University of Amsterdam

System & Network Engineering

Tinfoil attack

Research on the security threats and weaknesses of GSM-based communication in a BMW car

Final report

February 11, 2013

Authors:
Thijs Houtenbos thijs.houtenbos@os3.nl
Jurgen Kloosterman jurgen.kloosterman@os3.nl

Tinfoil attack: Research on GSM-connectivity in a BMW car

Abstract

A recent trend in the manufacturing and development of high-end cars is to deliver Internet connectivity, entertainment and remote services to both the driver and passengers. The goal of the research described in this paper is to find out what security threats are introduced when a 2011 BMW 528i is connected to the Internet by means of a GSM connection. When the GSM-module was discovered, the hypothesis was to let the car connect to a rogue GSM-network and then constitute a Man-in-the-Middle attack. As it was not possible to either remove or disconnect the module, the antenna on the roof of the car was attenuated with tinfoil and the 900MHz signal was jammed with the use of a GSM jammer. With this approach, it became possible to let the car connect to the stronger 1800MHz signal of the rogue network. When the car was connected to the rogue network, it became possible to monitor the traffic which is exchanged between the car and remote systems. For the currently available features in the Netherlands this does not pose a large threat, but it is advisable to consider the security of GSM in combination with future remote services and to improve the means of authentication that is currently implemented.

Contents

1. Introduction

Modern cars become more advanced every year [1]. In-car computers have evolved from engine control to media and entertainment systems. As part of the European eCall project [2] all new cars delivered from 2015 have to be equipped with GSM and position determination functionality (like GPS). This system allows emergency services to act faster on road accidents as newly produced cars in 2015 are able to both automatically report and send crash data. Many car vendors combine the GSM-module which is now required in new cars with their own in-car systems to provide customers with extra services such as news, weather, e-mail and a web browser. Some vendors are going even further by developing smartphone applications to let customers use their smartphone to control features such as the ability to remotely lock and unlock doors, adjust climate control and to show the vehicle location on a map. In this project research is done on the setup of such a system and possible threats in the security are identified.

2. Research question

The goal of our research project is to answer the following question:

What security threats are introduced by connecting cars by means of a GSM-module to the Internet and can weaknesses be identified in the implementation in a 2011 BMW 5 series?

3. Scope

During this research the long-range communication in a 2011 BMW series-5, implemented by means of a GSM-module, and equipped with an active subscription of BMW ConnectedDrive [5], will be investigated from a security perspective.

3.1. Background

The initial phase of the research describes the BMW ConnectedDrive system and services and identifies possible security threats through the following questions:

- What features are remotely available?
- What security procedures are in place to secure them?

3.2. Remote services

The next phase of the research focuses on the implementation of BMW ConnectedDrive and the GSM-module in the 2011 BMW 528i in order to answer the following questions:

- Can the SIM-card be identified?
- What mobile network is being used?
- Can the network connections of the car be manipulated to connect it to a rogue network?
- What traffic can be identified and possibly spoofed?

3.3. Remote exposure

In this phase of the research information will be gathered to answer the following questions:

- How is the car system exposed to the public Internet?
- What information about the car is accessible by visited websites?

4. Background

4.1. Evolution of cars

In recent years cars have gone through ongoing development to either improve safety, efficiency and comfort. Since the introduction of the car, the following list shows some of the car parts that have contributed the most in this development.

- Aerodynamics;
- Type of engine;
- Tires;
- Weight;
- Accessories.

By measuring the aerodynamics and to model the optimal airflow on a car, cars have transformed from bulky machines to more resemble the shape of a drop of water. As air is no longer obstructed by various parts of a car, fuel is being saved. In addition, the fuel consuming engines from the past have been replaced by more fuel efficient ones, which also account for a decrease in car weight and notably the development of other types of hybrid or electrical engines. By choosing the right tire for the right combination of weather and surface, another improvement was made.

But it is the combination of these developments that as a whole constitute a more fuel-efficient and also safer way of driving. Accessories as driving safety systems further improve car handling and driver awareness systems in case of lane departure and also enable the car to alert emergency services automatically as part of the eCall project.

The eCall project is an initiative by The European Commission with the objective to provide a rapid assistance service in the European Union. New cars should be equipped with a device that is able to automatically alert emergency services and to transfer viable information such as the number of individuals on-board, which airbags have been released, the GPS location of the car to improve the response time and information about the accident for emergency services to come up with a plan to help the individuals in quickest way possible. Several manufacturers have come up with their own implementations, from which some eCall manufacturer implementations are listed in the table below.

Manufacturer	**Name of manufacturers service**
BMW	BMW Assist Advanced eCall
Volvo	Volvo On Call
Ford	Ford SYNC Emergency Assistance

Table 1: Manufacturers and related eCall service

Although the implementation is based upon the same eCall specification, it is reasonable for the manufacturers to distinguish themselves from one another. Therefore, a

comparison between the implementations is not carried out as that is outside the scope of the project [3].

4.2. Connectivity

When speaking of connectivity the term tends to grasp all devices that communicate inside- and outside the car. After the in-car telephone became redundant as of the introduction of Bluetooth-enabled mobile phones, more developments were introduced to further make use of the features that a modern mobile phone provides. In addition, recent developments also include the ability for an end user to connect to the Internet in the car, which is done by connecting the car to the GSM-network.

To give an example of a new feature for mobile phones: some manufacturers have even developed a smartphone application that can remotely invoke procedures such as locating a car or remotely unlocking it without the use of a key [6]. Examples such as Ford's Applink [4] show that the mobile phone has become part of the car and by leveraging a Software Development Kit end users can cooperate in further application development, which can provide manufacturers with insightful information about what end users feel should be a part of the system.

4.3. Introduction to BMW ConnectedDrive

The car that is used during this research project is a 2011 BMW 528i, identified by BMW as model type F11. BMW ConnectedDrive is the name of all the services that BMW provides in a BMW vehicle, on the Internet and also on a compatible Android or iOS smartphone. The next section shows an overview on the numerous services ConnectedDrive offers. Some of the ConnectedDrive services give customers the ability to call BMW for assistance or information, this service was therefore conveniently named "BMW Assist".

Configuration of these services is either adjustable through a web site and from inside the car. As the research primarily concerns the means of communication, not all services will be described with the same level of detail. The ConnectedDrive services can be divided in the following categories:

Information request An information request can be used to request general information about routes, countries and places. A personal assistant can be reached 24 hours a day, 7 days per week at the BMW Call center. Both a speech and data connection are set up, so that the assistant can send the search result directly to the navigation system or message inbox of the car.

BMW Internet A BMW car owner has access to the Internet in the European Union through the in-car browser. BMW Internet is accessible if the current speed is less than or equal to 7 kilometers per hour. The BMW Internet browser is able to show and load

Convenience	**Entertainment**	**Safety**
Google local search	News	Manual S.O.S call
Information request	Weather	Automatic S.O.S call
MyInfo	My news	
Send-to-car	Buienradar	
Country information	Office	
BMW Routes	BMW Internet	
Streetview.	Ski sites	
	Snapshots	
	Webcams	

Table 2: Overview of ConnectedDrive services

images, but it is not possible to download a file, view a Portable Document Format (PDF) file or (flash) video.

Manual or automatic S.O.S call In case of an accident or collision the car is able to connect to a BMW call center with the use of a data- and speech connection to inform emergency services. The vehicle supplies BMW with important information such as the location and chassis number, but also the sensor information to determine the number of people in the vehicle and deployed airbags. Other details include the intensity of the impact and what type of collision the car was in. Based on the data sent to BMW, the risk of injury for the people in the car is calculated. The call center employee will forward that information to the closest available emergency services in the region the car had that particular accident. Additionally, a direct call between the individuals in the car and the emergency services is set up. When the emergency services arrive at the location of the accident, it is only possible for the employee in the call center to terminate the connection to the car.

BMW remote functions This feature can be used to control car features outside the car to either (un)lock a door, to adjust climate control before the car is started and to find the car on a map.

My BMW Remote (Android and iOS) smartphone applications have recently been introduced, but to use this functionality a car owner has to register before it is ready to use. Until then a driver can call the BMW call center to carry out remote functions, although the availability of this option differs per country. According to the source of the ConnectedDrive [7] website this is indeed possible for BMW 5 series in the Netherlands from September 2010, although it varies between models. When a user is locked out of their car, they can unlock it by calling the BMW Assist call center, provided they know their username, password and answers to security questions which were supplied on a personal profile. The profile can also be accessed on a website [5]. Another remote function is the tracking service. A stolen vehicle sends GPS information to a BMW Service Center, which will then contact the rightful owner in order to report the current

location of the car. The Service Center is even be able to disable the engine from starting.

In the Netherlands there is no number available for the BMW Assist call center, but there is a number for emergency services (0800-0357). This number was called and a hypothetical problem was described: the owner has left the key inside a locked vehicle and needs a remote unlock of the car. The response to this request was that such functionality is not available in the Netherlands at this moment. No information could be given about when exactly this will be available. In addition, a BMW dealer was contacted. Although they clearly had not heard of a remote unlock function, they mentioned that this functionality would be plausible in the future, but did not know when this would be realized.

4.4. Vehicle Identification Number

In all communication with the dealer or manufacturer there is a possible need to uniquely identify a car. This is where the Vehicle Identification Number (VIN) comes into play. The VIN is a reference number used by the car industry to uniquely identify vehicles. The standard has been defined in ISO 3833 and is in use since 1954. The full number includes the following information:

- Manufacturer;
- Vehicle attributes;
- Check digit;
- Car model year;
- Car plant code;
- Sequential number.

Within a specific manufacturer only the plant code and sequential number contain enough information to identify the specific car. BMW uses this short version of the number in their digital systems, for example to check for firmware updates on their website.

5. Mobile networks

5.1. Global System for Mobile Communication

GSM is a technology used for digital mobile communication. It was developed in the 1980's by a special committee of the European Conference of Postal and Telecommunications Administrations (CEPT).

The wireless communication is established between the Mobile Station (MS) and the Base Transceiver Station (BTS). The MS contains the Mobile Equipment (ME) and the Substriber Identity Module (SIM). The BTS handles the radio part and forwards traffic to a Base Station Controller (BSC). A BSC connects one or more BTS stations to the Mobile Switching Center (MSC).

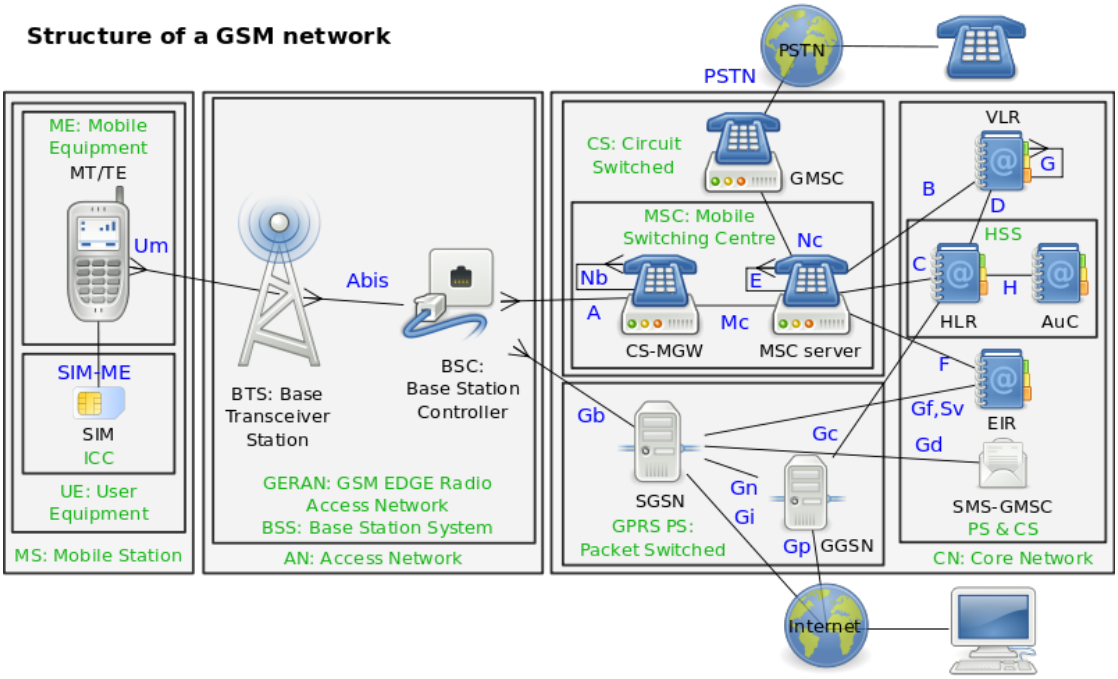

Figure 1: Structure of a GSM network

5.2. Subscriber Identity Module

The SIM in the GSM-network contains the subscriber information to identify the MS to the network. This is done by means of the International Mobile Subscriber Identity (IMSI) number which can be seen as the username in the authentication process.

Mobile networks are uniquely identified with a Mobile Country Code (MCC) and a Mobile Network Code (MNC). A complete list of all issued networks with their codes is published by the ITU[17]. The networks interesting for this project are listed in table 3.

The IMSI-numbers are administered by the network who supplied the SIM-card. To

MCC	Country	MNC	Network
204	the Netherlands	04	Vodafone Libertel N.V.
204	the Netherlands	08	KPN Mobile The Netherlands B.V.
204	the Netherlands	16	T-Mobile Netherlands B.V.
262	Germany	01	T-Mobile Deutschland GmbH
262	Germany	02	Vodafone D2 GmbH
262	Germany	03	E-Plus Mobilfunk GmbH & Co. KG

Table 3: MCC and MNC codes for relevant mobile networks

keep these numbers unique between different providers they start with the MCC and MNC numbers following a 10-digit Mobile Subscriber Identification Number (MSIN).

SIM-cards are also internationally uniquely identified by the Integrated Circuit Card Identifier (ICCID). This 19-digit number is stored in the SIM-card but also physically printed or engraved in the card. The ICCID starts with a maximum 7-digit issuer identification, the provider of the card, which includes a country code and an issuer identifier which is issued by the national regulation authority and often the same as the MNC.

5.3. Authentication Center

The Authentication Center (AuC) is a system on the carrier's part of the network. It holds the pre-shared secret key which is also present on the SIM-card module. This secret key is usually referred to as *Ki*.

When a MS subscribes on the network the *Ki* is used by the network to verify its identity. This is done in such a way that the actual key never leaves the SIM-card or the AuC.

This authentication is only done one-way. The BTS is in charge of all parameters on the network, including the used encryption. It verifies the identity of the MS, but it does not provide any means for the MS to verify the authenticity of the BTS.

After successful authentication of the MS it is provided with a Temporary Mobile Subscriber Identifier (TMSI) for use instead of the IMSI from then on in the current session. The authentication process between the AuC and the MS also leaves both parties with a shared secret *Kc* which can later be used by an encryption algorithm.

5.4. Encryption

GSM uses both frequency hopping and encryption to secure the communication. Both are dictated by the network, the MS can only accept the assigned proposal. For the encryption several ciphers of the *A5* family can be used, which consists of four different options named *A5/0* to *A5/3* (table 4).

The *A5/1* stream cipher is still the most widely used cipher in GSM-networks in Europe. Several research projects have focused on finding weaknesses in this cipher in the last ten years and can now successfully derive the *Kc* of an active session within

Cipher	Description
A5/0	Null-encryption
A5/1	Original encryption, stream cipher
A5/2	Weakened version of A5/1 for export
A5/3	KASUMI, newer block cipher

Table 4: A5 ciphers

seconds with a time-memory trade-off attack [8, 9, 10]. While one could look at the algorithm itself another possibility is to perform a downgrade attack or use no encryption at all (*A5/0*).

5.5. Frequencies

Worldwide two well-used frequency bands are defined for mobile communication systems using GSM.

Name	Band	Downlink (MHz)	Uplink (MHz)	Channels
GSM-900	900	890 - 915	935 - 960	1 - 124
DCS-1800	1800	1710,2 - 1784,9	1805,2 - 1879,9	512 - 885

Table 5: GSM frequency bands

It is up to individual countries to distribute these frequency bands between mobile operators. Most of them use auctions to do so. Some countries, like the Netherlands and the UK, have introduced frequencies for private GSM networks without the need for a license.

In the Netherlands part of the DECT-guardband, a spacing area to separate the DCS-1800 band from the DECT-band, is made available for private GSM[12]. These frequencies can be used without the need to get a license but with a requirement for registration with the government.

Name	Band	Downlink (MHz)	Uplink (Mhz)	Channels
DCS-1800	1800	1782,5 - 1784,9	1877,5 - 1879,9	874 - 885

Table 6: private GSM in the Netherlands

Starting February 26th 2013 the frequency space reserved for private GSM in the Netherlands is doubled and the registration requirement is dropped [13].

5.6. Fake Base Station Attack

As mentioned the MS has no way of authenticating the network it is connecting with. The only criteria for selecting a network comes from the preferred network list which consists of entries with MCC-MNC and an assigned priority. The factory assigned network has the highest priority to prevent roaming when not strictly needed, and usually includes partner networks in other countries to make roaming as cheap as possible for the network provider. When the MS is in a location with coverage of multiple BTS stations from the same network, it uses the signal strength as a last criteria to select the cell it will connect with.

None of the parameters involved in this selection process perform any form of authentication of the network. Thus with the right equipment it is possible to create a fake BTS, imitate the original network and trick the MS into connecting with this BTS by making sure it has the strongest signal in its range. The strongest signal depends mostly on the distance between the MS and the BTS. If the fake BTS is setup within meters from the MS it will always win this contest.

Since the network dictates the encryption protocol the fake BTS can simply tell the MS to use the *A5/0* cipher which is a null-encryption. The other ciphers cannot be used because the fake setup does not know the *Ki* stored on the SIM-card needed to generate a mutually known *Kc*. The MS must accept the parameters dictated by the network.

An attack like this has also been demonstrated and described at the Black Hat security conference in 2011 [11].

6. Test setup

This chapter describes the test GSM network that was setup during the project.

6.1. GSM network

A GSM-network was setup to see if it is possible to communicate with the car-systems on this interface. Open Source software of the Osmocom project [15] was used for the various parts needed to operate such a network.

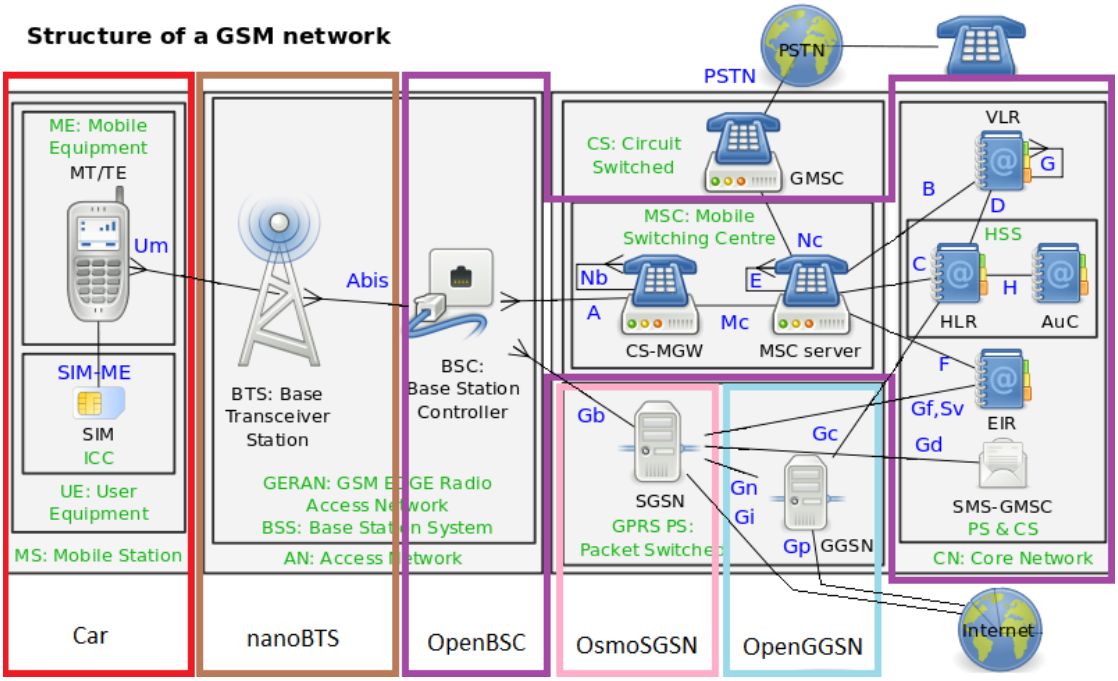

Figure 2: Test setup

6.1.1. Mobile station

In the test setup the GSM-module in the car implements the MS connecting wirelessly to the BTS.

6.1.2. nanoBTS

The wireless transceiver of the network was operated by an ip.access nanoGSM picocell supporting the GSM channels in the 1800MHz frequency range. Additionally the picocell has support for GPRS and EDGE data-connectivity with mobile stations and implements the Abis-over-IP protocol to connect with the BSC [14].

6.1.3. OpenBSC

The several systems needed to operate a GSM-network on the operator side are implemented by the Osmocom OpenBSC project [15]. The software supports the operator side of the Abis-over-IP protocol to connect with a transceiver station and integrates basic functionality for components like the Mobile Switching Center (MSC), Home Location Register (HLR), Authentication Center (AuC) and the Base Station Controller (BSC).

6.1.4. OsmoSGSN

The Serving GPRS Support Node (SGSN) handles the transition for data packets from the BSC to the GGSN. It can be seen as the BSC for data services. It also keeps the state for the current location of the subscriber within the BSC to route incoming packets on the correct circuit back to the MS.

For this project the software was patched to grant access to any subscriber requesting data access. By default only subscribers for which the MCC/MNC matches the running network are allowed to use data connectivity.

6.1.5. OpenGGSN

The Gateway GPRS Support Node (GGSN) connects tunneled data from the SGSN to an external packet switched network like a private intranet or the public internet. Providers operate a separate GGSN for every Access Point Name (APN) and interconnect with each other to exchange traffic from subscribers roaming on a different provider's network.

6.2. Network setup

The test network setup for this project has been run on the frequencies reserved for private GSM in the Netherlands (table 6). To prevent disruption of any operations on public networks the test network only allowed connections from devices where the IMSI-number has been manually approved to join the network. Any other device requesting to register on the network was rejected with cause 34 (Service option temporarily out of order) as defined in GSM TS 04.08 Annex G [16]. Furthermore the network was run with a low power setting in a remote area with open fields at least 100 meters in each direction. The test network indicated in its broadcast messages that this network cannot be used to contact emergency services by non-authorized subscribers.

7. Connectivity in the car

The device responsible for the car entertainment system is called *combox* in BMW cars. The connectivity between this device and remote devices is called *telematics*. In modern cars the combox and telematics are combined in one physical unit. Telematics wireless connectivity options include Bluetooth, GPS and GSM. Bluetooth for a connection with a mobile phone, a GPS receiver to determine the current position of the car and a GSM-module for connectivity used by remote services and to provide Internet in the car.

In the car used for this research the combox module is located above the rear-left wheel slightly hidden in a small compartment of the trunk. During the project efforts have been made to remove the inside of the trunk to physically inspect the module to determine what network operator provides the connectivity, but it turned out to be rather complicated to remove this part without breaking the car since the researchers are far from car-mechanics.

After inspection it turned out to be possible to enter the compartment to make photos of the equipment. On one of the photos a sticker was identified with interesting details like the type of the module, model number, part number, software version, hardware version and the SIM- and IMEI number (table 7).

Brand	Harman/Becker
Type	Combox Telematik BN2010
Model No.	BE a011
Part No.	84.10-9 257 151-01
Date	02.05.2011
HW	005.011.004
SW	003.004.031
SIM	89490200000716xxxxxx
IMEI	358279024xxxxxx

Table 7: Combox telematics module

As described in chapter 5.2 information can be derived from these numbers (table 8). For this research the provider responsible for the network access is interesting. From this number it can be concluded that the provider is one from Germany, which is very plausible since BMW is a German company. The specific issuer identifier was harder to determine from this information. Initially it was assumed that this would be Vodafone since the identifiers used in ICCID numbers often match MNC codes. Later it could be concluded from the IMSI-number that the provider is in fact T-Mobile.

Further technical details about this specific module were not found, except a test report from the certification for use on the network of the USA provider AT&T [18] which provides insight in the supported GSM frequencies and network types. The frequencies supported by the module are 850MHz, 900MHz, 1800MHz and 1900MHz with support for network types GPRS and EDGE.

ICCID	**8 9**	**4 9**	**0 2 0 0**	**0 0 0 7 1 6 x x x x x**	**x**
	Industry *Telecom*	Country *Germany*	Issuer	Individual account identification	Check digit

Table 8: SIM or ICCID number decomposed

8. Research

The research is primarily focused on the long-range remote connectivity provided in the car by means of a GSM-connection. To get insight in the traffic transferred over this connection and the security of that traffic a Man-in-the-Middle (MitM) attack was performed. Under normal circumstances the car is connected to the public mobile operator network (figure 3). No information about the network or signal level is available in the user-interface of the car.

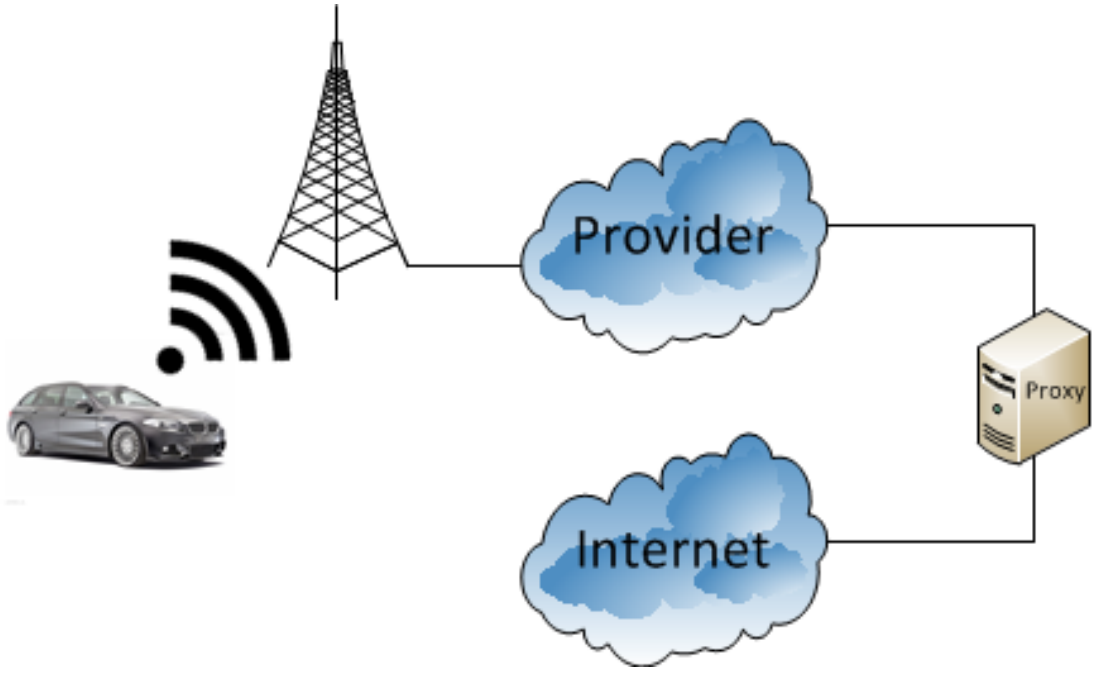

Figure 3: Normal connection

To analyze the traffic a test GSM network was created (chapter 6.1). The biggest challenge faced during this project was to connect the car with the test network. The GSM-module in the car is connected to the operator network during normal operation and when it is connected to an active network it will not actively search for new networks. Several attempts were made to disrupt the connectivity between the GSM-module and

the operator network, in order to force the module to search for available networks.

8.1. Power

The first idea was to temporarily switch of the power to the GSM-module. This would cause the active connection to drop and initiate a search for all the available networks and register on the most preferred one. Three possibilities were explored to disconnect the power of the module.

8.1.1. Fuses

All electric systems in a car are separated from the power bus by fuses. In case of a malfunction in any of the systems the fuse will burn itself due to the high power drainage and disconnect the failing system. Manually removing a fuse has the same impact, it disconnects one system from the power bus. The car researched in this project has two fuse boxes. One in the front of the car, behind the glove compartment, and one in the trunk of the car. Combined there are around 200 different fuses installed.

End-user documentation about the relation between a fuse and the connected system is provided with the car but this is far from complete. Only vague icons are used to describe the different systems in the car and it was not possible to identify the icon representing the combox module. Even the car mechanics at the BMW-garage were unable to find a link between the combox and any of the fuses in the technical documentation which is available to them directly from the manufacturer. Different fuses possibly belonging to the combox were disconnected but all without result.

8.1.2. Power cable

A second option to disconnect the combox from power was to remove the power cable connecting the combox to the fuses. As described in chapter 7 it was not possible to remove the parts from the car needed to physically access the module during this project. This blocked the possibility to remove the power cable

8.1.3. Disconnect battery

The last option to reset the power was to simply disconnect the battery in the car. All power in the car is provided by the battery so this would remove power from all systems in the car, including the combox. No more than five cables are connected to the positive side of the battery, for the negative side there is only one cable.

The negative cable was disconnected from the battery and kept loose for some minutes. Then it was reconnected while the test network was still running. Unfortunately the combox went straight back to the original network leaving the test network untouched.

8.2. Block radio spectrum

Another approach apart from removing the power off the combox module was to block the radio spectrum. The goal in this approach is still to disrupt the connectivity between

the combox and the public operator network, to force it to search for other available networks such as the test network. Available documentation for similar car models describes in very much detail where antennas for each system are located. The antenna for the telephone system and GPS receiver is placed in a fin outside the car on the back of the roof.

Special devices called *jammers* exist which are build with the purpose to interfere with the radio waves used in for example GSM. In the Netherlands most operators prefer the 800MHz-band over the 1800MHz-band. The lower frequency gives antenna's more range with the same amount of transmit power. The operated test network is configured on the 1800MHz-band. By jamming the 800MHz-band, where public operator networks broadcast, the combox module in the car should only see networks in other supported bands, like the 1800MHz.

The antenna in the fin on the roof of the car is more powerful than the one in a typical mobile phone. The combox is running on the power supplied by the battery in the car which has a much larger capacity than the one in mobile phones, it can use this to support higher transmit power. Portable jammers are operating on batteries and typically only work effectively within a range of about 15 meters. Presumably because of the large transmit power available to the combox and the good antenna, a jammer does not completely block all GSM radio signals sent to and from the car. Because the module still receives a small fraction of the signals it still considers the operator network to be alive and does not actively search for a new network yet.

8.3. Tinfoil

Tinfoil, nowadays made of aluminium instead of Tin, is a thin sheet of aluminium often used in households to conserve food or to shield cables. Aluminium is a good conductor and can therefore also be used to create a Faraday cage, an enclosure formed by conducting material that blocks or heavily attenuates external electric fields like radio waves. Placing an antenna inside a Faraday cage while transceiving radio signals with an antenna outside of the cage, will attenuate the signals and can, depending on the thickness or amount of layers of the cage, disrupt the connectivity completely.

During the research a cage of multiple layers of household tinfoil was placed over the fin on the back of the car in an attempt to disrupt connectivity between the combox and the operator network. The roof of the car is also made of conductive material and completes the cage on the bottom. Even with this cage in place the system was still connected.

When combining the tinfoil with the jammer, placing the jammer inside the cage, it is possible to simultaneously attenuate the external radio signal and block any remaining signals which now have a lot less strength. Only when combining the two methods it is possible to disconnect the combox from the public operator network (figure 4).

Figure 4: Combining tinfoil with a jammer

8.4. Connected

When the combox loses connectivity with the currently active network, it is forced to do a search for available networks in the process of selecting a new one. SIM-cards are programmed to give their home-network a higher priority in the selection process to avoid unnecessary roaming. By emulating the supposed home-network of the car it is possible to have it connect to the test network. Upon connecting the network identifies the mobile station by requesting it to send both the IMSI- and IMEI-number. The IMSI-number contains the real MCC and MNC of the operator who supplied the card (table 9). When the combox is connected to the test network all data traffic between the car and external systems are routed through the test network and can be inspected (figure 5).

IMSI	**2**	**6**	**2**	**0**	**1**	**4**	**3**	**4**	**x**	**x**	**x**	**x**	**x**	**x**	**x**
	MCC *Germany*			MNC *T-Mobile*		MSIN									

Table 9: IMSI-number decomposed

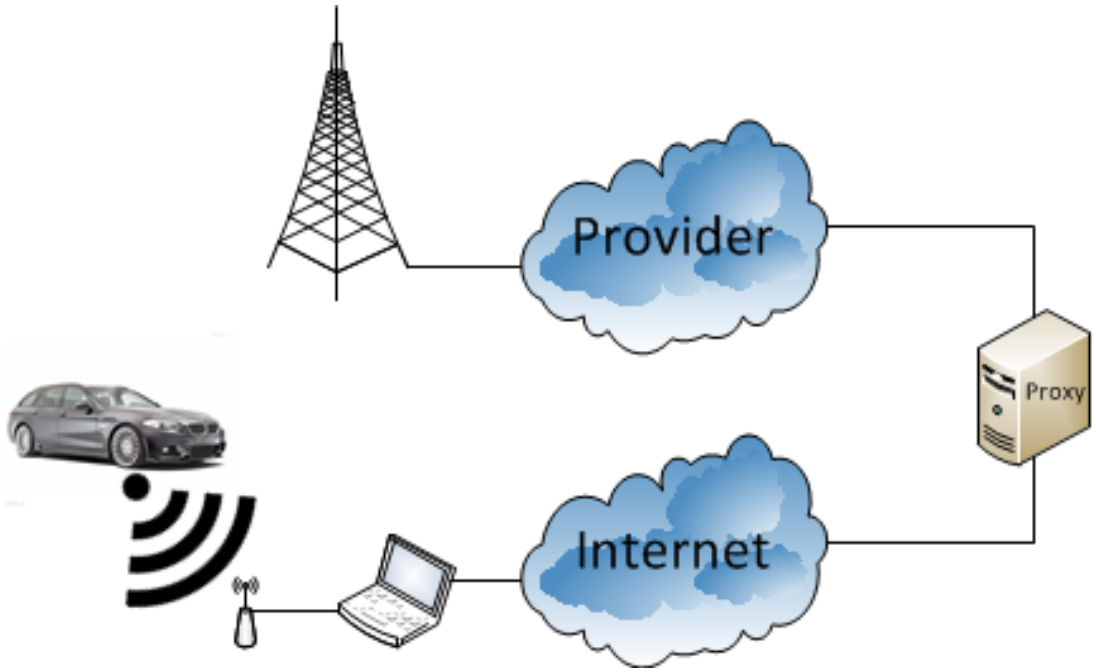

Figure 5: Connection to test network

9. Traffic inspection

9.1. Proxy

Traffic sent between the combox and the systems at the manufacturer is sent with HTTP through a proxy. Presumably this is done to separate the remote systems from the public Internet and to compress traffic sent to the car. The transfer rate on the GSM connection is not very high, maximum 114kbit/s on GPRS or 236kbit/s on EDGE, transfer times are decreased by compressing the traffic. Basic authentication is used to login on the proxy, this means the proxy username and password are transferred in a non-encrypted form over the network.

9.2. Vehicle registration

After the connection with a mobile network is established, the combox registers the car with the manufacturer (figure 6). The registration request includes the Vehicle Identification Number (VIN) (chapter 4.4).

A second registration is performed to register the location of a service supposedly called *PINGIUN*. Part of this registration is the IP-address of the combox, and a randomly chosen TCP-port on which a service is accepting incoming connections (figure 7). Basic authentication used for the proxy, meaning the username and password are sent base64 encoded, and the VIN identifying the tested vehicle, have been masked in the image.

Source	Destination	Protocol	Length	Info
192.168.0.4	160.46.255.1	HTTP	394	GET http://b2v.bmwgroup.de/nots/registerVehicle HTTP
160.46.255.1	192.168.0.4	HTTP	245	HTTP/1.1 200 OK
10.127.77.40	160.46.255.1	HTTP	394	GET http://b2v.bmwgroup.de/com/bin_auth HTTP/1.1
192.168.0.4	160.46.255.1	HTTP	599	GET http://b2v.bmwgroup.de/com/mainprov/prov.do?VIN=
160.46.255.1	192.168.0.4	HTTP	1181	HTTP/1.1 206 Partial Content (text/vnd.bmw.prov)
192.168.0.4	160.46.255.1	HTTP	595	GET http://b2v.bmwgroup.de/com/mainprov/prov.do?VIN=
160.46.255.1	192.168.0.4	HTTP	253	HTTP/1.1 204 No Content

Figure 6: Registration and provisioning

```
⊞ Frame 2418: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
⊞ Raw packet data
⊞ Internet Protocol Version 4, Src: 192.168.0.4 (192.168.0.4), Dst: 160.46.255.1 (160.46.255.1)
⊞ Transmission Control Protocol, Src Port: 65526 (65526), Dst Port: http-alt (8080), Seq: 1, Ack: 1, Len: 351
⊟ Hypertext Transfer Protocol
  ⊞ GET http://b2v.bmwgroup.de/nots/registerVehicle HTTP/1.1\r\n
  ⊞ Proxy-Authorization: Basic [redacted]\r\n
    Host: b2v.bmwgroup.de\r\n
    Accept: */*\r\n
    Proxy-Connection: Keep-Alive\r\n
    User-Agent: Aetsch0/1042901/\r\n
    BMW-Vin: [redacted]\r\n
    BMW-OTA-ID: 20130116-161629\r\n
    PINGUIN_RND: 2c\r\n
    PINGUIN_IP: 192.168.0.4\r\n
    PINGUIN_VERSION: 1\r\n
    PINGUIN_PORT: 50916\r\n
```

Figure 7: Registration and provisioning

9.3. Service identification

It is suspected the service listening for incoming connections on the combox can be used to remotely activate functions on the car, as part of the ConnectedDrive program. To activate functions on the car remotely an interface is required. A TCP-connection can be setup on-demand and without the delay and traffic overhead a polling solution would introduce. This would make it an efficient way to setup such a system. During the project efforts have been made to identify the service. The Nmap [21] services scan has been used to scan for known services. Nmap itself was unable to identify the running service, but upon manual analysis of the scanning traffic a reply of the unknown service was identified as reply to the service probe for TCP Kerberos [19]. The data in the reply appears to be encoded twice in ASCII. When decoding the reply data into characters

with the ASCII table and again decoding the resulting characters with the ASCII table the VIN number can be found in the message (table 10). To hide the identity of the car used for this research the VIN number in the example has been replaced with *A123456*.

Data	**Character**	**Data**	**Character**
31 32	1 2	12	DC2
30 30	0 0	00	NUL
30 30	0 0	00	NUL
30 30	0 0	00	NUL
30 30	0 0	00	NUL
30 30	0 0	00	NUL
30 30	0 0	00	NUL
30 30	0 0	00	NUL
34 31	4 1	41	A
33 31	3 1	31	1
33 32	3 2	32	2
33 33	3 3	33	3
33 34	3 4	34	4
33 35	3 5	35	5
33 36	3 6	36	6
30 30	0 0	00	NUL
30 30	0 0	00	NUL

Table 10: Unknown service reply

9.4. Web browser

One of the functions in the car entertainment system using the remote connectivity is an integrated web browser. The browser is identified as Access NetFront by the interface and the license details listed in the owner's manual [20]. Request headers have been collected by visiting a page hosted on a test server mentioned in the *Host* header.

```
Accept: */*
X-Forwarded-For: 160.50.X.X, 87.230.37.X
User-Agent: Mozilla/5.0 (Windows; Windows NT 6.1; rv:2.0b2) Gecko/20100720 Firefox/3.5
Accept-Encoding: compress, gzip
Host: minsk.studlab.os3.nl
Connection: Keep-Alive
```

Some of the headers contain remarkable information. The User-Agent used to identify the browser is set in such a way that it identifies as Mozilla Firefox 3.5 on the Microsoft Windows 7 operating system. The X-Forwarded-For header is added by proxy servers when forwarding the request for a client. The 160.50.0.0/16 range is registered with *BMW AG* and not advertised on the public Internet. It is possible this range is used to provide cars connecting with a special APN with an IP-address.

The browsers connects to webpages on the Internet through a proxy server. By hosting a proxy server in the test network on the IP-address of the official proxy server it is possible to provide the browser with internet access. Because there is full control over the connection webpages could also be forged or otherwise tampered with.

9.5. Provisioning

The connection is also used to provision the services in the car entertainment system related to ConnectedDrive. This provisioning can be manually requested with an option in the interface menu and occurs in an automatic way periodically. A small fraction of the XML-document is included in appendix A. The configured items include server addresses with port numbers, usernames, passwords and telephone numbers. Also the special APN name with corresponding login details is included. This APN is normally used by the car to connect directly to the IP network of the manufacturer. Public mobile network operators provide this service to large business customers and can deliver all IP traffic in the corporate APN via a dedicated- or VPN connection.

The provisioning information sent to the car is compressed but not encrypted. No signing of the data has been found, but a 229-byte stream of data in the provisioning document named *ecall* could not be deciphered during the research and could in theory be part of a signing process.

9.6. Applications

The car entertainment system contains several applications to directly access specific information. These applications include services such as the news or weather. When

accessing such a service the remote connection is used to request HTML-webpages with the information. The information is sent unencrypted (only compressed) to the car. As part of the project a modified version of the information pages has been hosted and presented to the car. The location of the pages has been redirected in the proxy server to use the modified pages when the newsfeed is requested. The car accepted them and displayed the modified pages in the application (figure 8).

Figure 8: Modified news feed displayed in the car

10. Conclusion

During this project the researchers have looked at the remotely available services and the implementation of the long-range connectivity implemented in a 2011 BMW 5-series by means of a GSM-connection.

The initial research showed that there are a number of remote functions available in the Netherlands, but it was unfortunately not yet possible to remotely unlock the car either through a mobile application or by contacting the BMW callcenter. The security procedures that are present to make use of a remote service can therefore only be considered from what is listed in the documentation. However, these procedures might change when the final service is introduced. Both the remote unlock and vehicle locator promise to be the most interesting from a security perspective, as improper security of those services can cause a risk for the car owner.

During the project the SIM-card has not been located but valuable information regarding the mobile network was still accessible. By setting up a GSM-network it is proven that the car can be made to connect to a rogue network after which network traffic can be monitored. By analyzing the data transferred over the test network it was possible to get an understanding of the communication between the car and systems of the manufacturer. The altered news feed showed that it is also possible to tamper with the communication. Although any serious implications may at this point be left for discussion, it is crucial to add an additional layer of security when implementing future functions like remote unlock or car location.

The problem which allows a rogue GSM-network to take over the connection is not due to wrong implementation in the car. It is a problem with using GSM-based networks and has been known for years. A real problem is trusting GSM-connectivity with sensitive data and without an additional layer of security.

11. Future work

Extract GSM information from combox The combox module contains information necessary to connect to GSM-networks. Part of this information is the pre-shared secret Ki to authenticate to the network and generate a session key for encryption. Future research could focus on the combox and a way to extract this information from the module. With this information it might be possible to create a connection to real GSM-networks while spoofing to be the car . This can provide access to the manufacturer network and possibly access to other cars connected in the same network.

Protocol analysis unknown service During this project it was not possible to identify the service running on the open TCP-port on the car. Future research could be to identify the service. A possible approach can be to extract the GSM key from the module and connect to the real network as described above. Once this connection is established the supposed communication from the manufacturer to the running service can be analyzed. Another approach can be to take the combox apart and search for an entry into the software running on it. There could be things like a hidden COM-port on the board or memory chips to dismantle and read.

References

[1] Car technology evolution, http://www.graphs.net/201208/car-technology-evolution.html

[2] eCall project, http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm

[3] EU eCall paper, http://ec.europa.eu/information_society/activities/esafety/doc/ecall/recomm/imp_assessm_fin.pdf

[4] Introduction of Ford Applink, http://arstechnica.com/gadgets/2013/01/ford-applink-opens- floodgates-to-in-car-ios-android-and-blackberry-apps/

[5] BMW ConnectedDrive, http://www.connecteddrive.info/index.php?cp_verfuegbar=nl

[6] My BMW Remote, https://play.google.com/store/apps/details?id=com.bmw.remote

[7] BMW Assist login, https://www.bmw-assist-login.com/cdp/release/internet/servlet/login

[8] Elad Barkan, Eli Biham, Nathan Keller, *Instant Ciphertext-Only Cryptoanalysis of GSM Encrypted Communication*, 2003.

[9] Tim Güneysu, Timo Kasper, Martin Novotný, Christof Paar, Andy Rupp, *Cryptoanalysis with COPACOBANA*, 2008.

[10] Karten Nohl, Sasha Krißler, *Subverting the security base of GSM*, 2009.

[11] David Perez, Jose Pico, *A practical attack against GPRS/EDGE/UMTS/HSPA mobile data communications*, 2011.

[12] *Regeling gebruik van frequentieruimte zonder vergunning 2008*, http://wetten.overheid.nl/BWBR0023553

[13] *GSM-picocellen*, http://www.agentschaptelecom.nl/onderwerpen/mobiele-communicatie/Dect+Guardband

[14] ip.access nanoGSM, http://www.ipaccess.com/en/nanoGSM-picocell

[15] Osmocom OpenBSC, http://openbsc.osmocom.org/trac/wiki/OpenBSC

[16] ETSI, *Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 specification (GSM TS 04.08)*, 1996.

[17] ITU, *Operation Bulletin No. 1019, Mobile Network Codes for the international identification plan for public networks and subscriptions*, 2013, http://www.itu.int/pub/T-SP-OB.1019-2013

[18] AT&T Developer Program, *Harman Becker Automotive Systems COM-BOX*, test report, `http://developer.att.com/developer/device_detail.jsp?id=6.3_v1_10800332`

[19] Nmap service detection probe list, `https://svn.nmap.org/nmap/nmap-service-probes`

[20] BMW 5-Series *Owner's manual for vehicle*, 2011, `http://5series.net/info/2011_5Series_OwnersManual_incl_xDrive.pdf`

[21] Nmap, `http://www.nmap.org`

A. Provisioning information

Information like telephone numbers, usernames and passwords have been masked. The goal of this project is to research the weaknesses rather than to expose sensible information.

Figure 9: Provisioning information

B. Abbreviations

APN	Access Point Name
AuC	Authentication Center
BSC	Base Station Controller
BTS	Base Transceiver Station
CEPT	European Conference of Postal and Telecommunications Administrations
DCS	Digital Cellular Service
DECT	Digital Enhanced Cordless Telecommunications
EDGE	Enhanced Data Rates for GSM Evolution
GGSN	Gateway GPRS Support Node
GPRS	General Packet Radio Service
GPS	Global positioning system
GSM	Global System for Mobile Communication
HLR	Home Location Register
HTTP	Hypertext Transfer Protocol
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
ITU	International Telecommunication Union
MCC	Mobile Country Code
ME	Mobile Equipment
MITM	Man In the Middle attack
MNC	Mobile Network Code
MS	Mobile Station
MSC	Mobile Switching Center
MSIN	Mobile Subscriber Identification Number
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
TCP	Transmission Control Protocol
TMSI	Temporary Mobile Subscriber Identifier
VIN	Vehicle Identification Number
VPN	Virtual Private Network
XML	Extensible Markup Language