print | close

5 Questions Automotive Designers Should Ask About Hacking

Electronic Design
Johannes Lintzen
Mon, 2015-12-21 16:00

By 2020, three-quarters of all cars shipped globally will be built with Internet-connection hardware. In the average modern car, more than 80 microcomputers communicate internally to control everything from the stereo to steering wheel, and all of those internally connected devices interface with the outside world via Wi-Fi or mobile telephony. But when the car turns into the "Internet on Wheels," how do we keep it safe from crashes, hackers, and privacy breaches?

Risks associated with rapidly growing connectivity include unauthorized access and malicious control. Just recently, white-hat hackers proved how they could remotely commandeer a Jeep Cherokee to come to a dead halt, blast the music, and max the air-conditioning. Though the means of securing any connected device boils down to the same core technology solution, the threat of a hacked car becomes far more severe and complex when we trust the integrity of these connections with our lives.

Related

Car-Hacked! Flaw in Jeep Revealed

What Does It Mean To Secure the Internet of Things?

M2M Connects Your Car To The World

One of the main benefits of the connected car is the very fact that it enables over-the–air (OTA) updates. With OTA, mandatory updates can be loaded remotely into the vehicles' systems without requiring costly recalls and unpleasant visits at the dealership for the customer. On the flip side, this capability adds another attack surface. Remote software updates require a process of verification to identify and block communication commands before they find their way into the vehicle system.

Why We Need To Go Beyond Encryption

Securing connections and providing authentication as well as non-repudiation in the Internet of Things (IoT) is a highly complex and multifaceted challenge—one that the embedded industry is already taking steps to outline and define. The same security challenges that apply to connected devices in general also apply to the connected car.

A typical go-to answer is encryption: Encrypt everything and you'll be secure. In the case of securing commands and communication in the connected car, however, encryption won't help. How do we secure over-the-air updates and critical in-car communications like steering, brakes, airbags, and tires, as well as non-critical ones like entertainment and climate control?

Encrypting data means encoding information in such a way that only authorized parties can read it. In IoT, the

ical security element consists of validating the communication commands between different and multiple nected components, i.e. the moment when the device unlocks the encrypted transmission from another device to execute the required action.

Validation occurs by:

• Ensuring that all connected components that constitute the car are kept secure and untampered with, despite multiple suppliers and throughout the lifetime of a car in the hands of different owners.

• Ensuring that the cryptographic keys used to unlock the device transmissions are created and managed in such a way that they remain unique and uncompromised.

These challenges come into play once the car is connected, which occurs in the field when the cars' firmware is updated—not in the secure production environment.

Assigning a Birth Certificate to Components

Cryptographic keys work as digital signatures that provide connected devices with a chain of trust. They form a trust anchor, if you will, that ensures authenticity and integrity in all device communications. These unique keys work as "birth certificates" to provide undisputable identity and guarantee that every action initiated by a smart device is authenticated and reliable, without third-party obstruction. Properly deployed in the case of the Jeep Cherokee hack, the hackers' signaling device would have been identified as a false sender of the command, making the remote commandeering impossible.

The connected car's chain of trust begins with validating the components at the manufacturing level and throughout the supply chain. By coding a cryptographic key into the connected device, or *seeding the chip*, at production time, identity—and trust—become embedded into the connected component before it even leaves the device vendor's facility. But how can automotive designers maintain that security from the point of manufacturing to commercial deployment?

To maintain the integrity of the car's cryptographic key material from point of production to commercial deployment, automotive designers need to consider continued key management to avoid compromised, cloned, or mismanaged keys. To handle the distribution and use of cryptographic material embedded within the vehicle system, an embedded key-management system will manage both code signing and verification of firmware updates, including automatic upgrades via OTA connections.

Where Did I Put My Crypto Car Keys?

There are different means of creating a cryptographic key via *pseudo* (software engineered) or *true* random-number generation (based on randomly occurring anomalies in physics), and of storing a cryptographic key.

Hardware-security module technology offers secure key storage even in the most hostile environments. The module can detect when any attack toward the key storage is happening, including drilling, heat, power blackout, or chemical attack, and automatically delete the keys immediately. In comparison, software-based cryptographic keys can be captured in the moment of unlocking, offering attackers the ability to learn the software, exploit vulnerabilities, and run attacks remotely.

In the connected car, computer systems (ECUs) embedded in the car need to have a physically secured area to store these unique crypto keys, with which the systems can prove the identity of all components and sign command messages. At the other end, the receiving ECU needs to have the ability to verify and unlock those crypto keys to validate the command before executing it. With hardware-based crypto-key storage and management, the various systems communicating over the central bus in the vehicle can communicate while

intaining the chain of trust via identifiable crypto keys.

Complementary next-generation solutions to secure the connected car include innovations such as Ethernet over fiber; enabling cryptographic solutions that scale with complex automotive systems; and mobile software-management solutions that securely manage all software in the car, including head units, ECUs, and telematics boxes—whether on the production line, at the dealer's lot, or the owner's driveway.

Looking Forward: 5 Questions to Avoid the Next Car Hack

For automotive designers working to ensure that a hack like the one on the Jeep Cherokee never happens again, there should be asking five questions about securing the connected car:

1. Is the supply chain secure? Can you be sure all of the car's components are real and not counterfeit?

2. Does the car's embedded computer system have a physically secure area to store certificates and cryptographic IDs? And does the receiving computer system have the ability to verify those signed messages by checking them against a chain of trust?

3. Once the components are embedded into the larger ecosystem that is the car, how can you ensure the various systems' communications over the central bus in the vehicle can communicate in a trusted manner?

4. How can you ensure all processes related to the software function of the car are covered by safeguarding measures, including development and production, at dealerships and service organizations?

5. Does your security solution cover all V2X communications? Including car-to-car communication, car-to-infrastructure communication, and roadside to vehicle communication? Or what about over the air updates? And lifecycle management?

The connected car is a thing of beautiful engineering and I'm sure it will make for some truly enjoyable road trips, aided by innovative command control and increased safety. With a hardware-based trust anchor, each connected device is supported from the point of production throughout its lifecycle, providing the root of trust that both vendors and drivers demand and anticipate before they hit the road.

Source URL: http://electronicdesign.com/embedded/5-questions-automotive-designers-should-ask-about-hacking