FireEye iSIGHT Intelligence

CONNECTED CARS: THE OPEN ROAD FOR HACKERS

SPECIAL REPORT / JUNE 2016

FireEye

INTRODUCTION

THE ACCELERATION OF THE "INTERNET OF THINGS" (IOT) REVOLUTION HAS INCREASED THE CONNECTIVITY OF PASSENGER VEHICLES, WHICH IS LIKELY TO IMPACT AVERAGE CONSUMERS SIGNIFICANTLY.

Today, most vehicle functions – steering, acceleration, braking, remote start, and even unlocking the doors – are controlled by software that accepts commands from a diverse array of digital systems operating both inside and outside the vehicle. However, this software contains millions of lines of code, and in these lines of code there may be vulnerabilities that can be exploited by individuals with malicious intent.

FireEye iSIGHT Intelligence analysts and Mandiant consultants reviewed the key threats to interior and exterior vehicle systems and assessed the top five threats created by vehicle software vulnerabilities. These include:

- Unauthorized physical access to vehicles
- Theft of personally identifiable information from manufacturer or third-party storage systems
- Deliberate manipulation of vehicle operation
- Hijacking vehicle systems to enable malicious cyber activity
- Extortion enabled by ransomware that renders vehicles inoperable until a ransom is paid

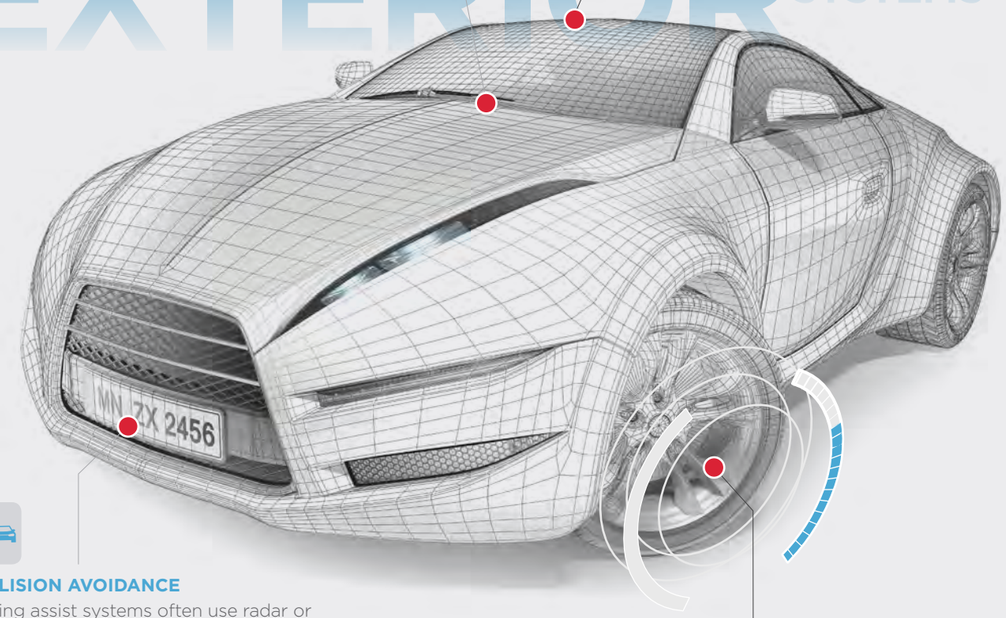
VEHICLE-TO-VEHICLE COMMUNICATIONS

Commonly referred to as V2V, vehicles will increasingly communicate with one another autonomously in order to assist with vehicle spacing and lane changing, while using other data that can improve vehicle operation.[1] Eventually, vehicle-to-infrastructure (V2I) will allow vehicles to communicate with traffic signals and road signs in order to better manage traffic flow and share data on road usage. Manipulating driver assist systems that use V2V or V2I could undermine safety and potentially cause collisions.

WI-FI INTERNET ACCESS

Wireless access points frequently featured in new vehicles raise the potential for abuse if they are poorly secured and connected to the vehicle's other systems. Ever-increasing bandwidth capabilities potentially increase the damage a malicious actor could cause.

EXTERIOR VEHICLE SYSTEMS



COLLISION AVOIDANCE

Braking assist systems often use radar or other sensors to detect an imminent crash. A compromised vehicle could send manipulated data to the ECUs that control this feature, either causing it to fail to engage or engage braking unexpectedly, leading to a forced stop or passenger injury.

TIRE PRESSURE MONITORING SYSTEM (TPMS)

Systems that monitor tire pressure frequently communicate over a short-range wireless connection that could be used as an infection vector for vehicle-specific malware. Multiple universities have already demonstrated vulnerabilities within the TPMS.[2]

[1] "Vehicle-to-Infrastructure (V2I) Communications for Safety," *U.S. Department of Transportation*, October 27, 2015, http://www.its.dot.gov/factsheets/v2isafety_factsheet.htm
[2] Bright, Peter, "Cars hacked through wireless tire sensors," arstechnica, August 10, 2015, http://arstechnica.com/security/2010/08/cars-hacked-through-wireless-tyre-sensors/

INTERIOR VEHICLE SYSTEMS

VEHICLE OPERATION ELECTRONIC CONTROL UNITS (ECUS)

The ECUs that control steering, braking, and acceleration can be manipulated in a compromised vehicle. The speedometer or engine temperature gauge can also be forced to show false data, either falsely indicating or masking vehicle malfunction.

KEYLESS ENTRY

Thieves have used signal boosters and interception devices to gain unauthorized access to locked vehicles through their keyless entry systems.[4] The latest trend in automotive innovation includes mobile applications for keyless entry and even remote start.

TELEMATICS SYSTEM

Many modern vehicles offer sophisticated telematics systems that incorporate the radio, Bluetooth and USB connections, GPS, and cellular assist functions. Most recently, vehicles increasingly feature Wi-Fi access points that provide a small wireless LAN to vehicle occupants. Each of these communications technologies offers a means to compromise and potentially control the vehicle.

ONBOARD DIAGNOSTICS (OBD) PORT

A self-diagnostic port where one can plug-in devices used to measure driving habits, conduct mechanical diagnostics, or enhance driver experience is a potential vector for malware.[3] For instance, a mechanic could inadvertently infect multiple vehicles using a compromised diagnostic tool.

CLIMATE CONTROL:

A vehicle's interior climate can affect a driver's comfort and therefore the ability to safely drive the vehicle. Manipulating climate control systems through compromised ECUs could blast the heat during the middle of summer, possibly forcing the driver to stop and exit the vehicle.

[3] Darren Pauli, "Mechanic computers used to pwn cars in new model-agnostic attack ," *The Register*, March 13, 2016, http://www.theregister.co.uk/2016/03/13/mechanic_computers_used_to_pwn_cars_in_new_modelagnostic_attack/
[4] Nick Bilton, "Keeping Your Car Safe from Electronic Thieves," *New York Times*, April 15, 2015, http://www.nytimes.com/2015/04/16/style/keeping-your-car-safe-from-electronic-thieves.html

RISK SECTION INTRODUCTION

While analyzing the current and potential risks to vehicles, FireEye reviewed published information to assess various threat scenarios, their likelihood of occurring, and their potential impact. We assess the top five risks created by vehicle software vulnerabilities to be:

Unauthorized physical access to vehicles

Theft of personally identifiable information from manufacturer or third-party storage systems

Deliberate manipulation of vehicle operation

Hijacking vehicle systems to enable malicious cyber activity

Extortion enabled by ransomware that renders vehicles inoperable until a ransom is paid

RISK 1

GAINING UNAUTHORIZED PHYSICAL ACCESS TO VEHICLES

Close access entry methods that enable unauthorized entry into vehicles are the easiest to conduct and therefore among the most common. They present the most immediate and realistic threat to technology-enhanced vehicles, notably because many vehicle manufacturers have opted to replace physical ignition systems with keyless systems that utilize mobile phone applications or wireless keyfobs.[5] Most unauthorized entry methods exploit the wireless communications between the vehicle and the keyfob carried by the driver.[6]

THREAT SCENARIO	Attackers exploit vulnerabilities in vehicle connectivity technologies to gain unauthorized entry or access to a vehicle.	
Likelihood	High	• Thieves have long sought to gain physical entry to locked vehicles. The ability to do so without incurring damage to the vehicle or leaving behind physical evidence lowers any deterrent factor. • Multiple close access and short-range exploitation capabilities could provide attackers with surprisingly easy access to otherwise secure vehicle spaces.
Impact	Medium	• Customers are less likely to purchase vehicles that are easily stolen or are vulnerable to the theft of of personal effects. • Insurance premiums for insecure vehicles are likely to be elevated due to increased risk of theft. • Manufacturers may be held liable for theft of insecure vehicles, and regulation may stipulate vehicle cyber security ratings similar to those already required for crash tests and fuel economy.[7]

[5] Paul Einstein, "Bye-bye, car key? Keyless systems taking over," *CNBC*, December 14, 2014, http://www.cnbc.com/2014/12/12/bye-bye-car-key-keyless-systems-taking-over.html
[6] Andy Greenberg, "This Hacker's Tiny Device Unlocks Cars and Opens Garages," *Wired*, August 6, 2015, http://www.wired.com/2015/08/hackers-tiny-device-unlocks-cars-opens-garages/
[7] Doug Newcomb, "Michigan Senator Proposes Auto Industry Step Up Cybersecurity Efforts To Avoid Legislation," Forbes, March 30, 2016, http://www.forbes.com/sites/dougnewcomb/2016/03/30/michigan-senator-proposes-auto-industry-step-up-cybersecurity-efforts-to-avoid-legislation/

RISK 2

STEALING PERSONALLY IDENTIFIABLE INFORMATION

Collecting personally identifiable information (PII) is a high priority for many criminals, hacktivists, and nation-state threat actors. Modern vehicles collect significant amounts of PII in the course of their operation in order to interface with the myriad of after-market devices that communicate with the vehicle's operating system. As a result, vehicles can now become an additional attack vector for parties interested in stealing financial information. This novel attack vector could also be extended to accessing pattern-of-life data – ostensibly innocuous data concerning travel destinations, driving style, and potential speeding or traffic violations.

In addition, automated maintenance or diagnostics services that communicate with a dealership may also offer a potential attack vector for criminals seeking PII held on dealership or manufacturer systems. Laws stipulating protection and storage requirements (both locally and cloud-based) for vehicles are still immature, meaning privacy policies among manufacturers are inconsistent and consumers are potentially left vulnerable to exploitation.

Threat actors may be interested in the following types of information that could potentially be accessed through a vehicle's system or stored on the vehicle itself:

VEHICLE INFORMATION	PERSONAL INFORMATION
Make, Model, Year	Owner Name, Address, Phone Number, Email
Global Positioning System Location and Speed	Owner Demographic
Vehicle Identification Number	Social Security Number
System Diagnostics	Mobile Phone Contact Lists
When the Vehicle Is On or Off	Mobile Application Logs and Configuration

Some attacks leverage multiple types of stored information. One example concerns a stolen car's GPS information, often containing a "Home" destination that would reveal the owner's home address. When combined with stored garage codes, a vehicle compromise has the potential to pivot to home burglary. As automotive telematics systems increase in complexity and offer more features, the attack surface could expand to include email, banking, and other sensitive mobile applications.

THREAT SCENARIO	Automobile data storage systems are breached, resulting in the theft of customer PII.	
Likelihood	High	• In the case of cloud storage, a car dealership or manufacturer may face targeted intrusion attempts by both criminal or nation-state-sponsored threat groups in search of PII. • In the case of local automotive storage, this may be an attractive target for local physical access to drivers' homes, boosting incentives for criminals. • Since mid-2014, we have observed several instances in which suspected state-sponsored threat groups deliberately targeted large stores of PII in other industries, such as government and healthcare.
Impact	Medium	• Negative press attention related to the industry's ability to safeguard sensitive PII. • Government regulation in response to exploitation incidents may raise industry compliance costs. • Litigation related to third-party breaches facilitated through stolen PII. • Costs related to credit monitoring services for affected customers.

RISK 3

MANIPULATING A VEHICLE'S OPERATION DELIBERATELY

Vehicle security researchers Charlie Miller and Chris Valasek demonstrated their ability to remotely hijack a vehicle's systems while in operation of a vehicle while in operation on a St. Louis highway.[8] As vehicles become increasingly connected to the Internet with an ever-growing roster of features and capabilities, we will see an increase in the options available to malicious actors to exploit vulnerabilities inherent in these expanded capabilities.

THREAT SCENARIO	Malicious actors or criminals commandeer a vehicle's control systems and deliberately crash it or injure the driver.	
Likelihood	Medium	• Long-ranged attacks are difficult to execute, and require extensive research of specific vehicle vulnerabilities. • Criminals and other actors are more likely to find improved return on investment through data theft rather than deliberate property destruction or personal injury.
Impact	High	• Personal injury, property destruction, and severe traffic congestion are all potential consequences of a successful deliberate vehicle crash. • Auto manufacturers may be held liable for improperly protected vehicles. • Drivers are likely to avoid purchasing vehicles deemed to be dangerous due to software vulnerabilities.

[8] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me In It," *Wired*, July 21, 2015, http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

RISK 4

USING VEHICLE ELECTRONIC CONTROL UNITS TO SUPPORT MALICIOUS CYBER ACTIVITY

Today's average automobile has around 70 Electronic Control Units (ECUs),[9] several networks including WiFi and 4G, and the potential for gigabytes of digital storage.[10] In a practical sense, a modern automobile is comparable to a modern computer network that is made up of computers, local and wide area networks (LAN/WAN), and file servers. Malicious activity has continued to follow advances in technology, as we now see with exploitation of mobile devices and infrastructure.[11] It is plausible to consider that cyber threat actors could view the automobile as the next frontier to support malicious activity.

Today, relatively few vehicles feature the connectivity needed to act as worthwhile command and control nodes for cyber activity. However, as more vehicles are connected to the Internet with other services that all demand greater bandwidth, the possibilities for compromise and hijacking will also rise.

THREAT SCENARIO	Vehicle ECUs or other components are compromised and repurposed to support other malicious cyber activity.	
Likelihood	Low	• Relatively few vehicles feature the comprehensive connectivity required to act as infrastructure nodes for a cyber activity campaign. • Likelihood will increase as more vehicles are connected to the Internet and other communication services.
Impact	Low	• Vehicles themselves are unlikely to suffer major deficiencies in operation, particularly because the actors hijacking the vehicle's components will attempt to keep their presence invisible to the owner. • Investigations into vehicle compromise could disrupt drivers' use of their vehicles during such an investigation, harming brand reputation. • Unsuspecting victims of ECU hijacking may also be charged with complicity in the malicious activity.

[9] Robert N. Charette, "This Car Runs on Code," IEEE Spectrum, February 1, 2009, http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code
[10] Toshiba Semiconductor & Storage Products, Storage Solutions for Automotive Infotainment Systems, http://toshiba.semicon-storage.com/ap-en/product/automotive/info-storage.html
[11] Yong Kang, Zhaofeng Chen, Raymond Wei, "XcodeGhost S: A New Breed Hits the US," FireEye Blogs, November 03, 2015, https://www.fireeye.com/blog/threat-research/2015/11/xcodeghost_s_a_new.html

RISK 5

EXTORTING VICTIMS THROUGH RANSOMWARE DEPLOYMENT

So far, ransomware has mostly targeted individual users and companies, hoping that ordinary people and firms will pay a few hundred dollars to unencrypt the files on their personal computers. More recently, ransomware has hit police stations and hospitals – organizations that may have very little choice to pay if backups are insufficient. Reports indicate some have paid thousands of dollars – often in an anonymous currency such as Bitcoin – to regain control of their systems.[12] Given this shift in targeting to capture increased revenue, criminals would be incentivized to develop and deploy ransomware to vehicles, especially given the public's heavy reliance on vehicles for daily activites – particularly in the United States. It is reasonable to predict that both individual consumers and businesses would pay thousands of dollars to regain control of a vehicle that originally cost them tens of thousands of dollars.

THREAT SCENARIO	Vehicle ECUs are rendered inoperable by ransomware	
Likelihood	Low	• To date, no ransomware samples specifically designed for vehicle systems have been used or made public. • Targets of ransomware have evolved from ordinary users' computers to larger organizations, of which hospitals are especially concerning.
Impact	High	• A vehicle's importance to the public means ransoms are likely to be paid, raising the financial incentive for cybercriminals to build and deploy ransomware designed for vehicles. A single driver may be able to reinstall software with a mechanic's help. • Public disruption could escalate rapidly if an entire highway of vehicles were rendered inoperable by ransomware.

[12] Richard Winton, "Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating," Los Angeles Times, February 18, 2016, http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html

Given the emergence of these new risks, automotive manufacturers and suppliers not only need to ensure the traditional operational safety of their vehicles, they also need ensure the security of both the vehicle operations and driver privacy. This requires an ongoing understanding about the nature of threats and vulnerabilities in a rapidly evolving landscape, and building in strong proactive security measures to protect against those risks. A one-time risk assessment is not enough since threat attackers are consistently evolving.

FireEye combines our industry-leading threat intelligence, incident response and red team capabilities with our ICS domain expertise to help the automotive industry improve their prevention, detection, and response capabilities. FireEye's Red Team Operations and Penetration Tests can provide firms in the automotive industry experience responding to real-world attacks without the risk of negative headlines.

Red Team engagements are goal oriented to evaluate whether a determined attacker could accomplish particular goals such as stealing sensitive information or taking control of a device or system, while penetration tests assess the preventative security controls in place for specific areas of critical systems and networks, such as applications, IoT, and wireless technologies.

FireEye iSIGHT Intelligence's Horizons Team conducts strategic forecasting to anticipate risks posed by emerging technologies and geopolitical developments, helping clients and the public better assess their exposure to a dynamic cyber threat landscape.

For more information, contact FireEye.

www.fireeye.com/redteam.html

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035
408.321.6300 / 877.FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye