Application Security in the Connected Automotive Ecosystem

21 September 2020

Over the last few years' it has become standard for automotive OEMs to provide mobile applications that enable vehicle owners and users to interact with the vehicle.

These applications provide a wide range of capabilities from being able to see how full the tank is, to remotely starting the vehicle through to advanced diagnostics. More recently the concept of digital car keys has started to become a key use case that is gaining popularity in the automotive world. BMW recently announced a collaboration with Apple to support this and earlier this year the Connected Car Consortium (CCC) released its Digital Key Specification Version 2.0 which is expected to be widely adopted by OEMs.

However, while mobile companion applications for Vehicles undoubtedly bring multiple benefits to vehicle users' they also bring new challenges as well. Unsecured mobile devices that interact with vehicle systems introduce a new set of potential attack vectors that hackers are increasingly seeking to exploit. Hackers can focus on leveraging exploits within the mobile device OS to install malware that can sit dormant until it detects that the mobile device has been connected to a vehicle, for example over Bluetooth, Wi-Fi, or NFC, and will then attempt to launch its attack against the vehicle and or its connected services.

As vehicles become more digital and learn and store more information about drivers and passengers (either within the vehicle or in related cloud services), the prize hackers from compromising a vehicle becomes more lucrative. Vehicle attacks are no longer just about stealing the vehicle or forcing the vehicle to behave in ways the driver did not expect. Attacks are increasingly about stealing personal information; ranging from profile history to usernames, passwords, and financial information.

A report published earlier this year by Upstream Research, UPSTREAM SECURITY'S GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2020, underlines this issue. Mobile applications are now in the top three most common attack vectors, along with keyless entry systems and backend server platforms. Such attacks are not just targeted at the vehicle itself; they are intended to pass malicious code on to the back-end server platforms. These platforms provide features such as vehicle tracking and access to additional vehicle systems such as engine management and telematics.

The challenge is not just confined to applications provided direct by the OEMs, but also resides in the ecosystem for aftermarket solutions. These are often connected into a wider set of systems inside the vehicle) such as ODBII dongles, alarm systems and audio solutions, all of which are increasingly being supplied with their own applications and services.

The rise of the sharing economy and the growth in popularity of ride and vehicle sharing services also increases the risks of attacks. With a growing trend to provide advanced services via IVI and Rear Seat Entertainment options, further increases the challenges, and these factors all contribute to the risks created from unsecured mobile devices interacting with vehicles.

What can the automotive ecosystem do to ensure that mobile applications do not pose a critical threat to vehicle security?

One approach that can be taken is to embrace the advanced capabilities embedded into mobile device platforms, that are designed to enhance the security of sensitive mobile applications. For example, the automotive cybersecurity solution, that leverages a Trusted Execution Environment, which is found in all modern Android devices, provides a protected environment for running Trusted Applications and Drivers, performing cryptographic operations and providing secure access to memory and peripherals.

By using such an approach, applications can be developed where the critical code is running in a secure, isolated, environment. Therefore, even if the main operating system on the device has been compromised the application, and its data, will remain protected from malware and other attacks. Furthermore, by using secure drivers, for features such as input devices, the display and biometrics, a Trusted User Interface (TUI) can be provided for all forms of user interaction with the application. This will prevent attacks such as silently capturing screen images, key logging or listening in to audio streams. Importantly such protection can be provided without compromising the usability of the applications and services.

As more and more digital services are rolled out in vehicles, with connected car applications such as digital agents, advanced content stores, and the ability to transact direct from the vehicle, security of the end to end ecosystem will become increasingly important.

Applications will play an ever-important role in how we interact with vehicles regardless of it we own them, rent them or are using public transport.

At Trustonic we believe that robust Application Security will play a key role in the digital evolution of the automotive industry.

Learn more:

https://trustonic.com/application-security/

TRUSTONIC

info@trustonic.com
trustonic.com

200 Cambridge Science Park,
Milton Road, Cambridge, CB4 0GZ. UK

Registered in England with
Company Number 07890730