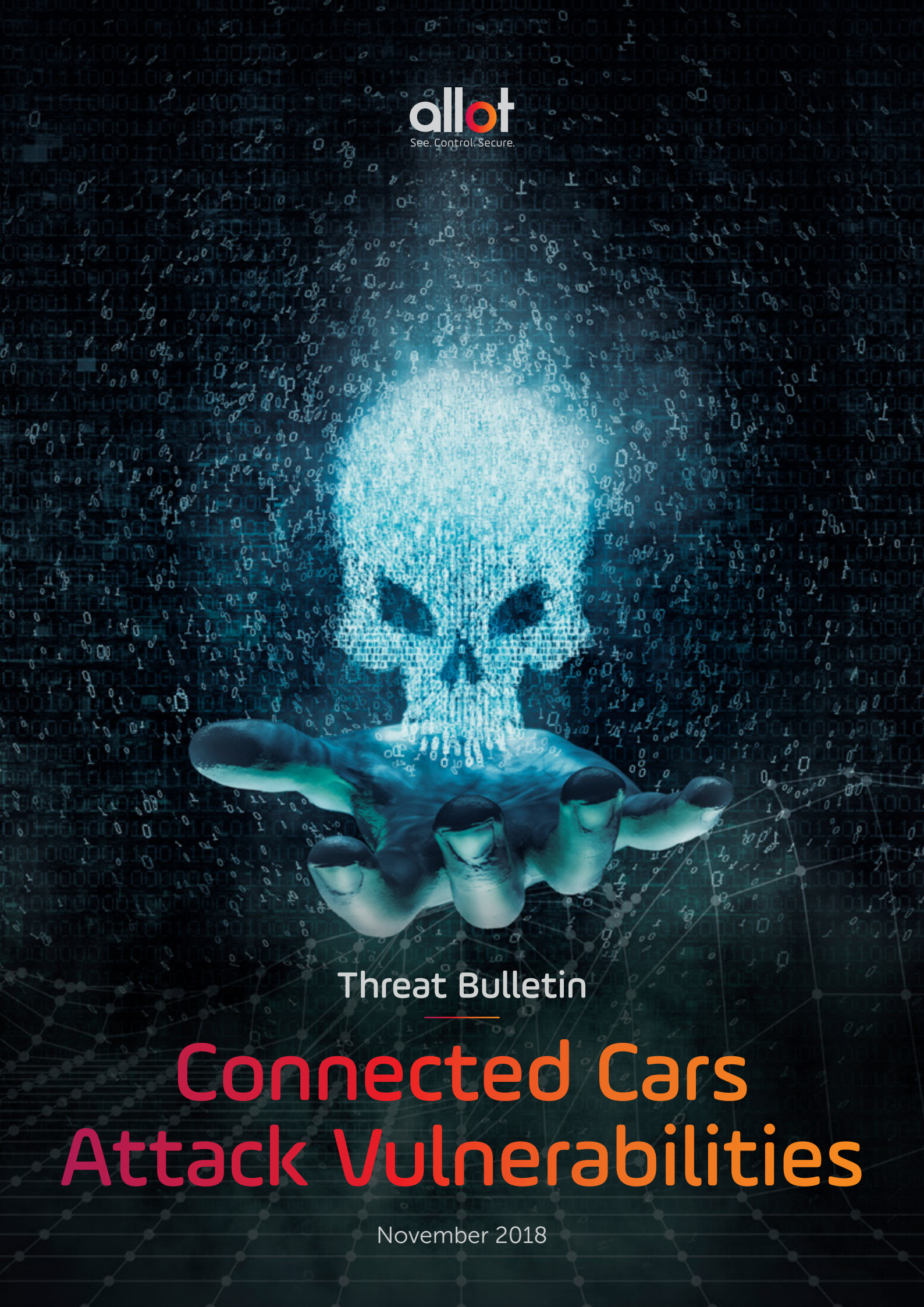

Threat Bulletin

Connected Cars Attack Vulnerabilities

November 2018

Connected Cars: Auto Attack Vulnerabilities

Imagine the following two scenarios:

Scenario 1 | A computer hacker remotely unlocks your car, disables the alarm system and steering lock, starts your car, and drives it away.

Scenario 2 | You are driving along the highway on a fine summer's day when your windshield fluid sprays onto your windshield, your radio immediately ramps up to full volume, your steering wheel develops a mind of its own, and your car then grinds to a halt in the fast lane.

While the first scenario would likely ruin your day, nobody got hurt. The second scenario could result in you losing your life.

The classic case of the Jeep Cherokee auto hijacked by professional hackers Charlie Miller and Chris Valasek in 2014 brought the real threat of connected car hijacking to public awareness. Their attack led to the recall of 1.4 million of the prestigious vehicle and the knowledge that smart car manufacturers had a problem on their hands.

Modern cars can be thought of as computers on wheels with each smart automobile containing more than 100 million lines of computer code in the Electronic Control Units, or ECUs that control systems from windshield wipers to brakes and steering. Gain access to those systems then there's just about nothing that will prevent a determined hacker from controlling or attacking your car.

The origins of computer connectivity in automobiles began with the 1990 Clean Air Act that came into force in the US, which compelled car manufacturers to enable systems to monitor the exhaust of the cars they produced. This resulted in the installation of on-board diagnostics ports that provided direct access to automobile systems. These ports were standardized to enable car mechanics to download diagnostic information to comply with government reporting regulations. The OBD-II is the current generation of the data portal used in most automobiles manufactured today, which are expected to reach 100% connectivity penetration in Western Europe by 2020.

Initially, the OBD-II port required physical access to obtain diagnostic information from an automobile. However, with the widespread use of Wi-Fi, cellular networks, and Bluetooth connectivity, remote access to the diagnostic ports have become the norm. OBD-II ports are now open for business as automobile manufacturers are tripping over themselves to make their cars the most connected on the market. On-board Wi-Fi, GPS, access points, and Smart radios are the norm, and there appears to be no chance to stop the connectivity revolution. However, due to the wireless accessibility that is now available with connected vehicles, so comes the risk from cyberattack from a range of malicious actors. These include the usual suspects who can hack a smart vehicle and demand payment for its repair to a disgruntled ex-employee who could nobble the entire fleet of their former employer.

Attack Surfaces

The top threats faced by connected car manufacturers and their customers include the following:

Vehicle Telematics: Hackers can intercept telematics traffic using GSM. They can use passive sniffing to locate the unencrypted data that enables them to perform a Man-in-the-Middle (MITM) attack.

SMS API: Hackers can spoof the SMS commands, sending direct commands to the device.

Web Interface and Mobile APIs: Hackers open accounts on a web interface using parameters such as SIM numbers. By exploiting a Web application, the attacker then obtains access to even more credentials.

Mobile Apps: Hackers attack mobile app vulnerabilities that provide access to auto systems such as radio. The attacker can then play file across multimedia devices.

Entertainment System: Hackers can create multimedia files that can change code on the system. This opens pathways to exploit the system and even spy on other parts of connected vehicles.

Firmware Upgrades: During firmware upgrades, the system must not accept external data. Failing to do so can result in backdoor attacks linking the automobile to the attacker's system.

Wireless Media: Hackers can attack vulnerabilities in wireless channels such as Bluetooth or Wi-Fi, which can bypass administrative privileges.

External Sensors: Hackers can spoof external sensors and force the vehicle into taking unwanted actions.

Wireless Key Entry: Hackers exploit wireless key entry by using a proxy bridge between the key and the automobile enabling them to lock or open the automobile at will.

External Device Access through the OBD-II Port: Could enable hackers to obtain access to the vehicle's internal systems.

Attacks on the Cloud Service of Automotive Provider: Could potentially enable the hacker to attack many cars with the one attack.

Technically Speaking

Modern cars contain a range of mini-computer devices known as Electronic Control Units, or ECUs. These components control all the automobile's systems including transmission, steering, and electrical peripheral devices. ECUs operate within Controller Area Networks or CANs that enable ECUs to operate at high speeds. As driver control of a motor vehicle has become less autonomous, so automotive computers are performing more and more calculations on the driver's behalf. Paramount of all aspects of the driving experience must be driver safety. As one observer noted, if your computer crashes, it may result in a bad day. If your automobile systems crash, it may result in the loss of your life.

New cars have multiple access channels to the Internet. The OBD-II port provides open access to all of a vehicle's CAN buses, which could ultimately lead to manipulation of CAN traffic by outside hackers. Generally, CANs offer no security protocols, which led to the US Department of Homeland Security charging Carnegie Mellon's CERT Coordination Center to perform security analyses to determine the vulnerability of connected cars. The results showed significant gaps in the measures taken by connected automobile manufacturers to make their vehicles safe.

The OBD-II port is a 16-pin connector port, which most automobile manufacturers have enhanced to provide additional connectivity.

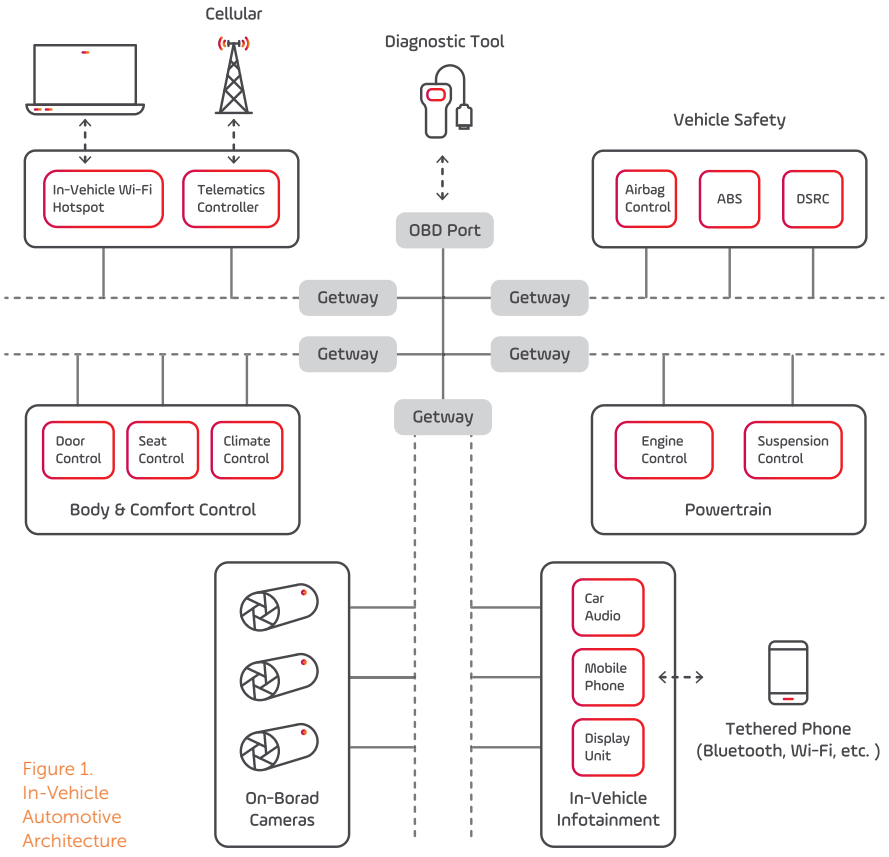

Figure 1. In-Vehicle Automotive Architecture

For example, General Motors created its LAN bus and Chrysler developed its CCD (Chrysler Collision Detection). These connectors, which are used to update software on the ECUs, link to other buses in the vehicle itself to perform additional testing.

The CAN protocol suffers from several security issues. These include:

- The OBD-II was originally designed for physical access, and security was a secondary concern
- Speed and timing are given preference over security

Such security vulnerabilities can easily result in exploits that can be leveraged by malicious individuals.

Risk Vectors

When assessing the potential risk faced by the drivers of connected, or semi-autonomous cars, a range of risk vectors must be considered. These range from the most critical including driver distraction, engine tampering, and steering control, any of which could result in fatal injury, to less critical vectors such as vehicle theft, insurance or lease fraud, and the loss of personal information. These risk vectors affect not only smart or self-drive cars, but also older cars that contain an OBD-II connection port

Solutions to Connected Car Vulnerabilities

Some solutions to the issues raised from connected car vulnerabilities include:

- In-Car Security Solution: Involves isolating safety-critical systems (for example, enhancing the ECU or communication channels) to reduce the effect of successful cyberattacks. In many cases, this includes incorporating real-time intrusion monitoring to detect potential attacks to the systems.
- Network-Based Solution: This approach can be very efficient in reducing many threats vectors for vehicles are Internet-connected including old cars with connected ODB port. This solution protects communication between vehicles and the automotive cloud, and other communication sources connected to the network. This solution should also incorporate Artificial Intelligence and Machine Learning security capabilities for identifying suspicious behavior. The objective of this approach is to protect the entire vehicle ecosystem.

Conclusion

Fortunately, there are many steps that car manufacturers can take to harden vehicle security. These include:

- Deploying network security that monitors IoT devices, such as connected cars
- Separating CAN communications from the network stack, which keeps CAN frames disconnected from external networks
- Signing and encrypting of firmware updates
- Enabling security by default

All software has vulnerabilities, but OBD-II devices are more sensitive due to the potential physical impact on the connected vehicle driver. Connected vehicle drives must pose the following questions to automobile manufacturers:

- How are automobile systems updated?
- Do the automobile systems use strong encryption when it is updated?
- Does the automobile send CAN information to the Internet?
- Does the vendor maintain a vulnerability disclosure policy?

Cyber carjacking is not easy, and the number of successful cases remains relatively low. However, with approximately 70% of Americans wary of motor vehicles with self-drive features, it is clear that most of the work in this area remains to be done.

Note that not only new connected cars are vulnerable. As mentioned above, older cars with Wi-Fi or cellular SIM card enabled ODB-II connectors can also become targets. CSPs must provide secure connectivity and protect the cars on their networks. Communication security must be one of the factors for Cloud Automotive Service Providers when choosing connectivity providers. Also, network-based security will enable them to identify abnormal behavior of their managed cars using artificial intelligence techniques to pinpoint anomaly activity.

Are you concerned about attacks on connected cars?
Allot's IoTSecure can assist.

Contact Allot »