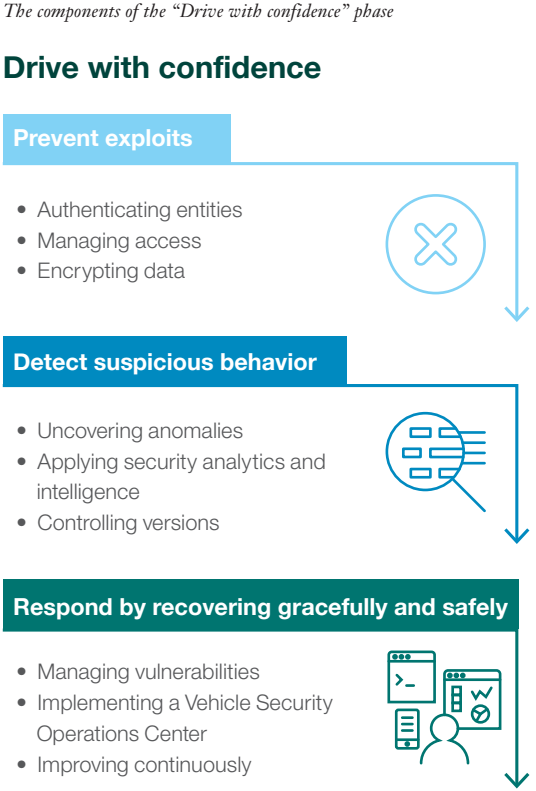
Authentication is the process by which identification is validated. People authenticate to the vehicle and to interfaces such as web portals and mobile apps. The components in a vehicle also authenticate to the vehicle infrastructure and to each other. The goal is to ensure that commands from people, apps and components are authorized. Identification positively informs who the person or what the component is. However, it does not prescribe what people or components can do.

A trusted identity is more than a username and password. In the context of connected vehicles, a trusted security module is essential. The module must:

- Provide authentication functions for interactive logins as well as positive identification of non-interactive components, such as ECUs.
- Attest to identities when queried.
- Inherently provide storage, signing and management of certificates and cryptographic keys, and implement strong authentication, such as two-factor and out-of-band mechanisms.
- Be flexible and extensible, implementing open standards, such as OAuth and SAML.[8]

Figure 3

The components of the "Drive with confidence" phase



Trusted identities in connected vehicles

Following are examples of authentication and use of a trusted identity in the connected vehicle ecosystem:

- The user authenticates to the mobile app or a web browser, which in turn communicates to backend systems and validates to any vehicles she owns. She can then monitor and control the vehicle.
- Smart traffic lights and roadside infrastructure may signal the vehicle to take certain actions, such as slowing down on sharp curves. Infrastructure components must present a trusted identity to prevent rogue actors from abusing this signaling mechanism.
- ECUs and control components must have a trusted identity to have the authority to send messages. This prevents rogue devices from sending malicious commands.
- Updates, including those installed locally or over the air, must have a trusted identity to avoid installation of malware.
- Third parties, including service and repair centers and content providers, must have a trusted identity.
- Apps must be trusted.

- Contain a cryptographic processor.
- Be tamper resistant.

Identification must also provide functions that are unique to vehicles. Examples of these functions include driving behavioral pattern analysis, seat sensors that determine the weight of the driver and confirmation capabilities that rely on entry keys or mobile phone signatures.

Managing access

Access management controls activities within the vehicle and between it and external components. Permissions to execute these activities must be defined for operations based on the identity of the requestor and target, the type of request (for example, a control message, a read request or a write request) and context (for example, a vehicle's speed or its geolocation).

Within the vehicle, ECUs are the likely target for malicious activity. There must be enforcement points that support ECU access rules. Because ECUs have limited processing capacity, managing these rules at so many endpoints can be complicated. However, there are a few strategies for implementing access rules, such as segmenting like components by subsystem function (for example, braking versus steering).

Encrypting data

Encryption protects the data itself and includes configuration files and telemetry in addition to consumer data, such as emails, texts and contacts. Data is stored (at rest) at many points within the vehicle, in the automaker's service network (the cloud) and with various partners. The data may be transferred (in motion) within the vehicle's operational networks, across the mobile network, over WiFi or Bluetooth or using Dedicated Short Range Communications (DSRC).

Encryption may be too processor-intensive or impose delays when applied across the Controller Area Network (CAN) bus. Today, this is not a feasible option. Automakers must evaluate the risk and not always strive for absolute security in every component when designing encryption into vehicle systems.

Encryption relies upon the security module referenced earlier. One additional requirement for customer data is that the encryption must be zero-knowledge. This means that the automaker and third parties may not decrypt the data; it's protected end to end, and only the consumer should have the ability to decrypt it. Many cloud providers are moving to a zero-knowledge model.

Recently, automakers have put a lot of emphasis on vehicle intrusion detection and prevention systems (IDPS) as a means of preventing attacks. Their hope is that they can take the same engineering approach they have applied historically to mechanical challenges and solve each security challenge with a single component or feature.

This approach has two weaknesses. First, the protection mechanisms are rule-based and therefore can only intervene when a "foreseen" attack type occurs. What happens when an attacker finds new pathways that were not written in the code? Second, attackers could one day seek monetary gains using ransomware or by targeting payment data instead of threatening the lives of passengers by going after the safety-critical components.

Effective prevention starts by architecting an end-to-end security strategy that works in an integrated fashion. The strategy should be based on a layered approach in which various actors interact and complement one another.

Access management in action

Following are examples of access management within a connected vehicle ecosystem:

- Only the anti-lock braking system (ABS) is authorized to send control messages to the brake ECUs; anything else must request these actions from the ABS, which acts as an arbiter and must contain access management control rules. The brake ECUs themselves must contain a simple control rule: Ignore all access control messages unless they come from the ABS and its trusted identity can be confirmed.
- When set into valet mode, storage compartments remain locked and the vehicle may be geofenced to within a half-mile radius and governed at 25 mph.
- Only humans and components directly involved in the processing of emails, texts and phone calls may access that data. The automaker's service cloud may access the vehicle's operating telemetry, including location, speed and odometer reading, but not data synced from the driver's mobile phone. Owners may, however, opt-in to allow the automaker or third-party maintenance service providers to have access to their calendar to schedule appointments.

Detect suspicious behavior

Uncovering anomalies

Detection can provide an early warning and allow automated systems and manual protocols to intervene to stop an attack before it compromises safety, security and data privacy.

Intrusion detection relies on instrumentation at strategic locations within the vehicle. This instrumentation may include the In-Vehicle Infotainment (IVI), bus systems, central gateways, domain controllers (in next-generation vehicle architectures) or the ECUs themselves. Data gathered may include events that these components have generated, such as log activity from the IVI or monitored communications on the control busses.

While the vehicle IDPS approach mentioned earlier has merit, it also has limitations in the detection phase. The IDPS is rule-based and mainly inspects and reasons about communication among the ECUs over the vehicle's CANs. Although this information is important, especially if an IDPS applies elaborate analysis techniques, the insights obtained represent only a relatively small subset of relevant security events internal to the vehicle's environment. Intelligence on the CAN bus is primarily focused on safety. Even though this information is critical for protecting lives, it will not provide the full perspective of suspicious or abnormal activities across other networks or OS data. Some attacks on the vehicle may be detected with this approach, but many sophisticated attacks will remain undetected.

Applying security analytics and intelligence

Security analytics must identify attacks on the integrity of both individual vehicles and across vehicle networks. This allows for forensic analysis of data collected that can be scrutinized with historical data to identify and understand attacker pathways.

Automakers are making great strides in the use of analytics, such as vehicle predictive service analytics. They know that a mechanical component is likely to fail — and even when, to some extent. This same predictive skill needs to be applied to security analytics, which are informed by use cases and derived from threat models.

A comprehensive context-based solution for detection executes some collection and processing locally and sends a manageable set of events, in near real time, to a central analysis platform. This process provides a balance between the limited in-vehicle computational abilities and the bandwidth restrictions of sending all data points to a backend system.

Controlling versions

Version guarantee is an important safeguard that combines the elements of a security module and detection capabilities to help ensure that all components in the vehicle are the latest versions and have the latest security patches applied. It also guarantees that no components have been tampered with.

A version guarantee system must first itself be trusted. Then it must confirm the trusted identity of all components and test their digital signatures against a master database provided by the automaker. The IVI itself is complex and includes many open source software libraries. The versions and signatures of the libraries must be maintained and tested regularly. To maintain transparency, automakers must provide some form of assurance to consumers, optimally in the dashboard or IVI. A simple, periodic message such as “All vehicle modules are valid and up-to-date” can go a long way to maintaining customer confidence.

Classifying vulnerabilities

Not all vulnerabilities are created equal: Automakers and legislators must work together to define a classification system for vehicle vulnerabilities that takes severity into account. For example, harm to passengers takes priority over loss of data. The response will depend on the classification of each vulnerability.

Respond by recovering gracefully and safely

Managing vulnerabilities

While feature updates are a matter of customer convenience, security updates are critical to customer safety, security and data privacy. When an automaker identifies a vulnerability within a vehicle or its supporting infrastructure, it must develop and deploy a patch to every vehicle before attackers can actively exploit the flaw.

Automakers may decide to provide over-the-air (OTA) updates and also allow consumers to visit a service center (such as a dealership) at their discretion. An automaker must gain the vehicle owner's consent before providing OTA updates, and must obtain owner consent to gather certain data about the vehicle operation. Consent needs to occur also whenever vehicle ownership is transferred and may become as simple as clicking an agreement on the IVI or at a web portal.

The details of OTA updates are complicated. A secure transmission medium from the automaker to the vehicle is necessary to prevent corruption of updates. A post-update signature verification, using a trusted module, is required. Finally, a test must be performed after the update is installed.

Before an OTA update is initiated the vehicle needs to be in an appropriate state. For example, it would not be prudent to update powertrain components while the vehicle is in motion. If a safe context is not achievable before the update deadline, the owner will be required to complete the update, either by putting the vehicle into a safe mode or by bringing it to a service center.

Implementing a Vehicle Security Operations Center

Automakers need to gather, analyze, evaluate and act upon all relevant information from vehicle operations — and should perform all of these tasks in a dedicated Vehicle Security Operations Center (VSOC). The VSOC is the mission control for safety, security and privacy for connected vehicles. It is the front-line security operations function that monitors cyber threats to a set of predefined fleet of vehicles (geography, model and make, for example) and analyzes events to classify and escalate security incidents for response and remediation. The VSOC encompasses the people, processes and technologies that handle threat monitoring, forensic investigation, incident management and security reporting.

VSOCs are designed to:

- Provide a central point for monitoring, synthesizing and acting on threats
- Prepare for and respond to cyber incidents
- Retrace full attack activity
- Search for breach indicators
- Enable business continuity and efficient recovery
- Prevent cyber threats from compromising a vehicle's infrastructure
- Provide insightful cyber-risk and compliance reporting.

The VSOC is comparable to a traditional business IT SOC, although VSOC security analysts must have deep technical domain knowledge of the automotive industry and even the specific make, model and version of a vehicle under attack. These analysts must also have expertise in the broader cybersecurity space.

Improving continuously

As with all processes, lessons learned feed back into the cycle. For example, automakers need to loop the forensic pathways described earlier, together with internal security testing, back into R&D to realize continuous improvements. These measures will help to close design flaws from the beginning of the design phase.

Some of the lessons learned will contribute to a better understanding of the attackers, their motives and tactics. This knowledge will enhance the threat models and will improve the Design and Build phases of vehicle security. Automakers should also share feedback with industry collaboration processes, such as the Automotive Information Sharing and Analysis Center (Auto ISAC), as well as with every stakeholder in the connected vehicle ecosystem. Similarly, there are many industry-driven initiatives that seek to develop standardization or best practices, including AUTomotive Open System ARchitecture (AUTOSAR), E-safety vehicle intrusion protected applications (EVITA) and SAE International's standard J3061, which provides guidance on vehicle cybersecurity. We expect to see more specific regulations and laws targeting IT security and data privacy for connected vehicles as we pave the way toward autonomous driving.

Ultimately, automakers will have to be prepared to comply with higher standards to provide better security and privacy, along with safety. Those that can deliver the safety and convenience features consumers desire while also assuring their safety and security will be best positioned to benefit from the true power of the connected vehicle.

Are you in the race?

- What is your comprehensive strategy and approach to bring vehicle security to the same level as safety within your organization and your partners' organizations?
- How are you applying historical and real-time security information about connected vehicles to understand attack vectors, attacker pathways and exploits?
- How are you continuously improving your feedback loop to harden the vehicle?
- How do you securely allow sharing of your connected vehicle data with third parties or partners?
- What are your mechanisms for gaining and sharing vehicle security expertise with your ecosystem?

Contributors

Arndt Kohler, Associate Partner, IBM Security Europe

Dr. Yaron Wolfsthal, Associate Director, Cyber Security Center of Excellence, Israel

Dr. Yair Allouche, CTO Connected Vehicle Security, Cyber Security Center of Excellence, Israel

Rob Carson, Content Strategist/Writer, IBM Institute for Business Value, IBM Digital Services Group

April Harris, Visual Designer, IBM Institute for Business Value, IBM Digital Services Group

About the authors

Christopher Poulin is a former Research Strategist with the IBM X-Force security research group. He focused on threat intelligence and security for the Internet of Things, including connected vehicles. He has over 25 years of experience in information security, beginning in the U.S. Department of Defense and spanning a variety of roles from software development to building a boutique security consultancy.

Giuseppe Serio is the IBM Global Solution Leader for Cyber Security in the Automotive and Aerospace and Defense industries. He brings more than 20 years of experience as he engages with clients globally to discusses security programs and the security challenges, including connected vehicle security. He collaborates with other IBM functions such as Research, Security and the IoT business units to develop and adapt security solutions to specific industry needs. Prior to IBM, Giuseppe was a Senior Consultant with PriceWaterhouseCoopers Consulting where he served in multiple international business transformation projects. He can be reached at giuseppe.serio@de.ibm.com.

Ben Stanley is the Global Automotive Leader for the IBM Institute for Business Value. He is responsible for developing thought leadership content and strategic business insights for the IBM automotive industry practice. Ben has over 39 years of automotive experience and has worked with major automotive clients around the world in the areas of business strategy and business model innovation. Ben's previous assignments include living in Shanghai, China for five years, where he led the IBM Automotive Center of Excellence. Ben can be reached at ben.stanley@us.ibm.com and you can follow him on Twitter @BenTStanley.

For more information

To learn more about this IBM Institute for Business Value study, please contact us at iibv@us.ibm.com. Follow @IBMIBV on Twitter, and for a full catalog of our research or to subscribe to our monthly newsletter, visit: **ibm.com**/iibv.

Access IBM Institute for Business Value executive reports on your mobile device by downloading the free "IBM IBV" apps for your phone or tablet from your app store.

The right partner for a changing world

At IBM, we collaborate with our clients, bringing together business insight, advanced research and technology to give them a distinct advantage in today's rapidly changing environment.

IBM Institute for Business Value

The IBM Institute for Business Value, part of IBM Global Business Services, develops fact-based strategic insights for senior business executives around critical public and private sector issues.

Sources and notes

1 Poulin, Christopher. “Driving security: Cyber assurance for next-generation vehicles.” IBM Institute for Business Value. 2014. http://www-935.ibm.com/services/us/gbs/thoughtleadership/automotivesecurity/

2 Stanley, Ben and Kal Gyimesi. “A new relationship – people and cars: How consumers around the world want cars to fit into their lives.” IBM Institute for Business Value. 2016. http://www-935.ibm.com/services/us/gbs/thoughtleadership/autoconsumer/

3 Greenberg, Andy. “Hackers remotely kill a Jeep on the highway – with me in it.” Wired. July 21, 2015. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

4 We’ve already seen an example with the Mirai worm, which compromised over 100 million connected surveillance cameras and digital video recorders, and other malware targeting everything from home routers to baby monitors. More than a billion cars are on the road today; imagine if just 1 percent of them were recruited into a botnet and used in a massive distributed denial of service (DDoS) attack.

5 Stanley, Ben and Kal Gyimesi. “A new relationship – people and cars: How consumers around the world want cars to fit into their lives.” IBM Institute for Business Value. 2016. http://www-935.ibm.com/services/us/gbs/thoughtleadership/autoconsumer/

6 Stanley, Ben and Kal Gyimesi. “Automotive 2025: Industry without borders.” IBM Institute for Business Value. 2015. http://www-935.ibm.com/services/us/gbs/thoughtleadership/auto2025/

7 Data ownership is not always black and white. For example, some retailers may want to know about the vehicles passing by their establishments - the volume of traffic, the brand and model of vehicle (perhaps to gauge the wealth of the potential consumer) and even the VIN to track recurring shoppers. Some of this information may be publicly available, such as traffic volume data, while some may be specific to the automaker, such as brand and model. And some of this data, such as VINs, may not be directly resolvable to consumer identities but may still be considered sensitive.

8 OAuth (Open Authorization) is an open protocol that supports secure authorization for web, mobile and desktop applications; SAML (Security Assertion Markup Language) is an open data format that supports the exchange of authentication and authorization information between service providers and identity providers.

IBM Global Business Services, Route 100, Somers, NY 10589

Produced in the United States of America, January 2017