Automotive Cybersecurity Threat Report

2022

CALLISTO

Index

1 Foreword

2 Global Automotive Cyber Security Research Institutions and Organizations

4 The Threats to Critical Components

5 Case Study – T-Box Threats

6 The Growing Threats of Intelligent Services

8 Case Study – Digital Key Threats

9 Summary

10 Trends and Challenges

11 About Us

12 References

Foreword

1200+

Security incidents

49%

Security incident increase

280+

Connected car related CVEs

8 times

Connected car vulnerability increase

With the development of "electrification, intelligence, and networking" in automobiles, automobiles have become "networked computers on wheels." Networking and intelligence provide automobiles with unprecedented capabilities, but in the meantime, they also bring more security threats. Since 2010, more than 1,200 security incidents related to smart cars that have been publicly reported, of which 207 occurred in 2020 [1]. In 2022, there were nearly 300 incidents, a 49% increase. In 2020, there were 30 CVEs (Common vulnerabilities & Exposures) directly related to automobiles announced, and by December 2022, the number of automobile related CVEs had soared to 284, an increase of 8 times in 2 years.

Since the beginning of 2022, the Callisto Automotive Threat Intelligence Center has analyzed automotive related cybersecurity information from media, academic research institutions, offensive and defensive competitions, social networking and deep, dark web. We also studied more than 300 automotive cybersecurity incidents and related 284 CVEs. The results show that smart cars are currently facing three major risks:

- The digital key has become a new "entry point" for hackers to "unlock" the vehicle. Relay attack, replay attack and impersonation attack are the main techniques;
- Intelligent services have become a new "control point" for hackers to "manipulate" vehicles, mainly in the form of leakage of identity credentials, abuse of service API, and illegal vehicle upgrades;
- ECUs have become the "key" attack surface for hackers to explore firmware vulnerabilities, system vulnerabilities and third-party components.

Global Automotive Cyber Security Research Institutions and Organizations

50+

Tracked by Callisto

40%

White hat

30%

Academics research institution

30%

Security company

In 2022, there were many smart car hacking incidents and serious vulnerabilities. The Callisto Automotive Threat Intelligence Center has tracked and studied these hacking incidents and vulnerabilities. The study shows that with the continuous enrichment of automobile intelligent functions, more and more hackers, security teams, academics research institutions and security enthusiasts, etc. have turned to security research and vulnerability mining in the automotive field.

David Colombo, a 19-year-old security researcher from Germany, discovered an API call privilege escalation vulnerability (CVE-2022-23126) in Tesla's third-party application, TeslaMate. It is used by some Tesla owners to analyze vehicle data. Through this vulnerability, more than a dozen of Tesla spread out the world can be remotely controlled.

Ayyappan Rajesh and Blake Berry, two students of Dartmouth College, disclosed in March that there is a "replay attack" vulnerability (CVE-2022-27254) in the remote keys of Honda and Acura cars, which can be exploited in the short-range access to lock, unlock, control windows, open the trunk, and start the engine of the target vehicle [3].

The NCC disclosed a vulnerability in Tesla's Model 3 and Model Y keyless entry systems. It takes less than 10 seconds to unlock and start a car by relaying Bluetooth link-layer data for attacking keyless entry [4].

Software engineer Daniel Feldman successfully cracked the software upgrade function of Hyundai/Kia's infotainment system, which requires the use of keys used by Hyundai Motor Company to manage software. Daniel Feldman searched Google and found that the AES key of the public example on the Internet is the key used by Hyundai automobile software. With this key, any user can tamper with the upgrade package, repackage it, and successfully write it into the infotainment system [5].

Bimmer Tech is a professional car modification company and a hacker team specializing in cracking car programs. BMW launched a subscription service for vehicle performance ($18/month for seat heating) in South Korea and the UK in August. By writing code, Bimmer Tech can add some new functions to the car, such as automatic headlights, mobile phone mirroring, adaptive cruise control, etc., and even help car owners delete some unwanted applications [6].

The Ransom EXX extortion organization posted on the dark web, claiming to have successfully hacked into Ferrari, a well-known Italian car manufacturer, and stole 6.99GB of internal files, including internal documents, data sheets, maintenance manuals, etc. [7].

Automotive cybersecurity research has been conducted for many years. New attack methods are announced every year. New vulnerabilities are being discovered constantly. Driven by organizations and individuals focusing on automotive cybersecurity, automotive cybersecurity issues are getting increasing attention. But in the meantime, continuous attacks remind us that automobiles are facing increasing threats.

Institution Type	Institution Name
Security company	Baidu X-Team
Car modification company	Bimmer Tech
White hat	Charlie Miller
White hat	David Colombo
Security company	GoGoByte
Security company	IOActive
Security company	KeenLab
White hat	Martin Herbert
Academics research institution	MIT CSAIL
Security company	NCC Group
White hat	Sam Curry
Security company	Sky-Go Team
Security company	Starvlab

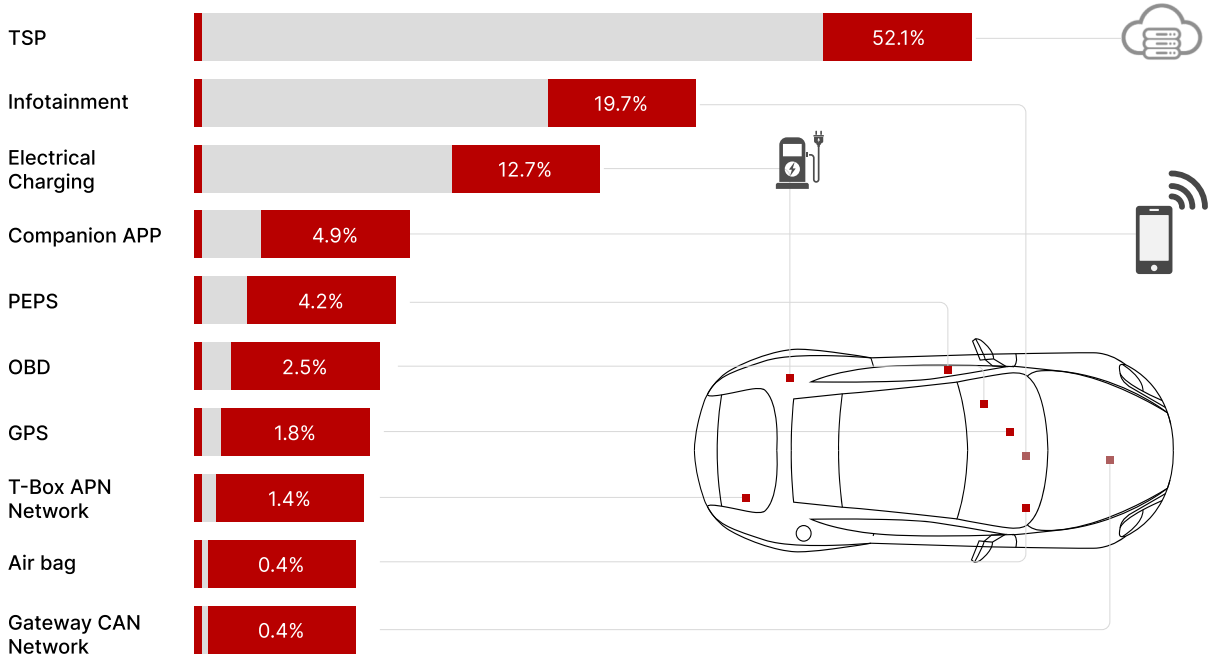
Note: Institution names are arranged in alphabetical order.

The Threats to Critical Components

With complex supply chains, ever-changing electronic and electrical architectures, and the increasing cyber threat, risk management in the automotive industry is facing unprecedented difficulties. Component manufacturers often provide critical components to multiple OEMs, so a component vulnerability may exist on multiple models of different car brands. In the past few decades, component manufacturers have often lacked cybersecurity measures for their products.

The Callisto Automotive Threat Intelligence Center conducted research on more than 700,000 vulnerabilities from the CVE, NVD, CNVD, CNNVD and other vulnerability databases. 284 vulnerabilities related to automobiles are studied in depth. The studies show that these vulnerabilities are mainly related to critical components of connected vehicles, cloud services, and electrical charging facilities. The critical components include T-Box, IVI, CGW, ADAS, GPS, airbags, and OBD. Among these vulnerabilities, there are 148 related to cloud services. These vulnerabilities mainly involve the leakage of authentication credentials, the bypassing of authentication mechanisms, and the lack of API security. Hackers can use these vulnerabilities to remotely control a large number of cars, and sometimes they even gain control of cars from different car makers. There are 136 vulnerabilities related to vehicle ECUs. These vulnerabilities allow attackers to use replay attacks, relay attacks, etc. to gain control of car doors, engines, and other components remotely.

In the GeekPwn 2022 competition in October, multiple car remote attack vulnerabilities were disclosed. Recently, the authorization vulnerabilities of Sirius XM were also exposed. These vulnerabilities all involve the safety of parts and components from suppliers. Suppliers provide key components for smart car manufacturers. However, when a component or service provided by them has a vulnerability, it may involve hundreds of thousands of vehicles from multiple OEMs. The impact often exceeds the estimates of the parties involved.

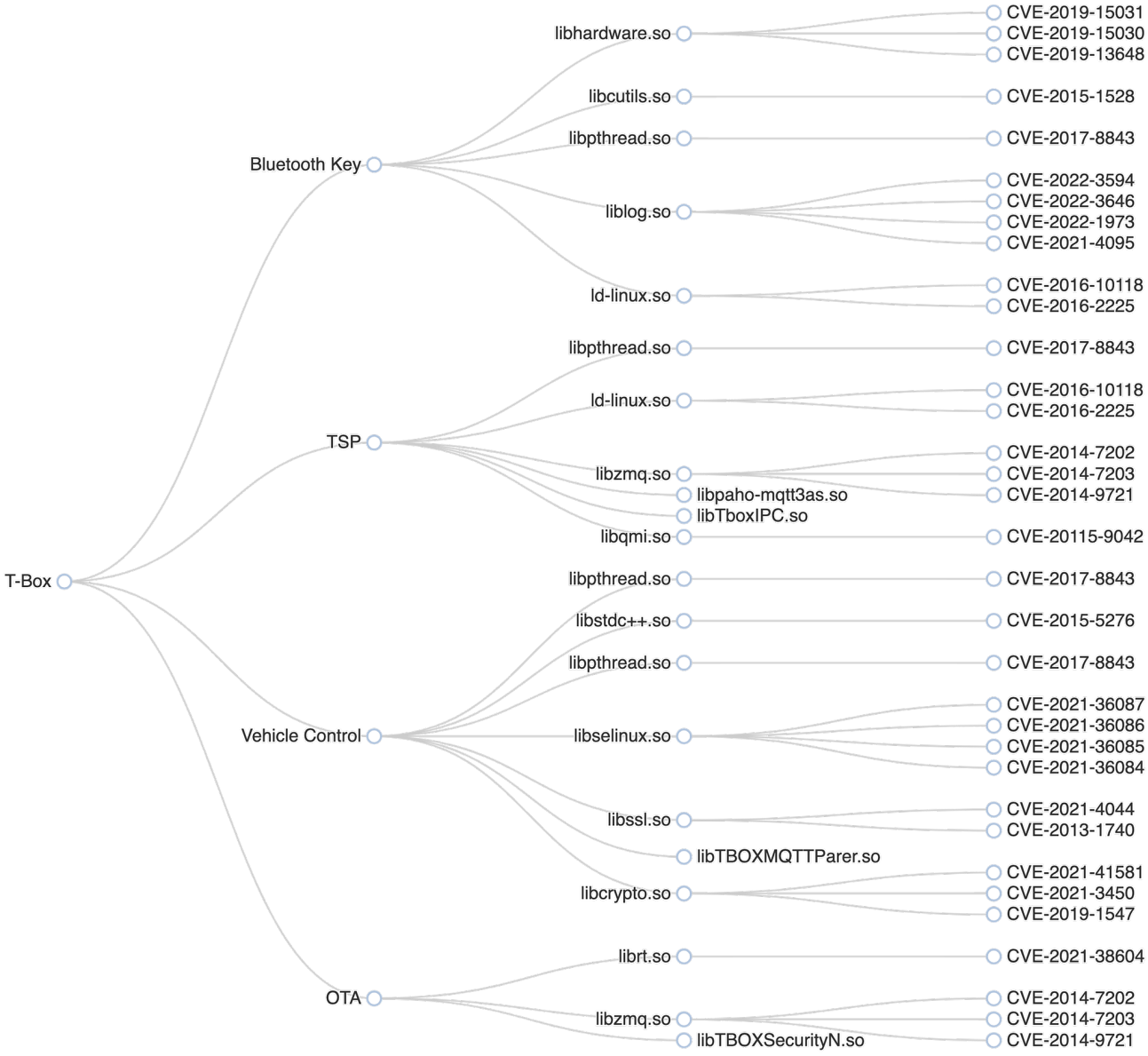


Case Study – T-Box Threats

The number of smart car ECUs continues to increase, and some vulnerabilities may be exploited by hackers to invade vehicles, illegally access TSP servers, steal other vehicle information, and even injure drivers and passengers.

The Callisto Automotive Threat Intelligence Center continues to analyze critical components, such as T-Box, IVI, CGW and ADAS from major smart car manufactures, and has discovered a large number of hidden risks. Taking T-Box, a key communication component connected to the outside of the car, as an example, through in-depth analysis of its applications, components and software libraries. 1326 applications and 14,000 libraries in 11 representative firmware were extracted. There are 1401 CVE vulnerabilities found. The firmware uses a total of 420 components, 12,000 libraries, and a total of 1752 CVE vulnerabilities found.

The Callisto threat intelligence platform maps applications, components, libraries, and CVE information with vehicle brands, models, and years one by one. When a component has a vulnerability, it can quickly locate other models, helping OEMs, Tire1, and Tire2 to identify complex critical component risks and threats and respond accordingly.



The Growing Threats of Intelligent Services

Under the new design methods such as "service-oriented architecture" and "software-defined automobile", the intelligent functions of automobiles are constantly being enriched. These design methods make the functional modules of automobiles more flexible and convenient. At the same time, it also facilitates the upgrade and update of vehicle functions, such as digital key, remote car control, advanced assisted driving, adaptive cruise, remote diagnosis and OTA upgrade, etc. These intelligent functions and services have been flexibly installed and configured on many brand models. However, this new design method also brings some security threats. Since the various components of the vehicle depend on each other, once a certain component fails, it may paralyze the entire vehicle and even endanger the personal safety of the drivers and passengers.

Threats to Digital Key Functions

The vehicle digital key uses wireless communication technology to realize the function of unlocking and starting the vehicle. Although the new function is convenient for users, but it also brings new cybersecurity risks and exposes some new attack surfaces. The Callisto Automotive Threat Intelligence Center has analyzed vehicle cybersecurity incidents since 2022, and found that 30% of cybersecurity incidents are related to vehicle digital keys. In the known attack incidents, there are two typical attack methods. The first is a relay/replay attack, in which the attacker intercepts a digital key signal to unlock the vehicle. Another attack method is to exploit the vulnerability of the digital key program. There are three main processes in digital key use. First, the user terminal initiates the request. Second, the cloud service checks the command. Third, the vehicle responds to the request. The program may have vulnerabilities or logic flaws in these processes, which can be used by attackers to implement unauthorized access.

Threats to Remote Control Functions

The remote control service for connected vehicles provides a convenient way to control vehicles, enabling remote vehicle start, remote locking/unlocking, remote air conditioning control, vehicle status monitoring, remote charging management, roadside assistance and etc. Vehicle owners use mobile devices to send remote control commands through a series of processes. There are two types of threats in the execution process, one type of threat is remote attacks, that is, hackers attack the vehicles through various networks, this kind of attack may lead to the damage of vehicle functions of operation, and may even endanger the safety of the driver and passengers. Another threat is the leakage of user information, such as information about a vehicle itself, vehicle location, speed, etc. Hackers can use information to commit criminal activities

Threats to OTA Service

Automotive OTA (Over-The-Air) updates are services for updating vehicle software remotely over a wireless network. OTA updates allow OEMs and dealers to send software to the vehicle's on-board terminal (T-Box) for installation. There are three types of threats to automotive OTA services. First, software update leakage occurs when the on-board terminal (T-Box) communicates with the cloud server during a vehicle software upgrade, and if encryption measures are weak, hackers may intercept the software. Second, with illegal software, hackers will monitor and even remotely control the target software by implanting a backdoor if the upgraded software is intercepted and tampered with. Third, loss of access, where hackers can tamper with the upgrade software and gain key permissions during the OTA upgrade process if it lacks security checks. Large-scale modifications to vehicle functions and controls can be made at this point, thereby endangering the safety of the driver and passengers.

Case Study – Digital Key Threats

How to securely share a digital key with target users? How to identify and authorize the digital key user?

The digital key replaces the traditional keyless system (PEPS). It only enables functions such as, unlocking doors and starting vehicle, but also allows for personalized settings and management of the key, which is not possible with traditional keys.

The Callisto Automotive Threat Intelligence Center recently conducted a Threat Analysis and Risk Assessment (TARA) on the new digital key and studied the digital key management functions and protocols. The main features include key registration, vehicle binding, key sharing, key revocation, and key cancellation, all of which are vulnerable to hacking. Taking the digital key sharing function as an example, a hacker can break the authentication protocol of the sharing process and abuse the binding relationship between the digital key, the vehicle, and the user. This allows an attacker to have the digital keys to multiple vehicles at the same time, enabling remote unlocking and starting of the fleet.

Data Sniffing

Sniffing the owner's application key-sharing command packets through Burpsuite, replaying, tampering, and forging the packets, as well as tampering and traversing the parameters of the service API to find vulnerabilities.

Reverse Engineering and Analysis

Reverse the signature authentication program, analyze the logic of signature authentication, reverse the message queue of the vehicle owner's application interacting with the cloud, and obtain the operation instructions and signature algorithm.

Vulnerability Exploitation

Tampering with the vehicle VIN information, user information and signature in the cracked signature program, bypassing the owner's authentication and enabling the authorization of any vehicle key to open the door remotely.

Fleet Hacking

Stealing the fleet's vehicle VINs and using the cracked signature program to enable batch authorization of keys and remote control of the fleet.

Summary

Cybersecurity Incidents ↑

Among the attacks in 2022, digital key attacks are the most widespread and have a high probability of occurring. This trend is expected to continue in 2023. The analysis shows that some of the attacks were carried out by the discovery and exploitation of vulnerabilities that had existed for years, and some were caused by the addition of a new attack surface to the digital key service. For these reasons, OEMs should strengthen their investment in securing development process management and security operations, rather than relying solely on penetration tests.

Attack Difficulty ↓

Judging from the team attack activity indicators in the case analysis of automotive cybersecurity incidents, the attack threshold of automotive cybersecurity is lowering, and the professional knowledge required to attack vehicles is also shifting from multi-field experts to skilled technicians. This situation has been increasing in recent years. It can be seen in a large number of attack cases, such as the theft of car owner information, the takeover of the OTA service platform, the theft of TSP data, and other attacks against the cloud. In order to prevent a large number of potential threats from the cloud in advance, car companies should increase the security defense of the TSP platform, isolate the service network, and strengthen cybersecurity and data security compliance management.

New Attack ↑

With the intensification of competition and technological advancement, the intelligent services and complexity of automobiles continue to increase. These situations will expose more attack surfaces and increase the attack value of vehicles. For example, "service-oriented architecture" shows the development direction of the car, and we also see more vulnerabilities and threats in the cybersecurity of the vehicle. In the face of new types of attacks, OEMs and suppliers should deploy cybersecurity measures as much as possible to reduce risks and meet compliance requirements and user expectations while developing new functions.

In order to cope with the risks brought about by the great changes in the industry, we will continue to conduct in-depth research on automotive cybersecurity capabilities, continue to exchange cybersecurity event analysis results and technical insights, strengthen close cooperation with the automotive cybersecurity community, and provide OEMs and suppliers with professional products and services.

Trends and Challenges

Risks often come with the exposure of the attack surface and the drive of interests. In the foreseeable future, unclear security threats will gradually surface.

Fleets begin to face unprecedented cybersecurity challenges

Except for sci-fi movies, attacks on convoys are rarely seen in reality. However, because of the huge benefits of attacks, it will become obvious and targeted in the future. Especially large convoys are already using "digital fleet" technology to increase business revenue and reduce costs. Hackers may launch attacks and extortion against multiple vehicles by attacking OEMs production lines, fleet platforms, or certain vehicle.

Vendors need to take on an increasingly important security role

Suppliers are using proprietary and open-source technologies to jointly provide services for car manufactures. The richer the functions, the more code, and the more risks that come with it. There is no general method to protect car manufactures from supply chain threats. However the cybersecurity measures of supply chain will greatly reduce the cybersecurity pressure of OEMs. Suppliers need to assume an increasingly important role in security.

Widespread use of intelligent driving poses new threats

Although there is still no clear time information for the commercialization of intelligent driving that covers L4, L2 has been accepted and popularized by drivers. Attacks against the intelligent driving domain will become a new research hotspot. The in-vehicle computing platform with strong computing power, remote OTA, and close integration with the vehicle control domain is bound to attract a large number of network security researchers to join in the security research on intelligent driving. Vehicle-road collaboration has introduced a new vehicle-cloud communication method, which brings new security risks. Callisto Technology has a solution for this, and if necessary, please contact our technical consultant.

About Us

Callisto was founded by the world's first group of technical experts focusing on automotive cybersecurity. With years of experience in the field of automotive cybersecurity, we start from the perspective of attack and defense, and integrate advanced artificial intelligence and Knowledge Graph engine. Through the algorithm analysis of the massive multi-source heterogeneous messages, instructions and API services of the intelligent connected vehicles, so as to resist the new attacks against automotive manufactures and supply chains. We provide threat intelligence and defense capabilities for connected vehicles, and protect the security of core automotive assets and intelligent services.

We maintain a great passion and interest in the automotive and cybersecurity industries, while we respect and learn from the engineering experience from the automotive industry over the years. We are committed to providing more professional and leading-edge security products and services to automotive companies. We emphasize fully unlocking the value of data, while using scientific analysis methods combined with practical application services to portray vehicle security status in multiple ways, automatically analyzing anomalies and disposing of risks, enriching the analysis dimension, and reducing the operational pressure on security personnel.

• Callisto Technology
Blog : https://www.callisto-auto.com
Email : contact@callisto-auto.com

References

1. Upstream 2022 Global Automotive Cybersecurity Report

https://upstream.auto/2022report/

2. How I got access to 25+ Tesla’ s around the world. By accident. And curiosity.

https://medium.com/@david_colombo/how-i-got-access-to-25-teslas-around-the-world-by- accident-and-curiosity-8b9ef040a028

3. Some Honda models have vulnerabilities that allow hackers to remotely control vehicles

https://m.freebuf.com/news/326833.html

4. Tesla BLE Phone-as-a-Key Passive Entry Vulnerable to Relay Attacks

https://research.nccgroup.com/2022/05/15/technical-advisory-tesla-ble-phone-as-a-key-passive-entry-vulnerable-to-relay-attacks/

5. How I Hacked my Vehicle

https://programmingwithstyle.com/posts/howihackedmyvehicle/

6. Hackers crack BMW premium features

https://zhuanlan.zhihu.com/p/555457027

7. Ferrari hit by RansomEXX ransomware, 7GB of downloadable data online

https://www.redhotcyber.com/post/la-ferrari-e-stata-colpita-dal-ransomware-ransomexx-7gb-di