National College of Ireland

Securing WPA2 Communication Channel for Remote Controlling of Self Driving Vehicles

MSc Internship
Cyber Security

Ayush Jain
x17142741

School of Computing
National College of Ireland

Supervisor: Vikas Sahini
Industry Supervisor: Javier Olaretta

National College of Ireland
Project Submission Sheet – 2017/2018
School of Computing

Student Name:	Ayush Jain
Student ID:	x17142741
Programme:	Cyber Security
Year:	2018
Module:	MSc Internship
Lecturer:	Vikas Sahini
Submission Due Date:	04/08/2018
Project Title:	Securing WPA2 Communication Channel for Remote Controlling of Self Driving Vehicles
Word Count:	XXX

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are encouraged to use the Harvard Referencing Standard supplied by the Library. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action. Students may be required to undergo a viva (oral examination) if there is suspicion about the validity of their submitted work.

Signature:	
Date:	8th September 2018

PLEASE READ THE FOLLOWING INSTRUCTIONS:

1. Please attach a completed copy of this sheet to each project (including multiple copies).
2. **You must ensure that you retain a HARD COPY of ALL projects**, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer. Please do not bind projects or place in covers unless specifically requested.
3. Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing WPA2 Communication Channel for Remote Controlling of Self Driving Vehicles

Ayush Jain
x17142741
MSc Internship in Cyber Security

8th September 2018

Abstract

Jaguar Land Rover is entering the market of autonomous vehicles a little late with an upcoming product which lets the driver remotely control the vehicle. But with development of this product, the risk of the vehicle being compromised is alarming. Since the product makes uses of Wi-Fi and as known, WPA2 has a few vulnerabilities, it is very necessary to secure the communication channel. It is a must because control of the vehicle completely relies on the instructions sent from the controller. If these instructions are modified on the way, it could prove very harmful. Though WPA2 has a few loopholes, some of this can be addressed easily. Channel can be secured by adding security measures like Digital Certificates, TLS and 2-way authentication. All these up the level of security of the transmission channel. This approach is implemented in this paper.

1 Introduction

In a swift of rushing into an autonomous world where devices are smart enough to perform tasks and train themselves from their own past experiences, security has become an apprehension. Today people are surrounded with different devices which are wirelessly connected to mobile phones and can be operated/controlled remotely. All these aims at providing mobility and better user experience to the people. Technology has reached to a magnitude where the vehicles are about to start driving on roads without any driver assistance or maybe where the washing machine itself would order washing powder when required. This reduces human efforts but at the same time instigates a fright in minds, What would happen if the device misbehaves or what if its hacked and misused? The questions seems fair to ask considering the cyber threats that the world is facing these days. There are many wicked minds in pursuit of some vulnerability which they can exploit and create havoc for some false reason which could be for money or even revenge.

This is why securing these devices or their communication channel between them is very crucial to avoid any third person from interfering or taking control over it and hindering the smooth working of these devices. The risk of being compromised needs to be considered with great concern and must be tackled with flat out efforts.

This paper deals with one such concern in context of a momentous project at Jaguar Land Rover (JLR). The project is called Remote Control Drive (RCD) which in layman terms, lets a driver to control the vehicle remotely using an application on the mobile phone. This application communicates with the vehicle over Wi-Fi and because of which the WPA2 vulnerabilities raised a concern and demanded efforts to secure the communication channel even more. These concerns are alarming because if a vehicle is compromised and if used for some immoral purpose, it could even lead to life threatening concerns. Dealing with this in advance is a priority part of this project.

It is an independent project accomplished by Ayush and Gaurav over a course of 12 weeks at JLR. It is primarily a simulation of the working of RCD for over both secured and unsecured channel. The ultimate objective being simulation to establish an even more secured communication channel to preserve the confidentiality and integrity of the sensitive data exchanged between the vehicle and the RCD application.

Section 2 expounds the related work done in different technologies which can be used for securing the channel for securely exchanging data over the Wi-Fi. This section also talks about the background of the project to help the reader to get comfortable with concerns and the need to develop a secured channel. Section 3 shades some light on technologies used for securing the channel and also a proper flow of the implementation of project. Section 4 elucidates authors contribution to the implementation. Different attacks carried out and different phases of involved in the development of secured channel are discussed in this section. Section 5 constitute of case studies and discussion about the observations and analysis of the attacks and later the paper concludes with a brief summary of everything.

2 Related Work

2.1 Background

Jaguar Land Rover, a British multinational automotive company, is one of the few companies that has shown illustrious advancement in self driving technology. It being a subsidiary of Tata Private Limited has a well earned legendary reputation of both companies at concern with every new launch of any new product or vehicle in the market. This makes it a prominent need for JLR to deliver its best and maintain a spotless position in the world.

Remote Control Drive (RCD) is an under development project with help of which JLR plans to get an edge when they enter in the world of self driving vehicles. Successful implementation and deployment of RCD would help JLR to climb up the ladder in the autonomous vehicle industry. As discussed earlier, RCD helps the user to drive their vehicle remotely by simply connecting the RCD application installed on a mobile phone with the vehicle over Wi-Fi.

The RCD functionality looks really appealing from a users perspective since it brings great ease of use. But from another perspective it brings a big time anxiety of being compromised and misused. Just like any coin flip, there stands two sides for this project aswell; where one being the benign motives of bringing automation in drivers hand and

other side where it might go in the hands of malignant fate which can be as threatening as threat to life.

But unlike natural disasters, this malevolent behaviour is avoidable if proper security measures are put in place where ever required. Ignorance of any vulnerability or loop hole might lead to paying off unaffordable price. This is how critical it is to deal with the pre-calculated risks and make concerted efforts to predict any future risks involved and also deal with them in advance if possible.

The product and its features needs effective security measures involved in its development since once the product is launched in the market it is not just the reputation of JLR that is at stake but also many lives. In order to be sure with the development a proper research was done for different technologies which could be considered from the security perspective and were analysed thoroughly before choosing the technologies. Section 2.2 discusses related work in the same area.

2.2 Literature Review

2.2.1 Wi-Fi

Wi-Fi in simple terms can be explained as wireless ethernet or as over the air connection between a device and the access point (Al-Alawi; 2006). Wireless networking technologies allow devices to communicate without cables. It is a protocol adopted in the past by 802.11 IEEE standard and devices needs to be approved by Wi-Fi alliance for incorporating it.[f1] Today almost every device makes use of Wi-Fi. Since it is very commonly used in day to day transfer of data or for connecting devices, it is significant to provide security to the channel over which the data is being transferred in order to maintain the confidentiality and integrity of it (Henry and Luo; 2002). Different protocols were launched in the past to serve the purpose of securing the channel are discussed below.

2.2.1.1 Wired Equivalent Privacy

As discussed earlier security has always been considered as an important problem that grows hand in hand with technological advancement. Similarly with wireless connections there appeared a risk of being compromised at any point. To deal with it, a security architecture was featured and was named Wired Equivalent Privacy (WEP). The name itself defines the objective of the protocol which is to provide secured connection similar to what a cabled connection would provide. WEP aimed at making lives of wicked people even harder by increasing the level of security (Buttyán and Dóra; 2006).

The protocol was ratified in year 1997 but soon in 2001 a few design flaws were exploited (Caneill and Gilis; 2010). And it was found that the protocol did not achieve its original design goals. WEP relied on RC4 encryption algorithm but its improper implementation lead the entire system to become insecure and unreliable (Kumkar et al.; 2012).

The most common attack on the WEP vulnerability has been key stream reuse. Since the RC4 depends on a constant secret key and a public key for encryption. And if same public key is used for more than one packet then all these packets are encrypted exactly

the same (Boland and Mousavi; 2004). This undesirable behaviour brings a major loophole in the algorithm and can be used to compromise the protocol. Regrettably this flaw was discovered after the protocol was deployed.

A few solutions were implemented in the industry to overcome the flaw. Like secret key size was increased from 40 to 104 bits. It proved to be a temporary solution since it would not solve the actual problem. Another solution was provided by Wi-Fi Alliance which proposed to upgrade to WPA protocol (Boland and Mousavi; 2004).

2.2.1.2 Wi-Fi Protected Access

After discovering flaws in WEP, WiFi Alliance constructed another WiFi protocol which was considered more secured as compared to the former one (Kumkar et al.; 2012). The protocol was named Wi-Fi Protected Access (WPA) and was made available in 2003. This new protocol in an attempt to avoid to key stream reuse vulnerability came up with primarily with two advancements.

First being increased size of the initialisation vector (IV) which is the public key. It was increased to 48 bits from 24 bits. Practically increasing public keys from 16 million to some 281 trillion which is a huge number (Boland and Mousavi; 2004). Second advancement in the protocol was switching from a constant secret key to a dynamic one. This brought randomness in the encryption scheme.

WPA acted as a very efficient patch against the WEP vulnerabilities. Since WPA adopted Temporal Key Integrity Protocol (TKIP) which still used RC4 stream cipher allowing to upgrade the devices to WPA from WEP (Potter; 2003).This protocol was more of a modified version of WEP with a few lines of code added to it. But still the solution was temporary, it too had a few problems.

The flaw would let a denial of service attack could be preformed if the attacker gets through different security levels in the protocol. The other flaw being a logical flaw in a function which initialises the encryption scheme. This flaw made the breaking of WPA easier than WEP (Kumkar et al.; 2012). But since this was just a temporary patch for WEP and the world expecting a more secured protocol which would guarantee advanced safety was most awaited.

2.2.1.3 Wi-Fi Protected Access 2

Finally in year 2004 Wi-Fi Protected Access 2 (WPA2) was officially announced and only certified devices were expected to use it. This protocol was expected to solve all the previously encountered problems. This protocol has two components first being encryption and second being the authentication. It uses Counter Mode/CBC Mac Protocol (CCMP) and Advanced Encryption Standard (AES) instead of RC4 encryption scheme. AES is an internationally accepted and is considered a robust encryption algorithm (Lashkari et al.; 2009). WPA2 also provides compatibility with WPA devices by using TKIP. It has two different modes : Personal and Enterprise depending on which the authentication is done. Personal mode makes use of a pre-shared key (PSK) to authenticate the user whereas Enterprise mode makes use of Extensible Authentication Protocol

(EAP) which is even more secured (Arana; 2006).

Inspite of WPA2 being considered the most secured protocol available till date it has some past found vulnerabilities. Key reinstallation attack being the most recent one (Vanhoef and Piessens; 2017). Now since the vulnerabilities are already discovered the protocol is vulnerable to different exploits. And for this reason WPA2 channel cannot be solely relied on for sensitive data exchange. For example, attacks on availability like Denial of Service, Key Cracking attacks on confidentiality of data and attacks like evil twin are capable of hindering the integrity of the data which is being exchanged over the channel.

Though it is vulnerable it is still considered the most secured protocol and is widely used. Wi-Fi alliance has announced the release of another protocol WPA3 recently. It aims at replacing the pre-shared key authentication with simultaneous authentication of equals. But complete adoption of this protocol might take a few years.

2.2.2 Cryptographic Protocols

These protocols provide communication security over a network. Cryptographic protocols aim at providing data privacy and integrity during the exchange of packets over the communication channel (Merritt; 1983). Some of the popular protocols are SSL and TLS and these uses certificates to secure the channel.

2.2.2.1 Secure Socket Layer

The SSL protocol was primarily developed to provide security to the data and avoid its modification or tampering while transmission (Al-Alawi; 2006). Different versions of the protocol were released to ensure the security of data and overcome previously found flaws. SSL version 1 was never published and version 2 was released in 1995. SSLv 1 and SSLv2 had various severe security flaws and were later replaced by SSLv3 in 1996. Comparatively SSLv3 was much secured than version 1 and 2. Still several attacks could be performed on SSLv3 on both, its key exchange mechanism and on the encryption scheme it used (Barnes et al.; 2015).

Poodle is the most common attack on SSL which breaks all the block ciphers. RC4 is the only non-block cipher supported by SSLv3 and even it is affected by the attack (Möller et al.; 2014). This attack stands for Padding Oracle On Downgraded Legacy Encryption. In order to exploit this vulnerability of SSLv3, the unauthorised person has to make only 256 requests to unveil the encrypted packets (Möller et al.; 2014).

All these justifies the fact that SSL protocol has proved to be unsecured and cannot be relied on for security.

2.2.2.2 Transport Layer Security

TLS protocol was developed with a similar motive to secure the data during the transmission. TLSv1.0 and SSLv3 differ slightly. This protocol constituted of two layers

named TLS Handshake and the TLS Record Protocol (Dierks and Allen; 1999). This version was launched in 1999 and it included a way to downgrade to SSLv3 protocol for backward compatibility; and this is why it was not secured enough to sustain for long.

Since TLSv1.0 was considered insecure and unreliable a new version namely TLSv1.1 was released in year 2006. This new version of TLS offered better security by making changes in the working of initialisation vector and also handling the padding errors in the protocol (Dierks and Rescorla; 2006). No real flaws did exist in this version but with a need of meeting new security issues the protocol had to be improvised.These improvisations were released in the newer version of the protocol called TLSv1.2.

Like mentioned above TLSv1.2 had a few improvements and to discuss a few it replaced the hash functions MD5 and SHA-1 with SHA-256 since both the functions used earlier could be broken. Then it supported AES encryption algorithm for better privacy of data. It even allowed using different authenticated encryption modes which replaces the CBC encryption mode (Dierks and Rescorla; 2008).

The above versions of the protocol are just minor improvements in the previous security flaws. And using the updated protocol is highly preferred to help in securing the traffic over transmission even more.

2.2.3 Digital Certificates

A Digital Certificate acts as an identity card for individuals/organisations. These certificates are verified and signed by trusted authorities[1]. A certificate contains all the necessary details about the owner. Digital certificates are widely used around the globe for authentication purpose. Certificate verification guarantees that the other party is who it is claiming to be. And to establish a secure communication knowing the person on the other end is a mandatory requirement.

Digital Certificates solve a big problem for public key cryptography which is the distribution of the public key and guarantees the authenticity of both the sender and the key. A certificate itself makes use of cryptography as it is signed by the private key of the root certificate authority. And to validate if the certificate is genuine, the public key of the certificate authority can be used against it.

Version 3 of X.509 format is used for these digital certificates. This standard is widely adopted by all the certificates to have a common structure of details. According to Housley et al. (1998), a typical digital certificate comprises of the following fields:

1. Version Number
2. Serial Number
3. Certificate algorithm Identifier
4. Issuer Name
5. Validity Period

[1]Microsoft : `https://technet.microsoft.com/en-us/library/bb123848(v=exchg.65).aspx`

6. Subject Name
7. Subject Public key information
8. Issuer Unique identifier
9. Subject Unique Identifier Extensions
10. Certification authoritys Digital Signature

Though digital certificates claims to valid identification but even these have some issues. Stealing root certificate authority certificates and misusing it to sign malicious content and distribute the content[2]. Also there exist issues with certificate authorities that issue certificates to the companies for usage. If identification of company is not done in depth and the company later is discovered to be fraudulent induces a severe security flaw due to irresponsibility(Leavitt; 2011). Certificate cloning attacks are quite with certificates.

2.2.4 Multi Factor Authentication

Single password protection has become an outdated solution for securing private accounts. Different systems have adopted different types of password patterns to provide greater security (Aloul et al.; 2009). For instance, some uses a 6 digit length alphanumeric password whereas some uses 9 digit length passphrase with special characters and other requirements.

This method of authentication is termed as single factor authentication. The problem with a single factor authentication is that if the password is leaked or exposed, any unauthorised person might use it to get authenticated and could get access to users personal account (Weber; 2010). And today with increased processing power many attacks can be performed to get through the security and gain access to the private accounts easily.

With the need to improve authentication process and safeguarding private accounts multi-factor or two factor authentication is more frequently used these days (Bauckman et al.; 2016). Similar to a single factor authentication a password is used for authentication. Along with this another medium of authentication is added to be sure about the person logging in. The other medium can be anything like getting a one time password through SMS or Email or even scanning a QR code from the phone.

Benefits of adopting multi-factor over single factor authentication can be justified as it is clear that even if an unauthorised person gets hold a users password, he/she cannot getting access to their private account unless the other factor of authentication is done (Owen and Shoemaker; 2008). This makes the authentication process much more secure and considering how commonly people use their phones the process comes in handy too.

[2] `https://zeltser.com/how-digital-certificates-are-used-and-misused/`

3 Methodology

3.1 WiFi Vulnerability Exploits

As discussed, the anticipated risk of any vehicle being compromised and used malevolently demands a strict counter action in advance. And as per above stated literature, in spite of WPA2 being the most secure out of all other Wi-Fi protocols, its vulnerabilities open doors for anyone to have a scope of compromising any vehicle (Vanhoef and Piessens; 2017). Closing these doors, or if not closing atleast blocking the entry through these doors, is the most significant part of this work.

In an attempt to do something similar, a simulation environment was developed using Java Socket Programming to test vulnerabilities and see if the communication over WPA2 channel is secure or not. After performing a few exploits like Wireless DOS, Dictionary, BruteForce and Evil Twin Attack; it was found that in some or the other way it is possible to find the pre-shared key and which is not a good sign for smooth and secure working of RCD. And if the channel is not secure and if it is possible for any third party to break in the network and compromise the vehicle, RCD has no good future as a product.

Attacks performed by the author are explained below,

3.1.1 Wireless Denial of Service Attack

This is an attack on the availability of a device or any service that a particular resource provides. A DOS attack is generally performed by flooding a particular resource by gratuitous traffic or requests to preoccupy the responding resource with unnecessary traffic and force it to shut down or become unavailable in some way so that it fails to respond to the legitimate requests (Ahmad; 2010).

In case of exploiting the WPA2 vulnerability, the access point was flooded with gratuitous packets sent periodically in order to flood the AP and force the two devices (viz. the Access Point and the authenticated device) to re-establish the connection and share the pre-shared key again.

3.1.2 Brute Force Attack

It is a popular attack similar to a dictionary attack, the only difference between two is instead of a pre-defined wordlist, all the permutations and combinations for a particular pattern of numbers and alphabets are tried to figure out the actual secret key (Apostol; 2012).

There are many well known tools available that can be effectively used from trying out different combinations of the key. The only problem with a brute force attack is that it can be very time consuming and requires a lot of processing power to try out different combinations (Bradbury; 2011). Sometimes the execution of the attack might take days or even months.

3.2 Development of Secured Channel

A simulation environment was developed using Java Secure Socket Programming with added security measures in order to add security to the WPA2 communication channel to avoid the sensitive data from being leaked or exposed. Transport Layer Security using 2-way Digital Certificate Authentication and multiple password authentications for the RCD Client was added to the authentication and communication process.

The digital certificates in this case were generated and signed in OpenSSL. A root and intermediate certificate chain was generated to sign the end certificates. The process is discussed in detail in section 4.3. The end certificates include the Vehicle Certificate and the RCD Client Certificate. Two level certificate verification was used so that the Root CA does not expose itself to the end entities. This helps in preventing Certificate Cloning Attacks to great extent.

In an attempt to secure the channel, Transport Layer Security protocol was used to prevent Man-in-the-Middle attacks and provide data integrity and confidentiality. TLS being a cryptographic protocol encrypts the data for transmission over the channel. Even if the channel is tapped the third person cannot figure out the content of the packets.

Adding to the security for authentication of the RCD client 2-factor authentication mechanism was implemented. This mechanism helps in gaining more control over the authentication process by asking the client to enter two different one time passwords generated dynamically every time. Even if a single password is compromised, the unauthorised person cant gain access until the other password is also sent to the vehicle.

All the above discussed technologies are used to provide additional security to the WPA2 channel and make it even more secure. The encryption of packets helps in gaining confidentiality and integrity to a great extent. Whereas digital certificates and two factor authentication helps in authenticating and authorising the user without any compromise.

4 Implementation

As mentioned above, a few attacks were carried out in order to verify if the vulnerabilities can be exploited in reality or it is just a theoretical concept. Section 4.3 includes different phases for development of secured environment for safe exchange of sensitive information over WPA2. It also talks about a differentiation between two different simulations carried during the internship.

4.1 Wireless DOS Attack

Using Airodump-ng[3] in Kali Linux, the handshake can be captured while the previously authenticated device tries to get itself authenticated again by sharing the pre-shared key again and establishing the handshake. The captured handshake file is stored with .cap extension.

Key Steps to perform the DOS attack are as follows:

[3] `https://tools.kali.org/wireless-attacks/airodump-ng`

1. Switch the wireless network card on the Kali Linux machine to monitor mode.
2. Scan through the network.
3. Find the target access point.
4. Run a replay/de-authentication attack on the desired access point.
5. Once the attack is successful, the two devices disconnect and re-initiates the process to reconnect.
6. When the devices tries to reconnect the 4-way handshake can be captured.

4.2 Brute Force Attack

Hashcat[4] was used for performing this attack using the handshake captured in the previous attack performed in section 4.1.

Key Steps to perform Brute Force attack are as follows:

1. For using hashcat, the handshake file needs to be converted into .hccap file. It can be done by either using online tool[5] or using command line tool as well.
2. Once done, the new .hccap file can be used to figure out actual password by trying out all the possible outcomes of a particular length of the password.
3. Current status can be checked whenever required. Lots of information can be found out the real-time status report.

Note: Dictionary and Evil Twin attack were performed and analysed by other team mate.

4.3 Development of Secured Channel

It was decided to incorporate Transport Layer Security, Digital Certificates and 2-way authentication to add up to the security of WPA2 channel. Entire development process was divided into 4 different phases. Each phase is discussed below.

Phase 1: Generation and Signing of Digital Certificates

For this simulated development self signed root certificate authority certificate was used. After the root certificate was ready, intermediate certificate was generated. The intermediate certificate was later verified and signed by the root certificate.

And this certificate chain was used by Gaurav (Teammate) to verify and sign the other certificates of client and server. All the certificate generation and signing was done using OpenSSL[6].

[4] `https://hashcat.net/hashcat/`
[5] `https://hashc.co.uk/cap2hccapx`
[6] `https://www.openssl.org/source/`

Phase 2: Keystore and Truststore Generation Keystore is used to store private key and the certificate of an entity. Two different keystores named KeystoreC and KeystoreS were generated each for the client and the server respectively. They were generated using keytool[7] in Java.

Truststore acts as common trust party which has the trust certificates or say trustworthy certificate authorities using which the signed certificates can be authenticated. This is why a single truststore was created named myTruststore.

Phase 3: Importing Certificate in Keystore and Truststore

Truststore acts as common trust party which has the trust certificates or say trustworthy certificate authorities using which the signed certificates can be authenticated. This is why a single truststore was created named myTruststore.

The certificate chain of the root certificate authority and the intermediate certificate was imported in myTruststore.

Phase 4: Code Development

Once all the certificates are in place, a proper initiation of certificate verification process can be started. The flow of the code had certificate verification of both the parties at both ends of channel. After the certificates were verified the server would initiate a TLS connection and start further authentication process by sending an email containing an 8-digit alphanumeric passphrase generated using secure random function in java itself.

The client receives the email and sends the passphrase to the server for verification over the encrypted channel. When the server verifies the received passphrase, it generates another 8-digit numeric pin which is displayed on the screen instead of sending it to the client. The client reads the pin and sends the pin back to the server for further verification.

When the server verifies the client, it allows the client to use the RCD features and remotely access the vehicle. Using all the added multiple layers of security the channel is expected to be secured to even greater extent than it was previously. Entire development process was done using Java.

The figure 1 illustrates a general flow of authentication without any added security to a basic WPA2 channel whereas figure 2 details the developed secured authentication flow of the process with added security.

[7] `https://docs.oracle.com/javase/6/docs/technotes/tools/windows/keytool.html`

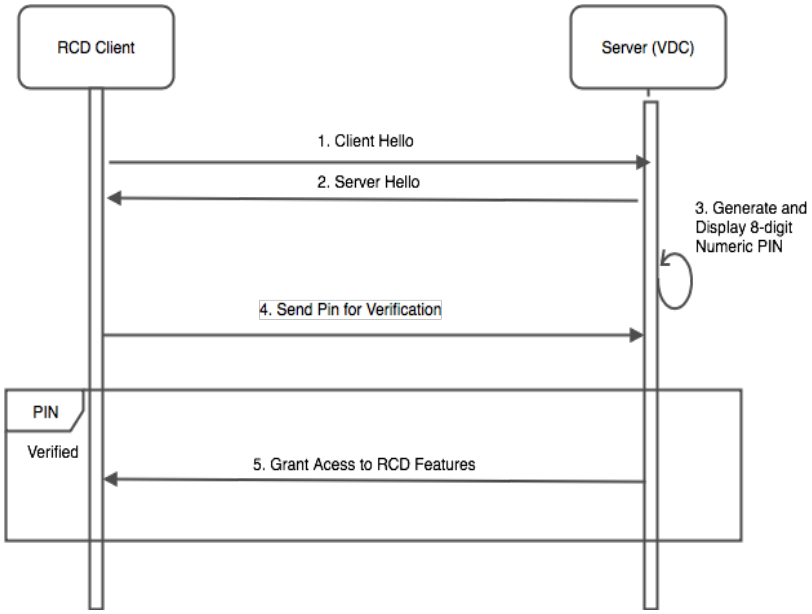

Figure 1: Basic authentication process

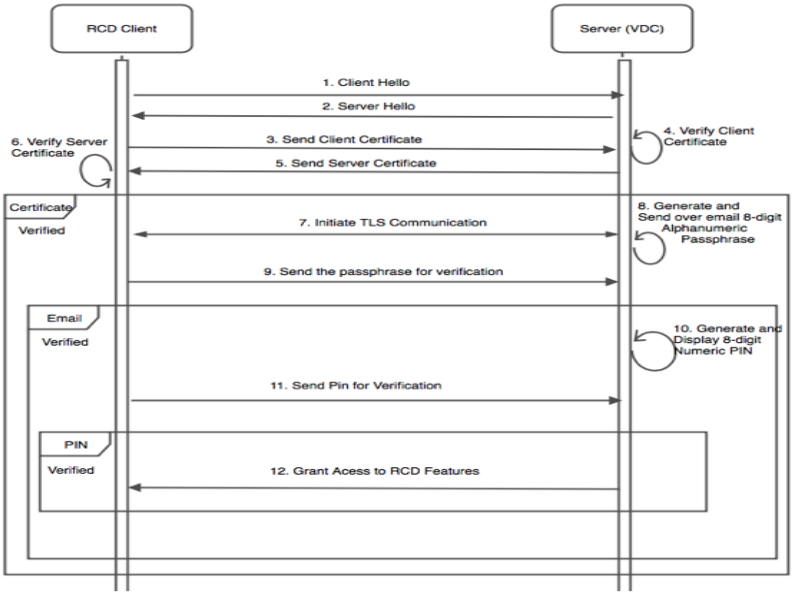

Figure 2: Authentication process with added security measures

5 Evaluation

5.1 Case Study 1

Based on figure 1, the packets transferred over the channel between the server and client were analysed using Wireshark[8]. It was very clear from the observation that the pin that the client sends to the server is transmitted in plain text and can easily be retrieved.

[8] `https://www.wireshark.org`

Figure 3 and 4 illustrates the traffic captured using Wireshark and the pin that was transferred over the channel from one entity to other.

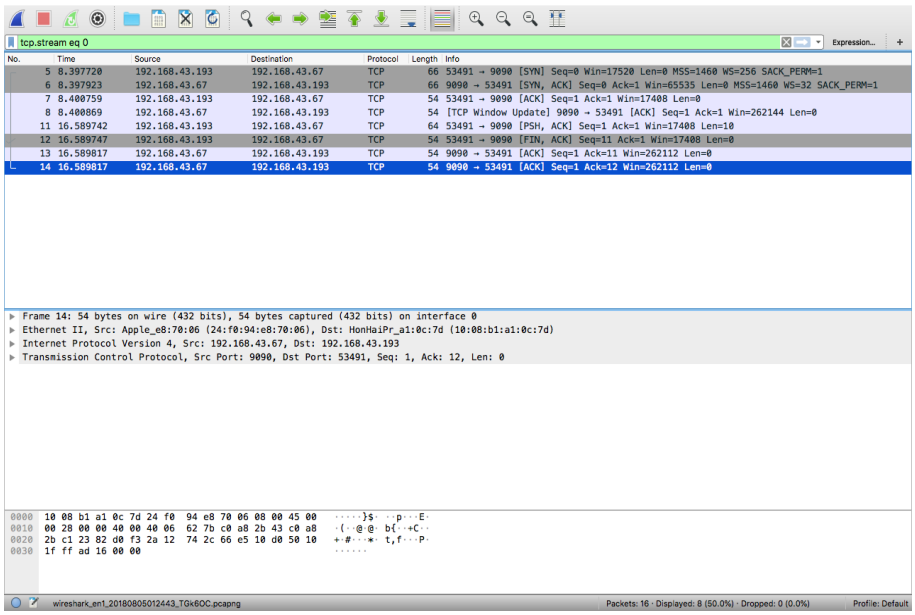

Figure 3: Traffic Captured over basic WPA2 channel

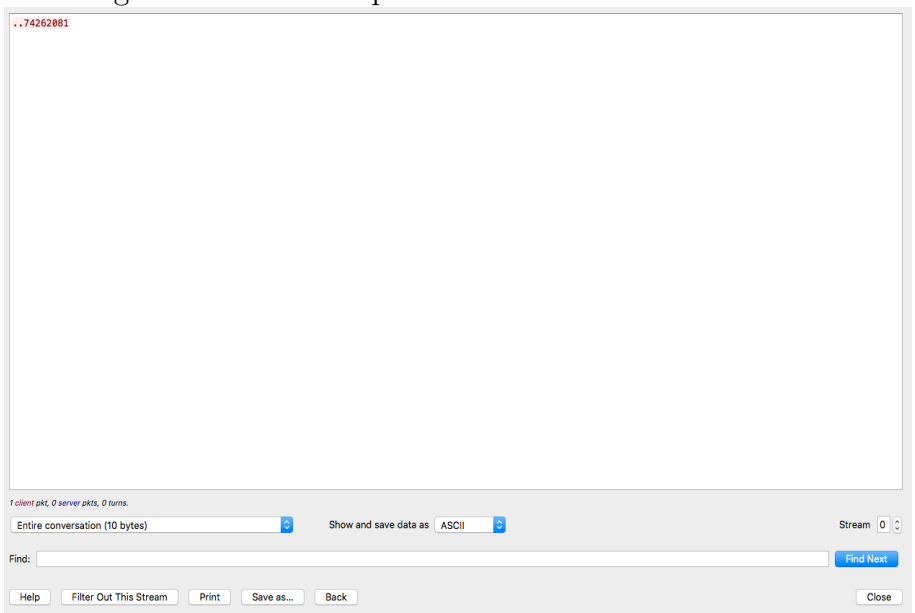

Figure 4: Clearly Visible Pin : Plaintext

5.2 Case Study 2

Based on Figure 2, the packets for the simulation with added layers of security was analysed using Wireshark. This time the traffic captured was more as compared to the first study. Also, the pin and the passphrase transferred over the same WPA2 channel is now encrypted and is hard to understand.

Figure 5 and 6 depicts the traffic captured using Wireshark and the encrypted data

of the packets.

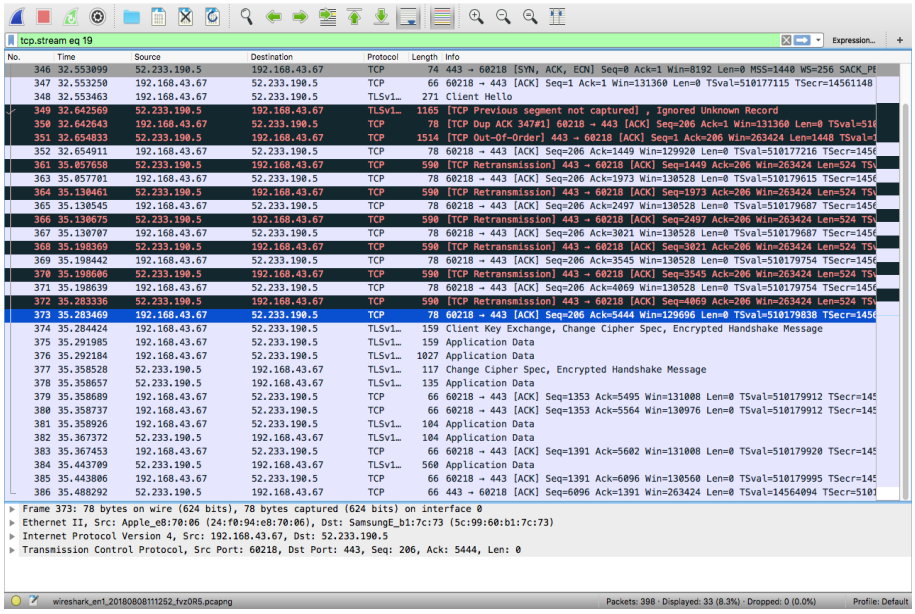

Figure 5: Traffic captured over the secured channel

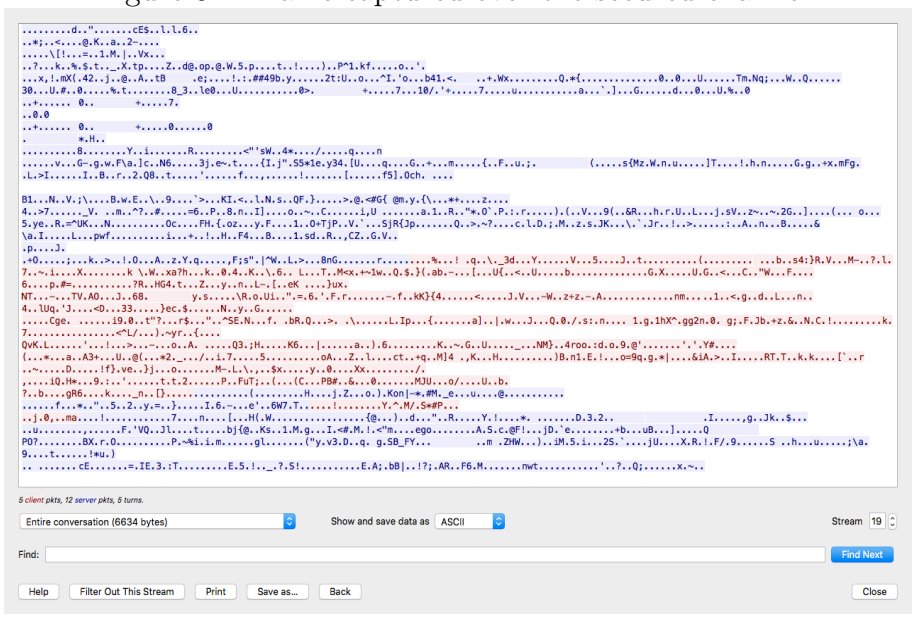

Figure 6: Data being Encrypted when transmitted over the channel

5.3 Discussion

WPA2 protocol for connecting the RCD application with the vehicle was selected because in spite of the vulnerabilities discovered in it, it is still considered the most secure Wi-Fi protocol. And adding security to a protocol which is already considered secured would add up to the safety of the vehicle and the user. TLS communication was chosen to maintain the privacy over the channel so that the data transferred between the application user and vehicle remains unreadable for an authorised person. This encryption protocol

enhances the level of security for in transit data.

Now for the vehicle to be sure of the RCD application user to be trustworthy a good authentication mechanism is required. Because its very important for the vehicle to trust the user before it grants him/her the remote controlling permissions. This is why digital certificates and 2-way authentication mechanisms were implemented.

Even the certificates are prone to different attacks like cloning attacks. But using an intermediate authority helps in eradicating that issue as well. Since the root authority remains unexposed. And for two factor authentication even if the unauthorised person gets one password, still another password which is sent over an email to the user is required to completely authenticate the user and gain access to the features.

In all, these measures together sum up to provide a greater level of security to the vehicle authorisation process and to the in motion sensitive data.

6 Conclusion and Future Work

Today with advancement in the cyber world, security has become a major concern. And it is necessary to take proper precautions so as to secure the products before deploying them in the market. Very often some new technology is released or some vulnerability in any old technology is found. To cope up with this uncertain upgrade and downgrade in technology and to improve it has become a mandatory thing. For instance, a few years back WPA2 was released to provide a heavily secured communication channel. And after a few years people started finding flaws/vulnerabilities in this most secured Wi-Fi protocol as well. It is considered the most secure protocol for last 14 years but even it is vulnerable. Still coping up with these and advancing more and more is really important.

It is said that if there is a code it can be broken. It doesnt necessarily be done right away but it might take years just like WPA2 instance. And one efficient way to add up to security is adding different layers of security to hide or say override different vulnerabilities. A similar approach was used to add up to the security of the channel.

The overall objective of the project was to try out exploits for WPA2 vulnerabilities and design a channel over WPA2 protocol with added security measures. The channel was even more secured by including TLS v1.2, Digital Certificates and implementation of 2-way authentication mechanism before granting permission to the RCD application user.

Entire development and securing process was a simulation of Remote Control Drive which lets the driver to remotely control their vehicle. Now since the idea of driving a vehicle can be devastating at times if the communication channel between the vehicle and the application is compromised. Considering this daunting situation a simulation for the secured channel was very important.

Since the RCD development is still in progress there is a lot that can be added or improved. Several application based features can be added like *(i)* Whitelisting mobile phones MAC address to avoid unauthorised access, *(ii)* Email can be encrypted, *(iii)* User

can be locked if more than 3 invalid attempts are made. Apart from these additions to the application, the simulation environment can also be tested in real environment with official RCD application and the vehicle to see if the security measures works properly in real scenario as well or not.

References

Ahmad, M. S. (2010). Wpa too!, *DEF CON* **18**.

Al-Alawi, A. I. (2006). Wifi technology: Future market challenges and opportunities, *Journal of Computer Science* **2**(1): 1318.

Aloul, F., Zahidi, S. and El-Hajj, W. (2009). Two factor authentication using mobile phones, *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, IEEE, pp. 641–644.

Apostol, K. (2012). Brute-force attack.

Arana, P. (2006). Benefits and vulnerabilities of wi-fi protected access 2 (wpa2), *INFS* **612**: 1–6.

Barnes, R., Thomson, M., Pironti, A. and Langley, A. (2015). Deprecating secure sockets layer version 3.0, *Technical report*.

Bauckman, D. T., Johnson, N. P. and Robertson, D. J. (2016). Multi-factor authentication. US Patent 9,509,683.

Boland, H. and Mousavi, H. (2004). Security issues of the ieee 802.11b wireless lan, *Canadian Conference on Electrical and Computer Engineering 2004 (IEEE Cat. No.04CH37513)*, Vol. 1, pp. 333–336 Vol.1.

Bradbury, D. (2011). Hacking wifi the easy way, *Network Security* **2011**(2): 9–12.

Buttyán, L. and Dóra, L. (2006). Wifi security–wep and 802.11 i, *EURASIP Jthisnal on Wireless Communication and Networking* (1): 1–13.

Caneill, M. and Gilis, J.-L. (2010). Attacks against the wifi protocols wep and wpa, *Journal, no. December* .

Dierks, T. and Allen, C. (1999). Rfc 2246: The tls protocol, *IETF, January* .

Dierks, T. and Rescorla, E. (2006). Ietf rfc 4346,, *The Transport Layer Security (TLS) Protocol Version* **1**.

Dierks, T. and Rescorla, E. (2008). The transport layer security (tls) protocol version 1.2, *Technical report*.

Gaurav, B. (2018). Secured communication over wpa2 for remote control drive, *National College of Ireland* .

Henry, P. S. and Luo, H. (2002). Wifi: what's next?, *IEEE Communications Magazine* **40**(12): 66–72.

Housley, R., Ford, W., Polk, W. and Solo, D. (1998). Internet x. 509 public key infrastructure certificate and crl profile, *Technical report*.

Kumkar, V., Tiwari, A., Tiwari, P., Gupta, A. and Shrawne, S. (2012). Vulnerabilities of wireless security protocols (wep and wpa2), *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* **1**(2): pp–34.

Lashkari, A. H., Danesh, M. M. S. and Samadi, B. (2009). A survey on wireless security protocols (wep, wpa and wpa2/802.11 i), *Computer Science and Information Technology, 2009. ICCSIT 2009. 2nd IEEE International Conference on*, IEEE, pp. 48–52.

Leavitt, N. (2011). Internet security under attack: The undermining of digital certificates, *Computer* **44**(12): 17–20.

Merritt, M. J. (1983). Cryptographic protocols.

Möller, B., Duong, T. and Kotowicz, K. (2014). This poodle bites: exploiting the ssl 3.0 fallback, *Security Advisory* .

Owen, W. N. and Shoemaker, E. (2008). Multi-factor authentication system. US Patent 7,373,515.

Potter, B. (2003). Wireless security's future, *IEEE Security Privacy* **99**(4): 68–72.

Vanhoef, M. and Piessens, F. (2017). Key reinstallation attacks: Forcing nonce reuse in wpa2, *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, ACM, pp. 1313–1328.

Weber, F. (2010). Multi-factor authentication. US Patent 7,770,002.