WHITE PAPER

SECURING AUTOMOTIVE IS CRUCIAL IN TODAY'S CONNECTED WORLD

A LOOK AT THE KEEN SECURITY LAB ATTACK OF THE TESLA MODEL S AND WAYS TO SAFEGUARD INTERNAL AUTOMOTIVE ECOSYSTEMS

Entrust Datacard™

Josh Jabs, Vice President, Office of the CTO and General Manager, IoT Solutions
Ranjeet Khanna, Director of Product Management – IoT and Embedded Security

“**Connected automobiles** will account for more than **82%** of cars sold by **2021**.”

Connected automobiles will account for more than 82 percent of cars sold by 2021. That means that in a few short years, the majority of cars on the road will essentially be data-centers on wheels.

This represents a huge opportunity for auto manufacturers and tech companies who supply connected services to the industry to create unique driving experiences and new channel growth. But, with innovation comes risk, which has been proven on several occasions in recent years by security researchers who hack into connected vehicles and shine a spotlight on vulnerabilities that could result in significant safety and privacy threats.

Keen Research Lab is the latest to highlight these risks in an ethical attack it launched on the Tesla Model S. The following analysis will take a look at connected car innovation, explore the details of the Tesla attack, and offer tips and solutions on ways to help ensure a secure automotive IoT – from supply chain through manufacturing, to initial ownership and the entire life cycle of the vehicle – to protect drivers and passengers in and around these innovative automobiles.

> “Connected cars improve safety of a vehicle by alerting drivers to weather warnings or other potential safety hazards.”

INNOVATION IS DRIVING THE AUTOMOTIVE INDUSTRY

It’s remarkable how much innovation has already happened when it comes to the connected automobile industry. Already, connected cars have enhanced the driving experience by improving:

- Infotainment. This audio/video hub has brought the driver and passenger experience to a new level, equipping cars with passenger video systems, Bluetooth voice and text capabilities, and expanded stereo options.
- Safety. Connected cars improve safety of a vehicle by alerting drivers to potential dangers such as cars in lanes next to them, reminding drivers of the speed limit, and weather warnings or other potential safety hazards.
- Navigation. Today, connected cars not only tell a driver where to go, but suggest the fastest way, alert drivers to construction and traffic conditions and reroute when necessary.
- Convenience. The driving experience is easier and more convenient with a connected car. Drivers can start their cars with the touch of a button on their phone, be alerted that their cars are unlocked or that it’s time for a maintenance service.

This is just a partial list of what has been accomplished over the past decade. And much more is on the horizon for connected cars. Use cases such as telematics analytics, automated ride sharing and car to car collaborative cruise control are at our doorstep. In the not-too-distant-future, driverless cars will likely hit the roads as car manufacturers race to be the first to market.

> “
>
> **39% of new car buyers** in Germany, Brazil, China and the U.S. were **reluctant to use connected services in a car** due to privacy concerns.
>
> ”

CONNECTED CARS POSE RISKS IF THEIR INTERNAL ECOSYSTEM AND USER INTERACTION ARE NOT PROTECTED

While connected cars have undoubtedly improved the driving experience, like all innovation, they come with risk. Automobiles contain highly complex computing systems that have had vulnerabilities that we have seen in “everyday technology” such as our mobile devices, web browsers and desktop operating systems. And when different applications and devices are added to a car’s ecosystem, they open up doors that could be potentially vulnerable to an attack.

Safety risks are a major concern when it comes to connected cars. Security researchers have demonstrated that they can remotely take over a connected car’s ecosystem and take control of the accelerator, brakes, steering wheel, transmission and any number of other components that can threaten the safety of people in and around the car. Car-buying consumers are aware of this risk. In fact, 40 percent of new car buyers in Germany, Brazil, China and the U.S. were afraid that people can hack into cars if they are connected to the Internet, according to a 2014 McKinsey Connected Car Consumer Survey.

Protecting privacy is another challenge of the connected vehicle. Connected cars collect huge amounts of data, which can be accessed by a hacker if they gained access to the system. Someone hacking the automotive ecosystem of a car could potentially obtain navigation information and know when a person is out of their house, in order to plan a robbery. Or, can hack into a phone that is connected to the system and steal important information like contacts or payment information. In the same survey mentioned above, nearly 39 percent of new car buyers in Germany, Brazil, China and the U.S. were reluctant to use connected services in a car due to privacy concerns.

ATTACK ON THE MODEL S

During the August 2017 Black Hat conference in Las Vegas, a leading information security event, representatives from Keen Security Lab presented the details for how they successfully performed a remote attack against the Tesla Model S, one of the world’s most advanced connected cars.

This was only the second remote attack demonstrated against an automobile and exploited a different chain of vulnerabilities than the previous remote attack, which was demonstrated by security researchers Charlie Miller and Chris Valasek on a Chrysler vehicle in 2014 and resulted in the recall of 1.4 million automobiles.

> In **2014,**
> Chrysler recalled
> **1.4 million automobiles**
> due to
> **remote attack vulnerabilities.**

The Tesla attack involved a complex chain of vulnerabilities and worked in both parking and driving mode, which is significant because the attacker does not need to have firsthand physical access to the vehicle, and remote commands while moving maximizes the potential physical risk to the driver.

Tesla responded to Keen Security Lab within 10 days with an update that fixed all of the listed vulnerabilities. This is an excellent response from an automotive manufacturer. However, the exercise brought to light the challenges when it comes to security within automotive systems.

HOW DID THE ATTACK HAPPEN?

Keen identified vulnerabilities in the Tesla Model S to gain access to the system and exploited them to put the attack into motion. Here's how:

MALICIOUS STEP ONE – DELIVERING THE EXPLOIT REMOTELY

We know that browsers have vulnerabilities, and browsers used in cars are no exception. There has been a history of vulnerabilities with WebKit based browsers, including the browser used by the Tesla Model S at the time of the Keen Labs research. If web browser technology in an automobile is vulnerable, a malicious actor could cause a vulnerable browser to address an infected website, effectively delivering the payload remotely.

Keen used the Tesla's WiFi mode that automatically scanned and connected to known SSIDs (WiFi access point names). The internal browser also automatically reloaded its current webpage, which is where the initial malicious payload was placed. Keen specified that the automobile's cellular connectivity mode could potentially be used by an attacker that is able to socially engineer the user. Imaging phishing, except this time it would be for automotive attacks.

“If an attacker can **alter ECU firmware,** they can effectively **change** the operation of the **car.**”

Keen took advantage of vulnerabilities that were first publicly published in 2011 and 2012 in order to accomplish their attack. The fact that vulnerabilities that were publicly known years before the attack occurred, demonstrates how the complexity of automotive systems can result in increased attack surface and opportunities for attackers.

MALICIOUS STEP TWO – GAINING CONTROL OVER THE IN-VEHICLE SYSTEMS

The browser exploit resulted in a low-level privilege for the attacker. In order for the attacker to proceed further, they would need a way to escalate their capability. To do this, Keen took advantage of an ‘old’ kernel exploit against Linux, first published in 2013, which resulted in the ability to disable ‘AppArmor’ – a Linux kernel security module – and then achieve uninhibited root level access. At this point, the attacker has what they need to accomplish the rest of the steps necessary to perform a malicious attack within the internal automotive ecosystem and ultimately affect how the automobile operates.

MALICIOUS STEP THREE – GETTING PREPARED TO AFFECT THE REAL WORLD

Automobiles operate with their own digital network and computing systems. Automotive components known as “Electronic Control Units” (ECUs) are responsible for many aspects of how a car operates, by receiving sensor data and sending commands to other components connected to mechanical parts. To alter the safe operation of an automobile, an attacker’s goal in this digital/physical system will almost always be to alter the control of one or more ECUs. Like many electric components, these ECUs have firmware that ultimately defines how they work. If an attacker can alter ECU firmware, they can effectively change the operation of the car.

Firmware integrity checking was present in the Tesla, but Keen was able to produce a customized firmware update package and also modify the functionality that resulted in the ability to update the firmware on a ‘gateway’ ECU. This updated firmware enabled the researchers to further send automotive network commands (CAN Bus) to other ECUs. ECU firmware code signing protection was not present in the Tesla Model S at the time of the 2016 research. Charlie Miller and Chris Valasek also noted that ECU firmware code signing protection was not present in the Chrysler automobile that they successfully remotely attacked.

MALICIOUS STEP FOUR – PERFORM DANGEROUS ACTIONS

Keen researchers were now able to send commands over the automotive CAN Bus network, but ran into limitations. For safety reasons, some ECUs did not respond to commands if the car was in driving mode. The researchers found a way to block speed messages at the point of the gateway ECU, enabling dangerous commands to be sent to controller devices while the automobile was in operation.

> “**Code signing firmware,** and the authentication and authorization of **unique identities** for vehicle components can **mitigate an automotive attack.**”

LESSONS LEARNED

As previously stated, Tesla has already responded by fixing the listed vulnerabilities. Keen has also suggested that Tesla update the version of Linux used by their devices. What else can be done to mitigate an automotive attack?

CODE SIGNING

Keen suggested that code signing be used as a protection mechanism for ECU firmware. This cryptographic method of verifying the integrity of ECU firmware makes a lot of sense, but it needs to be completely thought out. Automobiles will need to receive over-the-air (OTA) updates to many onboard ECUs, from verified sources. Software over-the-air (SOTA) updates can help provide upgradability and bridge the gap between the differences in software and hardware lifecycle. Thus, software management throughout the vehicle lifecycle becomes paramount for automakers. The ability to verify the integrity of the update package may need to take into account a complex firmware package with multiple parts. Properly implemented, code signing and secure over-the-air updates will be important tools in securing automotive ecosystems at scale and will be a competitive advantage for OEMs.

UNIQUE IDENTITIES FOR ELECTRONIC COMPONENTS – AUTHENTICATION

From a purely logical standpoint, why should a command originating from an automotive infotainment system be able to control a critical function such as braking or steering? Implementing unique identities for all critical electronic components makes it possible for devices to cryptographically authenticate to other devices. This means that automotive components will securely know the source and destination of the commands they are responding to.

> “**Embedding trusted identity** early in the automotive supply chain… **ensures** that only **authorized users, devices** and **applications** are able to **interact** or consume data.”

The Keen Security Lab research has underscored the need to take hard won security lessons about digital identities and authentication and apply them to automobiles. Thankfully, ECUs are increasingly being built with cryptographic capabilities and also hardware-based secure elements to safely contain these identities. Additionally, lessons learned from the mobile device world about secure bootstrapping can be employed in order to create trustworthy automotive devices, capable of strong authentication.

UNIQUE IDENTITIES FOR ELECTRONIC COMPONENTS – AUTHORIZATION

Not all components should be authorized to send or respond to commands, depending on their operating context. For example, why should an ADAS (Advanced Driver-Assistance Systems) technology such as parallel park assist be enabled while a car is driving at a speed that is unsafe? While it is prudent to enable mechanical safety functions, those functions should depend on data inputs coming from trusted sources. Knowing that source, and knowing the authorization level of that source is part and parcel of sound device centric security.

IOT SECURITY IS INTEGRAL TO THE SUCCESS OF AUTOMOTIVE INNOVATION

As automotive innovation continues to accelerate, it’s important that auto manufacturers ensure the security of their connected vehicles to protect drivers and passengers, and to ensure the viability of their products. Securing a car’s digital components requires manufacturers to establish a connected ecosystem and managed identities at the ECU and head unit level to allow for secure IoT strategies from supply chain through manufacturing, to initial ownership and the entire life cycle of the vehicle.

Embedding trusted identity early in the automotive supply chain provides a solid foundation for secure communication, command and control of vehicles and mitigated risk of attacks against the increasing complexity of innovative connectivity. It ensures that only authorized users, devices and applications are able to interact or consume data.

ABOUT IOTRUST™ SECURITY SOLUTIONS – ENSURING A TRUSTED INTERNET OF THINGS

Entrust Datacard has a long history of strong security for complex systems. Entrust Datacard™ ioTrust™ Security Solutions ensure a trusted Internet of Things by securing devices and data flows – from sensor to cloud – that drive transformational digital business outcomes. Our offerings, which are based on enterprise-grade encryption technologies, establish trusted identities for devices across IoT infrastructures. So you can create secure ecosystems and transmit data from devices in the field to value engines efficiently and securely.

ABOUT ENTRUST DATACARD CORPORATION

Consumers, citizens and employees increasingly expect anywhere-anytime experiences — whether they are making purchases, crossing borders, accessing e-gov services or logging onto corporate networks. Entrust Datacard offers the trusted identity and secure transaction technologies that make those experiences reliable and secure. Solutions range from the physical world of financial cards, passports and ID cards to the digital realm of authentication, certificates and secure communications. With more than 2,000 Entrust Datacard colleagues around the world, and a network of strong global partners, the company serves customers in 150 countries worldwide.

For more information about Entrust Datacard products and services:

Call
888-690-2424
Email
sales@entrustdatacard.com
Visit
www.entrustdatacard.com

IT17-4100-001

Entrust Datacard™