Study of security risks in modern vehicles and their solutions

by M. Kagalkar and S. Panda
17 December, 2023

Abstract

Modern vehicles heavily rely on wireless communication technologies like Bluetooth, WiFi and NFC to provide music, calling and navigation services. These wireless technologies introduce vulnerabilities that can be exploited by malicious actors. Despite the risk to user data and personal safety, this area has not seen improvements in some time. We aim to address these issues by implementing security concepts like authentication, encryption and privilege management to show how these systems can be protected adequately.

Keywords

Cyber Security, Cyber Physical System, Automotive Security, Infotainment System, Cars, Scooters

Introduction

The predecessor of the modern day car was a purely mechanical contraption. It gave users no interface other than a stick and pedals. Over the years, cars evolved physically [2] offering improvements like better engines, stronger build and comfortable seating. At one point in the past decade, they peaked in this area and most cars had nothing new to offer other than small changes to existing designs. This is when they decided to integrate electronic systems like display panels and software controlled braking, steering and acceleration [2].

Even with these changes, cars were still safe as the electronic components were isolated, and had mechanical fail-safes. Today's cars have started providing digital services like internet access, vehicle control and infotainment systems, allowing all passengers to connect to the car and use them. The risk here is that it is not always the passengers that connect to the car. The improved range of WiFi and Bluetooth technologies allows passengers in nearby vehicles and pedestrians to exploit weak connections and gain control of these services in the car. Many manufacturers who had completely overlooked such possibilities, are recalling some models or patching them remotely. Some famous cases are that of Honda and Tesla. The most exploited feature is the ability to unlock doors with a 'smart key', which is usually just a simple RFID tag without any additional security.

Attack Surfaces

[1, 3]

Direct Physical Attacks are possible through something known as the **On Board Diagnostics (OBD) port**. This is a port used for diagnostics of the vehicle. Since most manufacturers assume that someone who is accessing the ODB port is either a service technician or the owner there are no security controls on this port. As a result attackers who manage to unlock a parked car can plug hardware directly into the OBD port and carry out an attack.

Such an attack can also be carried out using the **USB port or CD reader** in older models.

Indirect Physical Attacks involve the car as a medium. The car network can used to perform **shell injection** on other connected devices. This exploits the trust that other devices on the car network are trusted devices belonging to people you know.

Bluetooth Network Attacks include buffer overflow, using a paired phone with a trojan, sniffing the MAC address and brute forcing the PIN of other devices. The attackers might be around the car as pedestrians or following in another car, and they would still remain in range. These types of attacks are more common than physical attacks and are not visible to the vehicle owner.

WiFi/Cellular Attacks
These attacks can be long range, and in some cases, internet based. With an increasing number of cars providing 'internet access inside', all the attacks possible over public WiFi are now applicable to cars too. Packet sniffing, phishing, MITM, denial of service and malware injection are possible, with an even longer range than bluetooth. Seeing the severity of this, manufacturers have tried to implement some security features like encryption protocols and the ability to remotely patch the software.

NFC and RFID Attacks
The most common type of attack in this category is the cloning and relay attack. Attackers use a signal capturing tool to read and copy the signals emitted by the key fob and other accessories. They then relay the copied signals to unlock the car, start the engine or control other vehicle parameters.

Solutions

The solution that must be applied immediately is following the policy of '**zero trust**'. All connections must use encrypted protocols like WPA for WiFi and HTTPS for internet traffic. This will act as a barrier to discourage attacks.

Another suggestion is to prevent any device from accessing the network unless it is explicitly approved by the owner. Shared music and video must be controlled in the application layer, using apps like Spotify or SharePlay. Users should not be connecting to the car network for media controls.

Manufacturers must also shield the NFC or RFID tags in key fobs, to prevent passive cloning of their signals. This can be implemented by providing a case that blocks signals, as we have seen in wallets.

Our most important recommendation is that highly privileged and important functions like unlocking doors, starting the engine and driving controls should NEVER rely on a single weak factor. There must be a physical check like a key or biometrics to verify the user for these actions. They must also be controlled using physical mechanisms.

Examples

- The new Tesla Cyber Truck uses digital touchpad buttons in the display to change gears, suspension height and other critical parameters while driving.
- The Mahindra Thar has a digital display with a menu that includes changing from 4WD to 2WD.
- The top-end MG Hector has open WiFi by default with internet access.
- Following multiple incidents where passengers could not open their doors digitally after a crash, Teslas now ship with a physical latch for the door.
- Honda recently admitted that their key fob system had a vulnerability that allowed attackers to freely unlock the door, but not start the engine. This issue cannot be patched.

Conclusion

Many of these issues occurred because the on board systems in cars matured very fast and the security implementations in them did not. They were not given the same level of security as a laptop or home network would have.

We must now upgrade modern cars with the same security controls used for a web server or your home network. These include encryption, firewalls, two factor authentication and regular updates to the firmware. Users must also be aware that they cannot completely trust their car's network or the devices on it without implementing these controls.

References

J Halahan and W Chen. (2017). Wireless Security Within New Model Vehicles

Jaafarnia, Mohsen & Bass, Adele. (2011). Tracing the Evolution of Automobile design

C Watney and C Draffin. (2017). Addressing New Challenges in Automotive Security

Case Study of MG Hector by Shark CyberTech

Report on the Honda key fob vulnerability by Security Intelligence