Automotive Cybersecurity for Connected Cars

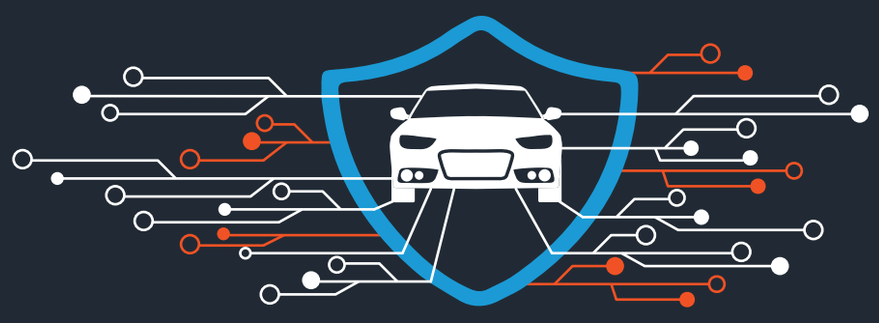
Because of software, cars are increasingly connected to the internet and becoming "smart." If properly equipped, they can also update their software remotely using over-the-air (OTA) technology and cloud-based service delivery. This automotive OTA revolution will provide many benefits for automakers and consumers alike, such as improving existing features; adding brand new features; and fixing software bugs without expensive, manual recalls and the consumer inconvenience of taking cars into dealerships for software related servicing.

However, along with the benefits of software updates and an internet connection comes a software related risk: cybersecurity threats. Most consumers are familiar with security concerns on their personal computers and smart phones. When these devices are compromised, damage to the hardware and software, theft of personal data and information, financial repercussions, and other annoying inconveniences can result.

Cybersecurity is taken very seriously in the automotive industry because human lives are at stake. Ideally, all connected vehicles should be continually monitored to detect, protect, and mitigate cybersecurity attacks. Fortunately, the automotive industry is collectively and individually focused on making rapid advancements in these areas—which are all reliant on the ability to perform software updates whenever necessary.

Security Model Cycle

Threat Prevention



The first opportunity to address cybersecurity is when a vehicle is initially designed and enters production. Automakers and suppliers need to collaborate closely to understand threat vectors and attack surfaces to ensure the latest architecture, technology, and processes are employed for the best protection possible.

Threat Identification

After a connected vehicle has been purchased, cybersecurity prevention shifts to continuous monitoring, vulnerability identification, and intrusion detection. Software embedded in the vehicle and running in the cloud work together to spot suspicious activity and known threat patterns. Once detected, intrusion alerts are issued to appropriate parties for mitigation planning.

Threat Mitigation

Once a cybersecurity threat has been identified and a mitigation plan developed, remote over-the-air (OTA) software updates can be used to resolve security issues and restore protection for impacted vehicle components and systems. Mitigation tactics can also be shared with other entities to stop the proliferation of cybersecurity threats across other vehicle brands and models.

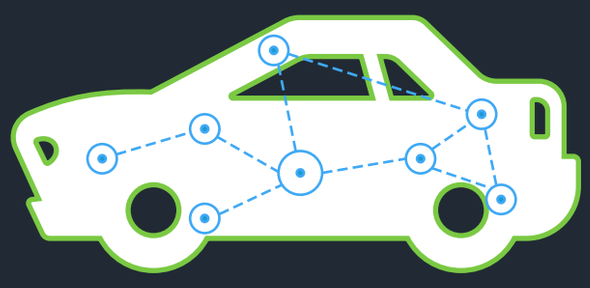
Airbiquity OTAmatic™

As a connected vehicle service delivery provider, Airbiquity plays a role in helping prevent cybersecurity attacks for our automotive customer's vehicles. When designing OTA solutions, Airbiquity follows a "defense-in-depth" approach where multiple security layers defend, minimize, and isolate cyber attacks. This limits the initial damage from breaches, while also allowing time for the development of mitigation actions to prevent additional damage. A key element of Airbiquity's OTAmatic™ OTA software and data management product is the integration of Uptane—an innovative and open security system for connected vehicle software updates.

Uptane: The First Compromise-Resilient Software Update Security System Designed for Automotive

100% Automotive

Unlike other security protocols which may have been shoehorned into automotive applications, Uptane was specifically designed to address comprehensive threat models for a highly complex vehicle with multiple electronic control units (ECUs). Uptane is particularly well suited for automotive applications today and in the future, including advanced driver assistance systems (ADAS), vehicle-to-everything (V2X) communications, and fully autonomous driving.



Strong Lineage

Uptane is based on The Update Framework (TUF), a highly robust and proven method for securing software updates that has been adopted by the Linux Foundation. Uptane's development is led by notable transportation, security, government, education, and research organizations.

- Department of Homeland Security (DHS) Grants D15PC00239 and D15PC00302
- New York University Tandon School of Engineering (NYU)
- University of Michigan Transportation Research Institute (UMTRI)
- Southwest Research Institute (SWRI)

Open Specification

The Uptane organization has put great effort into soliciting input and feedback from automakers, automotive suppliers, security professionals, and broader security communities across North America, Europe, and Asia. This all-inclusive approach is valuable because it provides an assurance that the protocol is thoroughly peer reviewed, audited by third parties, and meets the desired automotive requirements.

Compromise-Resilient

Uptane manages automotive security compromises using a "defense-in-depth" approach that favors multiple layers of security instead of relying on a single security mechanism. Uptane makes it extremely difficult for hackers to install malware on vehicles, even if cryptographic keys have been compromised. And because many security compromises are planned for in advance, there are clearly defined fixes that can be quickly deployed when the need arises.

Corporate Headquarters 1191 Second Avenue | Suite 1900 | Seattle, WA 98101

Web www.airbiquity.com **Email** contact@airbiquity.com **Phone** +1 206 219 2700

Airbiquity®