Preventing Vehicle Hacking through Mobile Technology

Sayali Bapardekar
Department of Computer Engineering
ASM-Institute of Management and Computer Studies, Mumbai University India

Abstract— Technology has come a long way. Today modern technology has made our vehicles just another computer that is on wheels and works on electricity for a pollution free environment. But as every coin has two sides this technology also has some disadvantages. This smart vehicle that work on electricity and takes its instructions from a smartphone app, if given in wrong hands can cause destruction and even a terrorist attack. This paper gives a small idea on how security can be increased to avoid the misuse of the smart vehicles.

Key words: Smart Vehicles, IoT, Fingerprint Scanner, NFC, Security, Hacking

I. Introduction

IOT (Internet of Thing) is the inter-networking of physical devices, vehicles, buildings and other items embedded with software etc. which helps these devices to collect and exchange data. IOT is one of the many boons that modern technology has given as to make our life simpler.

Automakers connect vehicles in two ways:

- Embedded
- Tethered

Embedded cars use a built in antenna and chipset.

Tethered connections use hardware to allow drivers to connect their cars to their smartphones.

Mobile Phone Technology used in Vehicles are:

- Bluetooth Low Energy (BLE)
- Near-Field Communications (NFC)

With all the benefits comes risk, as the increase in connected devices gives hackers and cyber criminals more entry points.

The most common ways that vehicles are hacked are through the diagnostics board under the steering wheel. Every software that is installed in a vehicle can be analysed and controlled by this board.

Almost a year ago, Chrysler announced a recall of millions of vehicles after a pair of hackers remotely hijacked the Jeep's digital system over the internet.

With researchers recently researching on the automobile development it is very clear that auto manufacturers have not placed enough emphasis on security of vehicles.

The most important thing that an smart car owner should keep in mind is to keep his car software and app up-to-date.

II. Current Technologies

A. IOT

IOT will become increasingly important in transportation and logistics in the next several years, especially as self-driving cars hit the roads in increasing number.

B. Advance Back Cameras

Infiniti car's Around View Monitor also offered on some Nisan's models remains the best in offering 360o view of your surroundings. The new Toyota Prius has these features as well, but they managed in giving a more uniform look.

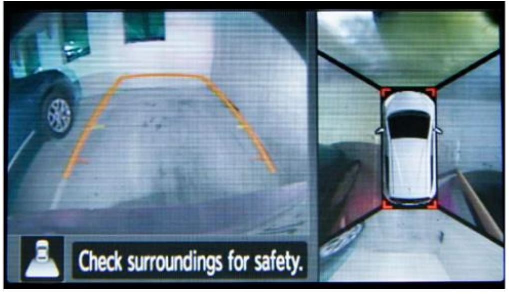


Fig. 1: Advance Back Cameras
Source: Autotrader

C. Improved smartphone Infotainment Integration

Just a few years ago we were happy that we were able to connect our Bluetooth devices to our cars and make calls and even play music from our phone to the car's audio system. Now, many cars allows a smartphone screen to be duplicated on a car's infotainment screen, from systems like Apple CarPlay and Android Auto

Fig. 2: Improved Smartphone Infotainment Integration
Source: autotrader

D. Smartphone Vehicle Management System

Vehicles equipped with vehicle management app OnStar provide features such as locate your car, call for roadside assistance, and even get health reports on your car's current status. Onstar is available on wide range of cars in a variety price category.

Some of the apps are My BMW Remote App- used to lock, unlock, horn and light flashing.

MyLincoln Mobile app- lets you start your car remotely and speak to support staff.

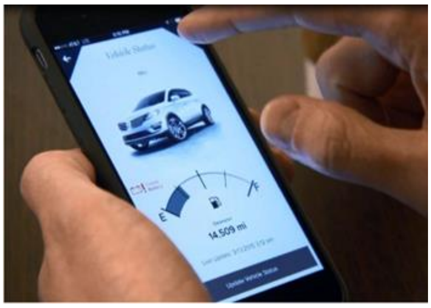


Fig. 3: Smartphone Vehicle Management System
Source: autotrader

III. ADVANTAGES

- Really time monitoring about the status of the vehicle
- Able to detect problems in the car early beforehand it turns out to be a major one
- Automatic emergency calls in an event of accident
- Medical assistance
- Maps, real time traffic updates through GPS
- Streaming radio and other music services

A. Disadvantages

- Requires strong internet connections without which some of the major features can go down
- In case of smart vehicles if cell phone gets stolen it creates a major chance that even car can get stolen.
- In developing countries, GPS system is not fully up-to-date which may sometimes cause the drives to lose his way.
- Lack of privacy as you are constantly been monitored and data about your where about is getting stored on the manufacturers system.
- If Cell phone is stolen you won’t be able to get access to your car immediately.

IV. NEW THEORY

As everything we do with the vehicles is getting automated security is the thing that comes in the mind first. This paper is just an research done by me to prevent the vehicle that is operated through an app from getting into wrong hands. This of course, has manly drawbacks and is not full flagged.

Providing security to the smartphone app as well as the car can be achieved in many ways. I have came across these two methods and think that these are the ways that are quick, not much time consuming and secured.

The Technologies we are going to use for these purpose are:

- NFC
- Finger-Print Scanner

A. Finger-Print Scanner

Finger-Print scanner are now a days available on every smartphone devices. Not very far we would be able to use these sensors to lock unlock our vehicles.

Finger Print Scanners are of three types

- Optical Scanners
- Capacitive Scanners
- Ultrasonic Scanners

1) Optical Scanners

Oldest method of capturing and comparing the fingerprints. This technique relies on capturing optical image, and using algorithms to detect unique patterns on the surface such as ridges or unique marks, by analysing the lightest and darkest areas of the image. Just like smartphones cameras, these sensors have finite resolution, and higher the resolution, finer the details the sensor can captured increasing the level of security. These scanners have typically a very high number of diodes per inch to capture these details up close.

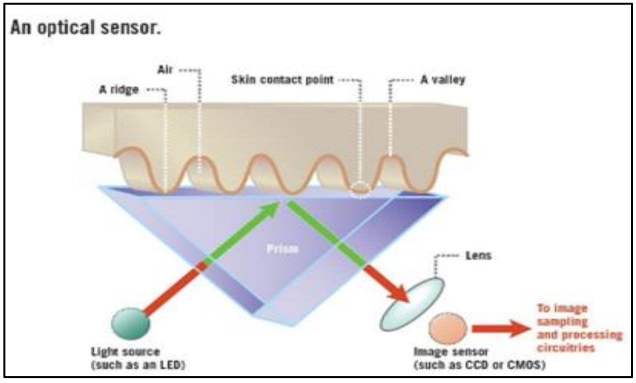
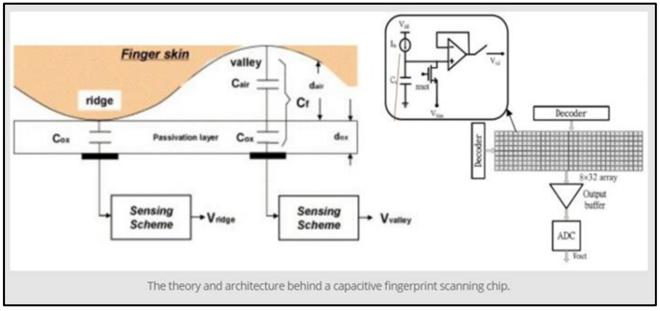

An optical sensor.
Air
A ridge
Skin contact point
A valley
Prism
Lens
To image sampling and processing circuitries
Light source (such as an LED)
Image sensor (such as CCD or CMOS)

Fig. 4: Optical Scanners
Source: android authority

2) Capacitive Scanners

One of the most commonly used fingerprint scanner. The core component used here is an capacitor. Instead of creating a traditional image of fingerprint, capacitive scanners use arrays tiny capacitor circuits to collect data about a fingerprint. As capacitors store electric charge have them placed on the surface of the scanner allows them to keep track of miute details of the fingerprint. The charge stored in the capacitor will be changed slightly when a finger’s ridge is placed over the conductive plates, while an air gap will leave the charge at the capacitor relatively unchanged. An op-amp integrator circuit is used to track these changes, which can then be recorded by an analogue-to-digital converter.

Once captured, this digital data can be used to compare distinct and unique finger attributes. The images cannot be replicated. The security comes from hardware or software hacking.



The theory and architecture behind a capacitive fingerprint scanning chip.

Fig. 5: Capacitive Scanners
Source: android authority

3) Ultrasonic Scanners

The latest fingerprint scanner to enter the market is the ultrasonic sensor, which was first announced in the Le Max Pro smartphone. To capture the details of the fingerprint, the hardware consists of ultrasonic transmitter and receiver. An ultrasonic pulse is transmitted against the finger placed over the sensor. Some of this pulse are absorbed and some of it bounces back, depending upon the ridges, pores and other details that are unique to each finger. Sensors detect mechanical stress used to calculate the intensity of returning ultrasonic pulse at different points on scanner.

4) Algorithm used in Fingerprint Scanning

Physical scanner is a dedicated IC that deals with interpreting scanned data and stores it in useful form in the smartphone's main processor.

Typically these algorithms look for ridges and line ends, together these are known as minutiae. If a scanned finger matches many of these minutiae it is considered as a match.

Rather than comparing whole fingerprint comparing only the minutiae reduces the processing time required to compare fingerprint, helps avoid errors, also allows finger to be placed anywhere.

This information has to be kept safe and away from any code which could corrupt it.

ARM processors keeps this information safe on a physical chip using its Trusted Execution Environment (TEE) based TrustZone Technology.

To prevent software snooping secure hardware platforms such as fingerprint scanner communicates directly.

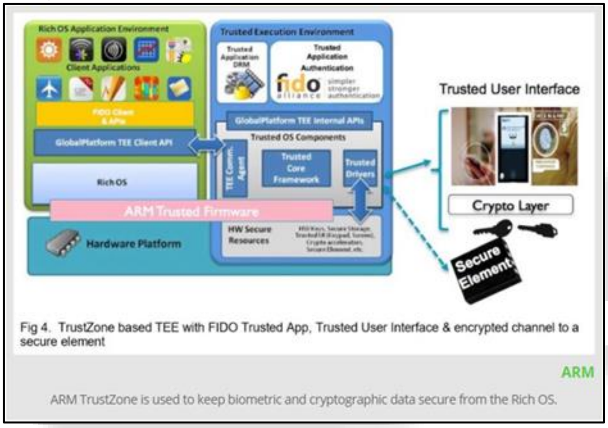


Fig 4. TrustZone based TEE with FIDO Trusted App, Trusted User Interface & encrypted channel to a secure element

ARM TrustZone is used to keep biometric and cryptographic data secure from the Rich OS.

Fig. 6: TrustZone Technology
Source: androidauthority

B. Near-Field Communications

Near-Field Communications is a communication protocol which enables two electronic devices, one of which is usually a smartphone, to establish communication within 4cm (1.6 in) of each other.

NFC devices are used in contactless payment systems, sharing photos, videos, contacts and files.

NFC devices acts like an electronic identity document and keycards.

Keycard locks are operated by keycards, a flat, rectangular plastic card with identical dimensions that of the credit cards. Several key cards are used, mechanical holecard, barcode, magnetic stripe, and smart card and RFID proximity cards.

1) Algorithm for the New Theory

- Step 1- Start.
- Step 2- User downloads an app that the car manufacturer has provided when he reserves an vehicle.
- Step 3- User secures this app with his finger print to avoid unauthorised access. The app would contain its own finger print scanner such as ultrasonic scanner.
- Step 4- User is given 5 chances the enter in correct finger print. Exceeding which the user won't be able to access the app for a particular period of time.
- Step 5 -To open car with the app. The car manufacture data system then sends an encrypted data record which is particularly an ID to the smartphone app that is communicated to the keycard present in particular vehicle via NFC present in the smartphone.
- Step 6- The ID is time limited so that the ID won't work after the driver is done with the car.
- Step 7- After the driver is done with the car the driver locks the car again with the app.
- Step 8- The App keeps on updating the user with the status of the vehicle, the repairing required, the servicing scheduled, Oil to be changed, Petrol levels etc.
- Step 9- User should keep the app updated.
- Step 10- Stop.

Hack to the Future
> HOW HACKERS AND CARMAKERS ARE BATTLING FOR CONTROL OF YOUR RIDE.

Fig. 7: Algorithm for the New Theory
Source: Google Images

V. Conclusion and Future Additions

This paper is just an idea about how security can be increased to avoid security issues by using biometric technology also we used the idea of NFC based keyless unlocking of car which is already been brought into use by OLA keys.

If ever the smartphone containing the app gets stolen the user can contact the car manufactures providing the ID to make note about the stolen phone and provide him with an alternative.

In Future more security and more ideas can be implemented to enhance security in this application.

References

[1] IOT- https://en.wikipedia.org/wiki/Internet_of_things

[2] Mobile in Automobile Industry- http://www.moweble.com/mobile-in-automobile-the-future-technology-in-cars.html

[3] KeyLess Unlocking of cars- http://www.adandp.media/articles/smartphone-vs-the-car-key

[4] FingerPrint Scanners- http://www.androidauthority.com/how-fingerprint-scanners-work-670934/

[5] Current Technology in Automobile Industries- https://www.autotrader.com/best-cars/must-have-automotive-technology-for-2016-247093

[6] Vehicle Hacking- https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/

[7] NFC- https://en.wikipedia.org/wiki/Near_field_communication

[8] KeyCard- https://en.wikipedia.org/wiki/Keycard_lock

[9] Smart Vehicles IOT Based- https://iot.telefonica.com/blog/the-many-faces-and-advantages-of-connected-cars