White Paper
Vlad Gostomelsky,
Senior Managing Security Consultant

Connected Vehicles

Understanding the Risks of Cyber Threats

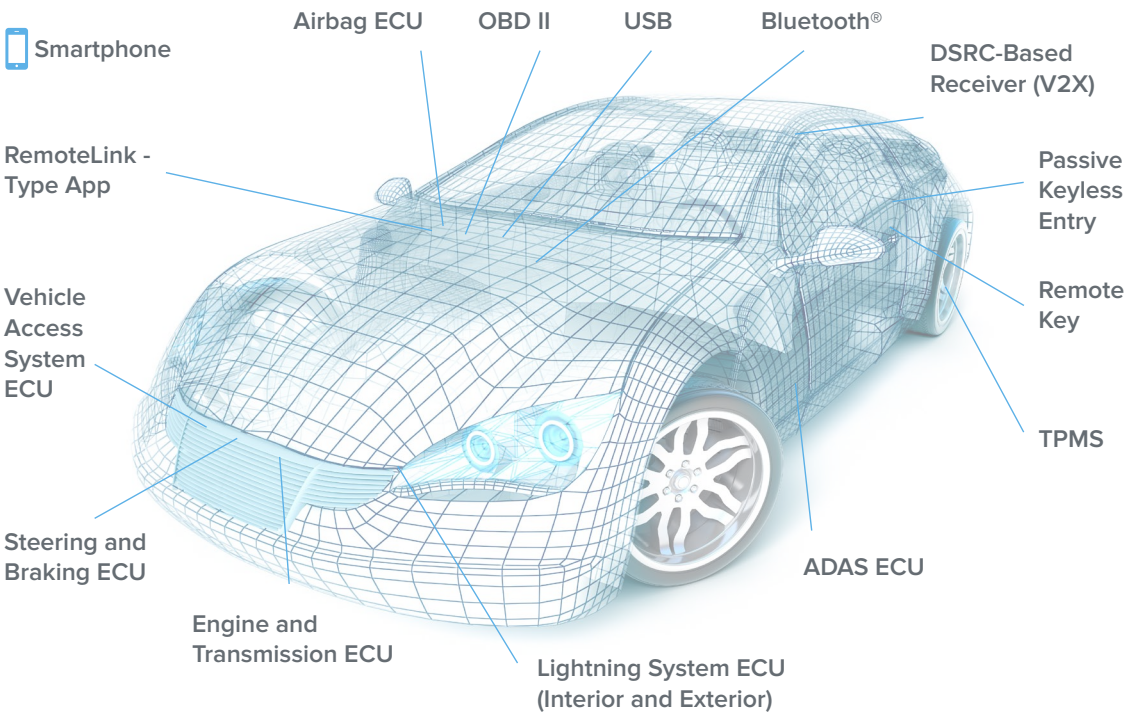
Executive Summary

Preventing, detecting, and remediating attacks on networks, devices, and applications have been important concerns and challenges for the technology industry. But as consumer electronics, network- and cloud-based services, and the new world of connected devices converge, the personal vehicle has become a target. The auto industry—automakers, software developers, chipmakers, and other component manufacturers in the automotive supply chain—is becoming increasingly aware that both components and finished products are potential targets for malicious attacks.

This paper describes why cyber threats are becoming a critical concern for automakers and how such threats can affect vehicles. Easily compromised auto systems can be a channel for malicious activity with enormous consequences for drivers, law enforcement, and society in general. With help from Spirent Communications, automakers can begin to take steps to protect their products, their customers, and ultimately, their businesses from the all-too-familiar consequences of cyber-attacks and security breaches.

Connected Vehicles

Understanding the Risks of Cyber Threats



Cyber Security Becomes More Personal

Internet and software-dependent systems are standard components of today's vehicles—from information, navigation, and entertainment services to critical safety, performance, and maintenance systems. The ability to connect smartphones and "smart" aftermarket systems provides drivers with a multitude of innovative services and features—and an expanded threat surface for a cyber-attack.

Many of today's vehicle systems lack the basic security defenses that protect even the average credit card. Unlike a compromised credit card, which can be cancelled and reissued, a connected car is not easy to disconnect. The unprotected information, entertainment, and other electronic systems in today's vehicles therefore represent a growing risk as drivers become more reliant on Bluetooth devices, smartphones, and a range of third-party products and services. In effect, cars and trucks are wide-open portals through which cyber attackers can steal data, endanger safety, compromise privacy, or even commit terrorist attacks.

"Cyber-attackers will take the easiest path to achieve their goals - the low-hanging fruit," said Sean Pike, program vice-president for IDC's Security Products group. "Connected vehicles offer unprecedented access to personal and logistical information that can easily be packaged and sold on the black market or extrapolated to conduct large-scale public attacks.[1]"

People Are the Weakest Link

Cyber-security professionals agree that people are usually the weak link in any security strategy. When it comes to personal accounts or devices, people rarely adhere to standard security best practices.

For example, users rarely change passwords on their personal accounts with any regularity. They tend to use the same login credentials across devices and services, meaning that if an attacker breaches one account, the attacker has access to all of the user's accounts.

Likewise, people don't change the encryption keys for their vehicle's connected Wi-Fi from the preset factory keys. Many drivers are unaware that such keys exist and, in any case, would typically have no idea how to change them. Basic human nature sets up the perfect environment for hackers to access data through a number of unsecured electronic automobile systems.

Security Systems That Aren't Secure

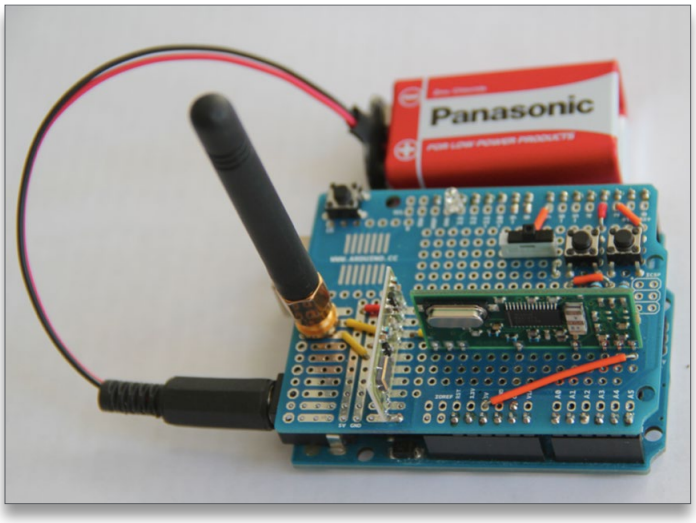
Vehicle security systems themselves are at risk. Higher-end vehicles with remote starting and antitheft devices have been hacked successfully. The doors to a $60,000 vehicle can easily be opened with an $11 radio. Wireless key fob signals can be amplified by wireless scanning devices—even when the key fob is in the house or the owner's pocket in a grocery store—allowing thieves to open doors, start cars, and drive away. The car itself is not always the primary target, however. Thieves can open the car, search for personal information, and use it for identity theft, burglary, or other nefarious purposes.

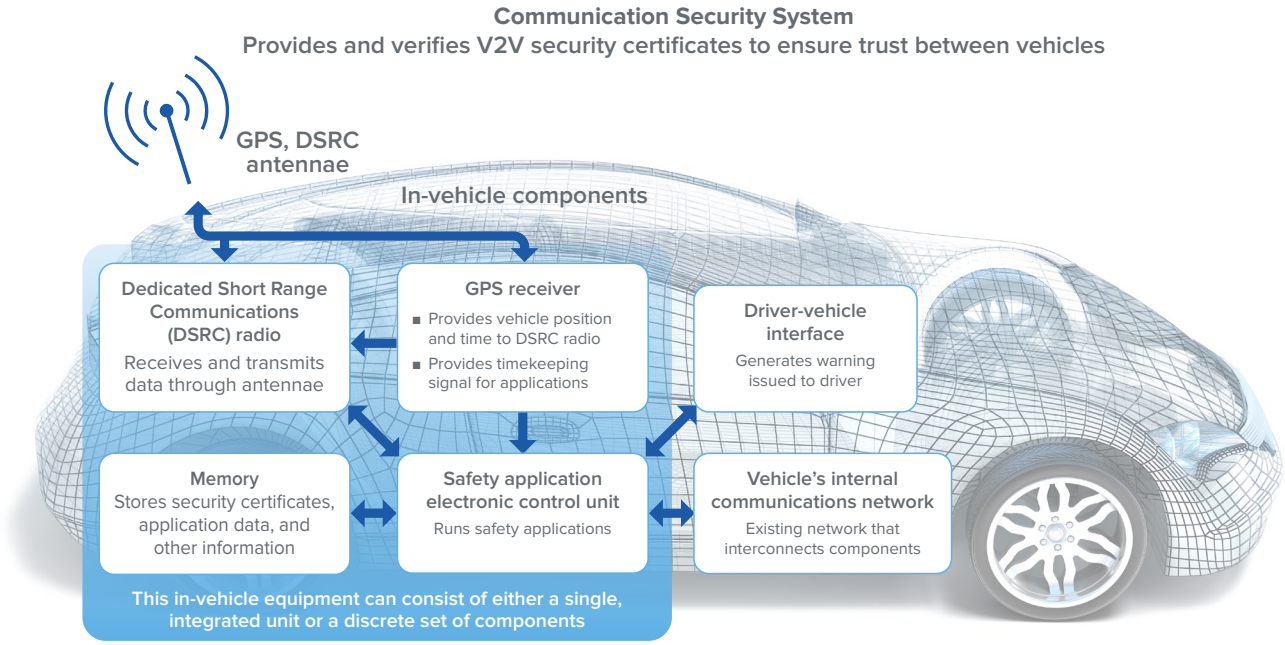
Information & Entertainment Systems—The Easy Way In

Today's head units—the interface for a vehicle's entertainment and navigation systems—give drivers electronic capabilities ranging from basic radio reception to integrated cameras, screens, Wi-Fi, DVD and CD media, MP3, GPS navigation, and Bluetooth wireless connectivity. For cyber-attackers, the head unit represents an easy way to enter a vehicle and launch an attack.

The Bluetooth technology that wirelessly connects mobile devices to computers is simple to hack. Therefore, a smartphone synched with a head unit, using Bluetooth, is also simple to hack. Many head units save smartphone address books to enable features such as voice-activated calling. However, when the phone or the head unit is unsecured, attackers can easily access personal information and use phone messages, texts, contacts, places visited, and e-mails for social engineering attacks.

Applications add functionality to smartphones, but they also increase the risk of a data breach. The more apps that reside on a smartphone, the larger the attack surface. This is especially true if apps are downloaded from websites other than an app store, because such apps can contain malicious code that extracts data. When users spend large amounts of time on a smartphone and in their cars, attackers have more time to compromise a system successfully and can access more data to steal. For example, a cyber-criminal can use stolen data to track people's daily routines—knowing when they are not at home and how long it might take for them to return, and making it easy to plan a burglary or other criminal activity.





Compromising Electronic Systems and Processes

Vehicles can be attacked through the head unit, with the attack confined to information or entertainment systems. But an attacker who compromises the head unit can also move laterally within connected vehicle systems to attack other components, such as the vehicle's Controller Area Network (CAN) bus[2].

The CAN bus is implemented as a closed network to enable communications and coordination between multiple Electronic Control Units (ECUs) within the vehicle. Most vehicles have at least two CAN buses: one that manages communications between sensors, engine systems, airbags, brakes, electrical systems, and other critical systems, and one that controls climate settings, seat positioning, and other non-critical functions. Vehicle service and maintenance diagnostics also rely on the CAN bus, and vehicles support 3G or 4G Wi-Fi connections to their manufacturers for this purpose.

By hacking the bus connections, attackers may be able to expand malicious attacks within the vehicle or push them to the manufacturer. The CAN bus may not include any security features such as encryption or authentication to ensure that messages sent between ECUs are legitimate. An attacker who gains access to the CAN bus may be able to create and send "spoofed" messages between ECUs and cause any number of potential problems.

Vehicles are supposed to work reliably and respond quickly to driver input. When they don't, they become dangerous to the driver and to every other vehicle on the road. In early 2019, a researcher demonstrated how he was able to access to thousands of cars and gained the ability to kill their engines. He did this by breaching two GPS tracking companies and accessing the accounts of over 30,000 people. Believe it or not, this incredibly hack hinged on the fact that the companies were giving users the default password of "123456." ("Hacker Finds he can remotely kill car engines after breaking into GPS tracking app." Motherboard, Apr 24, 2019)[3]. One can only imagine the ensuing difficulties for a driver on a major highway.

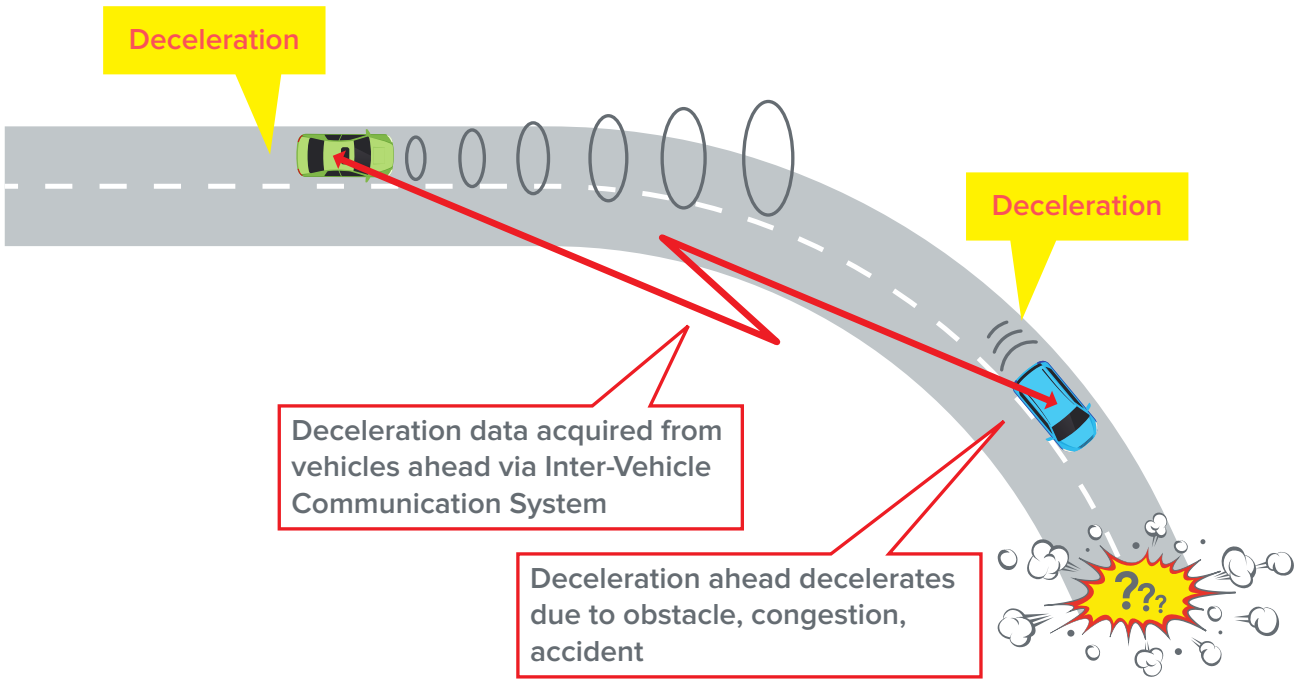
[2] *A Controller Area Network (CAN bus) is a vehicle bus standard designed to allow microcontrollers and devices to communicate with each other in applications without a host computer.*

[3] *https://motherboard.vice.com/en_us/article/zmpx4x/hacker-monitor-cars-kill-engine-gps-tracking-apps*

V2V and V2X Communications Can Multiply Consequences

Cars use vehicle-to-vehicle (V2V) communications to broadcast their speed, location, unique ID, and other data 10 times per second. Many automakers are looking to capitalize on this data to support new applications. For example, laser, ultrasound, and radar technologies can be used to gather data about road conditions and proximity to other vehicles. Camera imaging can detect markings on the road to keep a vehicle in the correct lane. The Advanced Driver Assistance System (ADAS) uses this capability to provide lane-departure warnings. Today's ADASs also use radar for collision detection warnings and adaptive cruise control, which allows a vehicle to follow the car in front of it. If the data being broadcast by a car is compromised, multiple vehicles can be affected.

If owners do not change the default factory settings and passwords, they potential could become an easy target. As the vehicle broadcasts signals, these signals can be hacked and used to override commands and cause the vehicle to slow or stop. They also can be used to infect other vehicles on the road. Hackers can track law enforcement officers through wireless scanners, just as law enforcement agencies can use the car's radar broadcasting signals to identify the car and how fast it is going. Because there are no current standards for how this data can be used, it isn't hard to foresee how a driver's own vehicle could be used to prove that the driver was texting, distracted by a DVD player, or in contact with someone committing a crime—all thanks to unsecured Bluetooth and Wi-Fi systems.



As ever-more-intelligent and autonomous cars appear on the scene, Vehicle-to-Infrastructure (V2X) communications can also potentially be used to create havoc. Vehicles use V2X to communicate with infrastructure such as traffic lights to help regulate traffic flow, and cell towers transmit the data to satellite-based systems that produce road condition and weather reports. Drivers' mobile apps also communicate with infrastructure such as tollbooth lanes and work zones, significantly expanding the attack surface of a connected car. Hacked V2X connections can be used to send false road condition reports, emergency notifications, or traffic updates—creating panic or huge traffic jams.

Both V2V and V2X communications are managed by On Board Equipment (OBE), which integrates with the CAN bus to provide information to vehicle systems. Not only does this integration demonstrate the critical need for security, it illustrates the potential for widespread unintended consequences when connected vehicles are not secure. It also illustrates the complexity of navigating through a connected-vehicle future. Securing the 30,000 components in the average vehicle will be challenging enough. Even then, as the technology and security industry is well aware, no means of security is 100 percent breach-proof.

Future Integrations

We're only at the beginning of achieving what many people envision for the connected car of the future. Consumer mobile apps already exist that can start the car and unlock doors. New apps will identify vehicles as a "member" of a service—a paid parking garage patron, authenticated entertainment service user, or billing subscription customer.

Internet of Things (IoT) capabilities are also being built into today's vehicles. A connected car adapter allows owners of NEST thermostats to program the temperature of their homes remotely. The adapter transmits an estimated arrival time, based on vehicle location and other factors, so that the thermostat adjusts the temperature at exactly the right time. Dozens of IoT product manufacturers already have plans for integrating cars with a "connected home experience." Aftermarket developers will merge vehicle platforms with other IoT platforms. For example, fleet management systems will consider vehicles as IoT endpoints connected to a centralized system to capture telemetry data, identify maintenance needs, and deliver software updates.

Although the applications mentioned above are designed to increase convenience, efficiency, and safety, attackers can just as easily turn them against the user. The ability to connect vehicle ID tracking with an app or smart-home IoT device can give an attacker the data needed to stalk a victim. The argument for securing connected vehicles only becomes more convincing.

When you consider the myriad points of connection inside a vehicle, with third-party products and services and with public infrastructure, the challenge of securing it all becomes infinitely more complex. Each integration point represents another potential attack vector into a vehicle and its related products and services. Security policies, design, and comprehensive testing processes must be included throughout the lifecycle of a vehicle.

Challenges to Securing Connected Auto Systems

Given the extensive coverage of network data hacks in the press, one would think that the similar systems built into vehicles would include baseline security measures. However, there are at least four major reasons why this isn't the case:

- **Long planning and production cycles.** According to the Auto Alliance (https://autoalliance.org)[4], it typically takes 5 or more years for a technology or new vehicle model to progress from design and testing to production and sale. Not only does this long lead time make it difficult to predict what types of security will be required, today's threats can morph and change within weeks.
- **Complexity.** Today's high-tech automobile typically includes 30,000 parts, all of which perform specialized functions in carefully specified ways. To secure 30,000 specialized parts from multiple vendors and ensure that they work as expected without conflict or malfunction is a huge, expensive challenge.
- **Added costs.** Auto buyers are usually highly sensitive to sticker prices. Adding a single 30-cent chip to improve encryption in a system can increase a car's cost by $50, once all of the sourcing, testing, packaging, and other costs are included. Given the large number of systems that lack security, it's easy to see how costs can add up quickly.
- **Unpredictable customer use patterns.** People use their personal technology in millions of different ways, which makes it difficult for automakers to predict which capabilities will meaningfully increase performance, be widely adopted, deliver the best user experience, or create a new competitive advantage. To further complicate matters, even when a feature set is chosen, it must be tested against all of the possible ways that security measures could be subverted.

[4] *https://autoalliance.org/innovation/*

How Spirent Can Help

As the technology industry has already seen, nothing is compromise-proof, and vehicle manufacturers must adopt this mindset as they design, test, and produce the next generations of connected cars and trucks. This is where Spirent Communications can add value.

Spirent provides innovative products and services that help the world communicate and collaborate faster, better, and more securely. We've worked with automakers since the late 1940s, helping them test and validate their designs and products. Today, we're helping automakers, including Tier 1 manufacturers, define security strategies, establish testing processes, and validate new designs. The Spirent auto industry team includes experts in security, computer electronics, engineering, components, and the automotive industry, all working together to help automakers and component manufacturers address important security priorities with a full range of services:

- **Security program design.** We design security programs from the ground up that are built on security and auto industry best practices and expertise in comprehensive wireless, cloud, application, and communications technologies, testing, and analytics. For manufacturers who want to incorporate security into vehicle lifecycle planning, Spirent has everything needed to expedite the process.
- **Already-built systems.** To help mitigate risk, Spirent provides testing, vulnerability assessment, and security recommendations for automotive systems already in production.
- **Vehicles in production.** Even vehicles in pre-production can benefit from Spirent testing. We can assess potential vulnerabilities and provide recommendations to help prevent exploitation of those vulnerabilities.

About Spirent Communications

Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks.

We help bring clarity to increasingly complex technological and business challenges.

Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled.

For more information, visit: www.spirent.com

As the industry moves forward, Spirent supports the development of industry best practices and standards to strengthen connected-vehicle security. At a minimum, best practices should be established for testing security in vehicles to ensure that the vehicle meets a baseline standard. Another best practice may be to give customers the ability to turn off entertainment systems or features. Industry standards should be specified for connected-vehicle systems and components. For example, security standards for the CAN bus can help ensure that automotive systems and components are secured consistently without introducing malfunctions. There is much work yet to do, and Spirent is committed to helping the auto industry take the next major step forward—to secure their products and provide the safest possible vehicles in our connected world.

spirent™
Promise. Assured.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com

Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com

Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

Rev C | 05/19