Annual ADFSL Conference on Digital Forensics, Security and Law 2019

May 15th, 2:00 PM

Vehicle Communication Within Networks - Investigation and Analysis Approach: A Case Study

Dieter Steiner
Special Operations Command 11 , Germany, dieter.steiner@polizei.bund.de

Lei Chen
Georgia Southern University, lchen@georgiasouthern.edu

Darren Hayes
Pace University, dhayes@pace.edu

Nhien-An Le-Khac
University College Dublin, an.lekhac@ucd.ie

VEHICLE COMMUNICATION WITHIN NETWORKS – INVESTIGATION AND ANALYSIS APPROACH: A CASE STUDY

Dieter Steiner
Federal Police Operations & Investigation, Special Operations Command 11, Germany
dieter.steiner@polizei.bund.de
Lei Chen
Department of Information Technology, Georgia Southern University, GA 30458, USA
lchen@georgiasouthern.edu
Darren Hayes
Seidenberg School of CSIS, Pace University, New York, NY 10038, USA
dhayes@pace.edu
Nhien-An Le-Khac
School of Computer Science, University College Dublin, Ireland
an.lekhac@ucd.ie

ABSTRACT

Today, vehicles are an important source of digital evidence in criminal investigations. Modern day cars store a wealth of digital information, including recent destinations, favorite locations, routes, and personal data, such as call logs, contact lists, SMS messages, pictures, and videos. Moreover, the growth of in-vehicle sensors and event data recorders, which continually provide feedback to automobile manufacturers and third-parties, provide tremendous potential for forensics examiners. Recently, the field of vehicle forensics research has caught the attention of both digital forensics investigators and academics. To date, most relevant research have conventionally focused on digital traces of multimedia and GPS systems found in vehicles. However, today vehicles are manufactured with a vast array of communication options, including Wi-Fi, Bluetooth and NFC (Near Field Communication). Up until recently, these options were reserved only for the more expensive automotive models; nonetheless these capabilities are now available for just about all vehicle models. However, these vehicle communications and their corresponding networks have not been explored in detail as they relate to traditional digital investigations. Consequently, this paper focuses on the communications produced by modern vehicles and identifies relevant and important artefacts. Furthermore, as a case study, we examine types of data that can be captured, and methods used to extract artefacts from this data.

Keywords: Vehicle forensics, vehicle communication, vehicle security, forensic case study, Mercedes Benz car forensics

1. INTRODUCTION

Vehicle forensics is a relatively recent field of study, which has garnered interest from both academics and digital forensics investigators. Recent advances in technology, coupled with the introduction of new regulations, have generated more digital data and, consequently, provides a new source of valuable evidence for investigators. In terms of regulation, in some countries the government has mandated that all vehicles be manufactured with an event data recorder (EDR), or "black box", which continually captures data points that include speed, reliability of brakes, seat belt usage and many other important metrics. Other advances in technology have created new sources of evidence for investigators. The integration of smart vehicle technologies, which are often based on open source operating systems, create even more digital breadcrumbs. For example, most digital entertainment systems, are based on Android, and come standard with vehicles today. It has become commonplace for our smartphones to automatically connect, via Bluetooth, with our vehicles and to synchronize the contacts from our smartphones to our cars. Moreover, vehicle navigation systems, which generally come standard with vehicles today, provide a wealth of information for investigators. Vehicle navigation system evidence can include trackpoints, waypoints, track logs and routes, among others.

Today, vehicles contain a plethora of communication options, including Wi-Fi, Bluetooth and NFC. Automobile manufacturer Mercedes Benz has been a pioneer in developing cutting-edge information technologies, many of which were first tested in their A-Class models in an effort to gain big data feedback from their consumers.

The present-day existence of information technology in vehicles, and its use by vehicle manufacturers, began in 2002 with FMS (Fleet Management System), which allowed manufacturers to record live telemetry data, export it and, if necessary, provide real-time advice to truck owners to mitigate the risk of damage or prevent accidents. This information has resulted in companies being able to provide the optimal time and place where parts should be exchanged on a route and when inspections should be scheduled to avoid excessive delays. The increase in bandwidth in the mobile communications sector and the desire of customers to be permanently available creates an even greater digital footprint. These communication technologies were also introduced in passenger cars. Initially, cars maintained a Bluetooth transmitter to facilitate connections to the user's smartphone, but this has morphed into a GSM module, with a Bluetooth connection, NFC and Wi-Fi adapters [10]. These integrated vehicle communications have been further advanced with the introduction of Google Auto and CarPlay. Manufacturers develop applications to make the use of their vehicle smarter for the driver. Vehicle software updates occur wirelessly, and they also regularly transmit their telemetry data to the manufacturer. Tesla models communicate with other Tesla vehicles when in close proximity, which also facilitates updates.

The aforementioned discussion illustrates how automobiles no longer simply rely on the on-board storage of data but rather appear to be closer to the concept of a Smart Home network [14]. Moreover, on-board vehicle memory is now merely used as a local cache. Thus, there have been significant changes in vehicle networking, data storage, communication and the user experience. These dramatic changes have not been adequately addressed in the academic literature or by digital forensics investigators. Instead, they continue to rely on existing, well-known practices, including monitoring telecommunications and evaluating radio cell

data, or have focused on the extraction of data stored in the memory chip [11].

On the other hand, this permanent communication also poses a danger to deployed forces, which influence traffic behavior and location data due to this uncontrolled outflow of data and the potential for external influence, without any physical influence on the vehicle. Furthermore, the entire storage of vehicle data also represents a danger to manufacturers for concealed / legendary working forces, as a legend would have to be extended to these points. For example, human trafficking is one of the most frequently committed crimes today. To date, the investigator has aspired to gather data from navigation systems and smartphones. If this evidence was not used, a smuggling ring was difficult to profile, as routes taken were not detected. Utilizing the recorded telemetry data, by means of the aforementioned FMS, one would be able to determine the route, its duration and rates of speed. Amongst other recorded metrics, contents of the FMS include vehicle speed, service and distance [1]. This shows that manufacturers store information that may be critically important to investigations.

The purpose of this paper is to study communication data between the vehicle and the vehicle manufacturer, their value to investigators and the threat to their own assigned forces of security authorities. According to current opinion, data recorded from the vehicle flows directly to the vehicle manufacturer. Verified communication processes, representations of content and established data protocols could not be detected during the research phase. The contributions of this paper are:

- An innovative approach to analyzing data from vehicle communications;
- Explain the differences in communication protocols, from telemetry, to in-vehicle network modules (Wi-Fi, NFC, and Bluetooth) and remote vehicle connections via smartphone applications; and
- A case study on a 2016 Mercedes Benz E-Class model.

The remainder of this paper is structured as follows. In the next section, we briefly review related work in the context of vehicle forensics. We present our research approach in Section 3, and then the case study is highlighted in Section 4. We then describe our findings and analysis in Section 5. We provide a conclusion and discuss future work in Section 6.

2. RELATED WORK

Cars today contain a system similar to a network of computers with both wired and wireless connections. Hence, the probability for misuse of these communications has increased. Moreover, since many standards and protocols are identical to home networks, identical vulnerabilities exist [2].

Berla [3] with their iVe forensics tool, has been the preeminent force in vehicle forensics in recent times. The forensics data extracted can include travel routes taken by the driver, media, location information and connected devices.

In 2011, at the Usenix 2011, Checkoway et al presented an overview of the attack interfaces of a modern car [4]. Car manufacturers are not equipped to deal with these high-tech attacks, while network vulnerabilities persist.

Car hacking continues to be problematic today, whereby a hacker could actually endanger the lives of people in a car by taking over the steering wheel or applying brakes. For example, a Jeep was hacked by Valasek and Miller, who presented at DefCon 2015 and the details of the compromised vehicle were described in a recent white paper [5]. Of particular note was their ability to control the

steering wheel and make the car "turn sharp left" and then veer off the road. Another note is that they managed to successfully query every Jeep and car, with the same on-board unit, and determine their present location. It was however challenging to communicate with a single car, as opposed to communicating with just one targeted vehicle.

Research conducted by ADAC, the German automobile club, discovered several weaknesses in BMW's ConnectedDrive [6]. It prompted BMW to introduce HTTPS connections to the factory, instead of maintaining weaker HTTP connections.

Research conducted by the FIA in 2015, entitled "My car, My data" provided an overview of the data a car is collecting [7] on both drivers and passengers. It should be noted that not all similar data is sent over a mobile connection, while it can be read by the maintenance software of the manufacturer.

In a briefing note, BigBrotherWatch.UK made several startling statements about the potential misuse of e-call [8]. Interpol informed the Sunday Times that e-call is already used by some police forces to track cars [9].

Apart from the technical possibilities, an ethical discussion arises if all of these possibilities can be used to fight crimes. One opinion is that by embarking on a life of crime, you are willingly sacrificing your privacy. Conversely, another opinion is that innocent citizens should not have to sacrifice their privacy [15].

In [10], the authors described some of the challenges associated with digital forensic investigations of vehicle systems. They demonstrated how artefacts of forensic interest could be recovered from the various electronic modules and placed such as memory chips of the entertainment system in a Volkswagen car. They did not discuss the vehicle communication data.

The authors in [11] addressed vehicle communications by demonstrating how to analyze mobile wireless data to examine the location and use of a vehicle.

3. PROBLEM STATEMENT

Nowadays, vehicles reside within a network where data is collected, transported and analyzed. More and more vehicles communicate with the automaker's server, via the provider's installed IMSI (International Mobile Subscriber Identity), while telemetry controllers are directly connected to the automaker's data center. Additionally, automobile exhibitors have already implemented an eCall called TPS (Third Party Service) in their systems. This protocol transmits a greater level of encrypted data in comparison to the EU directive and with the EU eCall service [16]. The manufacturers may continue to offer their own emergency service, TPS-eCall, as an alternative, in addition to being able to offer additional services. This will allow additional information to be obtained despite encryption. Statements made by the security authorities, in reference to the eCall system, view the system as being politically sensitive since the system has been a target for malware (backdoor), which impacts some EU countries. Access to TPS systems, by the security authorities, has been facilitated with court orders. However, access to these systems has been quite restrictive. In this case, the car-sharing operator would initially hand the data over to the court for evaluation, in response to an order from a higher regional court. These data were not handed over to the police investigative office. The opportunity to gain deeper insight into the communication process improves the probability of obtaining while also being more targeted. As a result, investigators and forensic scientists are faced with a quandary in the absence of legal standardization for this data, which in turn cannot be collected.

In fact, data generated by devices connected to a Wi-Fi hotspot, is assumed to be the property of the official provider. Generally speaking, it is currently a complex matter to gain usable data from the communication traffic of vehicles. Most traffic is encrypted using SSL / TLS in the TCP / IP model, and found within the transport layer. In addition, the encryption of data directly after its creation within the used system is of importance, as well as data which are kept ready for transport. This poses a problem for investigators and forensics analysts since the data is not readily available to be captured, analyzed and processed.

Hence, the aim of this paper is to recognize how vehicles and computing centers communicate and which communication structures can be identified. Data is transmitted and analyzed by means of telecommunication monitoring. Nevertheless, it is important to clarify whether the previously legally required data is still sufficient or whether an adaptation of laws and technical systems is required. The existing traffic and its analysis are determined by the possible communication directions available via the Internet, for which a network module controls different communication paths: (i) Telemetry; (ii) Manufacturer Smartphone application remotely connected to the vehicle; (iii) Smart Device.

In order to achieve the aforementioned objectives, the approach should be determined by the network protocols and telecommunication data, so that (i) communication directions can be tapped, (ii) protocols are recognized, (iii) content is evaluated and (iv) the necessary adjustments to systems and legal bases are recognized.

4. CASE STUDY

4.1 Experiment Platform

For this research paper, a Debian-based operating system, Kali Linux 2017.3, was used. Wireshark v.2.4.6 was utilized to process archive files and parse individual frames. Dshell, with Decode v.3.0, was used for an advanced analysis of the converted files. A breakdown of the routes, addresses, and the associated stored content was performed with the OSINT (Open Source Intelligence) tool Devploit v.3.6.

The warden data packets, derived from the network traffic between the vehicle and server platform, are required. Through existing frames, and the information contained therein, an analysis can be performed, and a conclusion established.

To perform this procedure, a vehicle model with a GSM/UMTS (Universal Mobile Telecommunications Service) module, which was a Mercedes-Benz E350 built in 2016, was selected. Using this module, all data generated within the vehicle, via control units, infotainment system, navigation system, Bluetooth and WiFi, we deactivated. To obtain a comprehensive overview, we collected data via telecommunication diversion. As a result, various file formats were created and subsequently converted. The stored data includes information about all of the systems involved, the time that the network connection was established, the amount of data, the route of the data transfer, the protocols and services.

The vehicle can only be monitored if the IMEI (International Mobile Equipment Number) or the IMSI is transmitted to the provider. Since the data was not available on request from the vehicle dealer, the vehicle was monitored using an IMSI catcher. The mobile standard for each vehicle module can communicate while the IMSI is activated (Nederland, Vodafone Libertel in our experiments)

A connection was established using a data call number +882 39XXXXXXXXXX and this carrier code represents a number from Vodafone Malta and is listed under International

Networks. This phone number is used to open and keep a data port using the GPRS service. Within the telecommunications monitoring system, only the outgoing call could be determined, and the phone number of the other party was unrecognizable. Subsequently, the various file formats and their functions were presented and followed by a complete telemetry communication between the control units of the vehicle and the target servers addressed by the various protocols.

4.2 Data

In our case study, the raw data was collected by a third party, i.e. the provider, who adjusted the data to comply with the German Telecommunications Act.

Snoop files

The creation of the snoop files builds on the provider-created raw data. As previously mentioned, we are referring only data that the provider is obliged to produce by law. The snoop format was selected based on the underlying architecture of the telecommunications surveillance system. The telecommunication system wardens the raw data by communication string and converts it into a snoop archive. In order to carry out an analysis of this data, by means of the aforementioned programs, they were exported from the telecommunication system. Only pure network data, not telecommunication data can be exported. The disadvantage is that the connection cannot be represented by means of data packets.

pcap files

The *pcap* format stands for packet capture and utilizes a free network interface. By creating network data with the extension pcap, network analysis tools can analyze and process this data offline.

The Snoop files are probabilistic Oracle Solaris archives. Although they are compatible with Wireshark, they are built on Kali Linux command line utilities, e.g. it is not possible to use the network forensics framework Dshell (US Army Research Lab), as these concerted *.pcap* archives contain significant deficiencies in the information they contain. This deficiency is caused by the provider itself, as it represents a data overload for him. For example, this is characterized by missing MAC addresses in individual frames.

As previously mentioned, the telecommunication monitoring system created archives for the communication setup / execution. For analysis and research of the communication channels these archives were summarized daily.

4.3 Car Telemetry Information

By definition, telemetry represents the remote measurement and transmission of measured values of a sensor (control unit) located at a measuring location (vehicle) to a spatially separate location. This receiving station can collect, record and / or evaluate this data. The telemetry method used in this area is referred to as far field telemetry, since the measurement data is transmitted over longer distances. During our experimentation, our tests were performed using an integrated eSim GSM/UMTS module. As a protocol for data transmission, the GPRS protocol (General Packet Radio Service) was used. The 2017 test vehicle utilized an LTE (Long-Term Evolution) module.

GPRS

GPRS is a packet-oriented service, which allows a connection to be maintained without permanently reserving a radio channel. Only in a real data transmission, the radio room is occupied and is locked for other users. Another reason why this protocol is used is that delivery costs are calculated by volume of data rather than duration of connection.

Akamai Technologies

Akamai Technologies, Inc. is an American content delivery network (CDN) and cloud service provider. Akamai's Content Delivery Network covers between 15% and 30% of all web traffic. [3] This hardware deployment represents a speed increase for website operators, as it always drives the server closest to the end user. This means that no original web pages of the domain are accessed, but web page copies on servers of Akamai Technologies.

4.4 Car Application Information

For vehicle models with GSM / UMTS / LTE modules, the vehicle manufacturer offers applications for smartphone users.

These provide the potential for (i) remote control of the vehicle, (ii) information transfer from current events, and (iii) personalization of ECUs (Engine Control Unit).

The connection between the application and the vehicle communication servers are outside of the telemetry network. The use of the application (s) requires registration and activation by the vehicle owner at the vehicle manufacturer, as well as the establishment of a user account. For this device, vehicle data from the vehicle registration, in addition to proof of ownership were needed. The following protocols and procedures were therefore recorded.

This first communication setup was exported and displayed by Wireshark.

As previously discussed under Devploit, the tool displays a variety of servers that are addressed by the application and supplied with information. In addition to various paths, that may have to do with the application itself, there are also two connections that represent "places.mercedes-benz.com" and "production-suite.mercedes-benz.com". Both show yet another peculiarity that the data traffic is handed over to Akamai Technologies. The other available means of communications are via Deutsche Telekom AG (DTAG).

4.5 Car Internet Information

In this section, the communication structure / process on the World Wide Web is considered. This consideration is limited to the first structure / process since all further processes are identical to a normal Internet communication.

Before a communication to the Internet can take place, the IMSI of the installed eSIM module must be activated by the provider. The activation takes place in the customer center of the provider personally, an online registration is not provided. After this activation, devices connected to the vehicle's Wi-Fi can dial IP addresses in the public area. Below are screenshots of the activation phase of the Internet Inthecar account (Figure 1).

Interestingly, inquiries are initially made to Google and Apple and only then a request to Vodafone takes place. Here, was the expectation that Vodafone's communication platform would take place first and then the connections of the operating systems, applications and other data connections.

This process means that the communication ports were opened from the outside and an internal configuration was not required. This is because Google and Apple made direct inquiries and set up a communication link.

Another finding is the lack of device allocation, based on this network data, an assignment to a device is not possible, which can be of crucial importance in an investigation.

Furthermore, no RTP (Real-Time Transport Protocol) stream was detected by Wireshark, as well as no Wi-Fi traffic. In contrast, in the package 4043, http information was sent which was "hotspot-detect", which signals the successful connection to an access point. Due to the non-existent data, one can only interpret and speculate which devices are communicating via the UMTS module at this time.

4.6 Monitoring Wi-Fi module

In order to detect and verify data processing algorithms, the previous Wi-Fi module was recorded using *airodump-ng*. This was done with a laptop connected to an Alfa Networks Wi-Fi antenna AWUS036ACH.

4.7 Artifact capturing and extraction

4.7.1 Dshell

The program Dshell represents a network forensic framework, which supports the decomposition of network acquisitions through plugins. Using Dshell, the required information of the pcap file was converted by decoder into a text file.

Reverse-flow generates a message if the client transmits more data than the server. The default threshold value 3.0, means that the client transmitting data is three times as much data as the server. This decoder is used to detect communication irregularities, since usually the data sent by the server is usually larger than the one supplied by the client. This may indicate that the client is sending more information at once because it has broken connections or contained information for forwarding to clients or servers that are not included in the TCP response of the server. The data obtained thereby shows us the source IP, which represents a private IP of the BTS, the destination IP, which is displayed to us in the form of an open IP and hereafter unit how many times more data the client sent to the server than vice versa. For example:

```
  10.33.228.130:46861 -> 80.154.131.254:443 **
client sent 9.40 more than the server **

  10.33.228.130:46863 -> 80.154.131.254:443 **
client sent 4.36 more than the server **
```

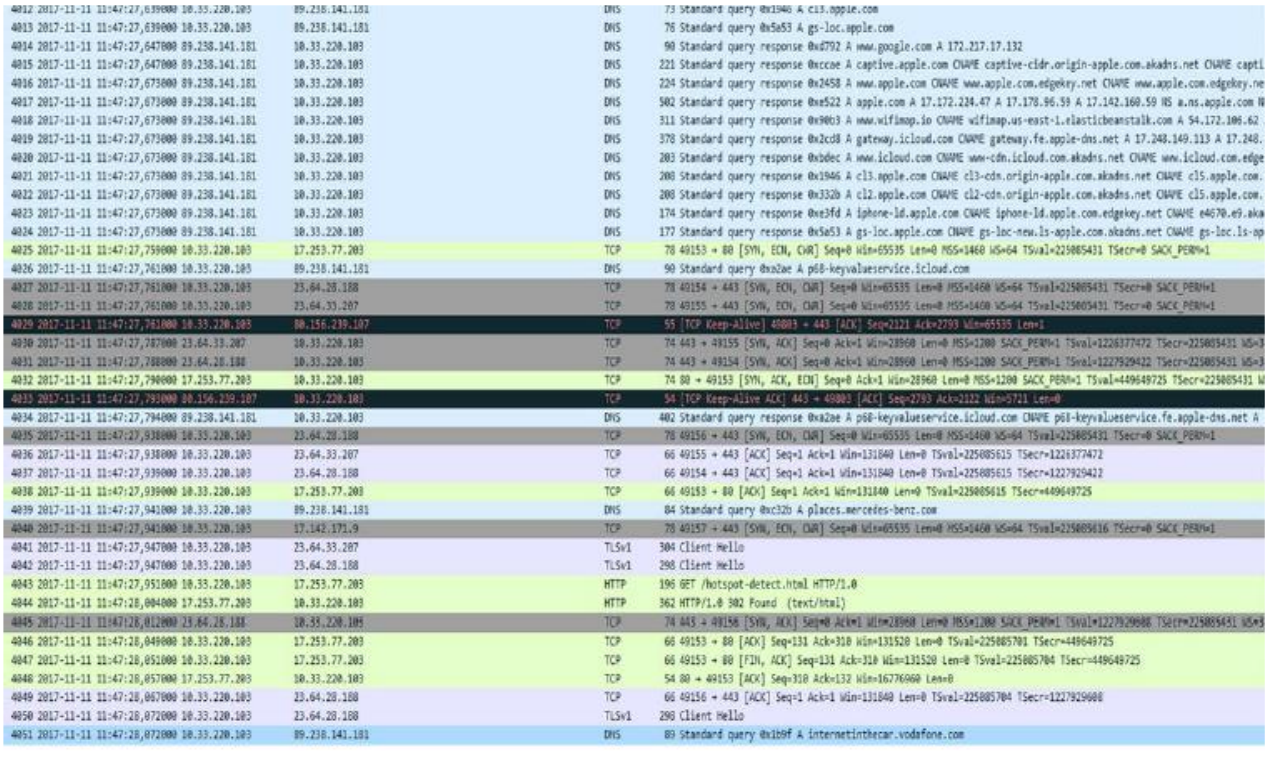


Figure 1. Activate phase of the Internet Inthecar account

netflow, Real-Time Transport Protocol (RTP) information were also generated.,

followstream content is displayed in the same sequence as it appeared on the network. This decoder was used to represent content of the data transfer. HTML was used to make the transport easier to capture. The area shown here has been reduced by the unreadable, encrypted areas. Subsequently, a connection between vehicle and server is shown, it was shown only data which were freely readable, except for the area of the encrypted content data content which was not verified was deleted for better representation.

4.7.2 Devploit

The Devploit tool [13] developed to gather information from Joker Security. It brings together various OSINT tools in the field of network reconnaissance. This tool chosen because, although several products are combined under one roof, they are not executed automatically.

Telemetry data. The servers involved and the communication process show that investigations in a technical evaluation, without content analysis, can display modules that provide new starting points. The following diagram intended to clarify connection processes within the IP data network. The connection establishment and the keeping open of the data ports takes place via a GPRS call. This call used in all forms of communication (telemetry, remote app, InternetInTheCar). The resulting problem areas discussed later.

Remote Application Mercedes Me. Here it shown which requests, IPs and protocols the smartphone application uses, which connections established between the vehicle and the communication servers. The excerpts provided here intended to illustrate this overall. The vehicle dealer activated this application shortly after the start of the surveillance. In the following examples, only the application compounds per se and hereafter two further compounds that are not directly used by the vehicle /application user but are used in direct connection with the vehicle manufacturer and the reseller.

InternetInTheCar.Vodafone. This is a Dutch eSIM of the provider Vodafone. This eSIM activated by Vodafone Germany. The activation took place personally with presentation of the identity card in a branch office of the provider; Resellers are not allowed to activate this service.

5. FINDING AND ANALYSIS

In this section we discuss the results extracted from our case study as noted in previous section.

5.1 Collecting the IMSI / IMEI

IMSI/IMEI was recorded in areas protected against radiation from other sources. It was found that the Mercedes-Benz E-Class has only one IMSI and transmits via an antenna in the rear window. The built-in Wi-Fi module connects as soon as the ignition of the vehicle is activated. By default, the Wi-Fi module is activated use for Internet communication with other devices are possible.

Communication between the remote application and the vehicle may take place after activation by the dealer from whom the vehicle was purchased. Telemetry data is transmitted by the user without further activation. The infotainment/navigation system update is linked to an optional contract. Through these systems, the area of the live traffic is processed, which permanently updates traffic mediation, determined position and calculates optimal routes. With the vehicle having a TomTom navigation system installed, the open access

from the vehicle DNS server to the TomTom Server could not be detected.

The installed eSIM in this vehicle can implement the standards GSM (2G) and UMTS (3G) and tries to log in to the networks of Telekom Germany, Vodafone and O2 respectively, i.e. the existing IMSI has no network lock and may be used as required register all networks available in Germany. These dial-up attempts are started as soon as the vehicle door is unlocked, further interaction is not required. A data traffic was interrupted with locked vehicle: this is probably due to the lack of power flow, as upon unlocking the closing mechanism direct contact to the DNS server *recursive.ns247.net* and thereby contacted to other servers and existing data. This shows that remote access to the vehicle, with locked security mechanisms, is not possible.

5.2 Export from the telecommunications system

Data within the telecommunication monitoring system is assigned to an IMSI or IMEI. Each connection setup by means of GPRS is assigned to it data packets. We also noted that the monitored device is recognized by the user-agent being used. The user-agent is characterized by the fact that it represents the operating system used, the browser and the IT device used.

Besides, due to the non-existent MAC address of the individual device, data assignment based on the packet data becomes impossible. This MAC address is only used for the internal connection (User Equipment - Router on the DSL). Since the information is collected at the data output of the provider, these are not available. Therefore, it is absolutely necessary to store the entire telecommunications traffic, otherwise the connection to the used IMSI / IMEI will be lost.

Another storage issue with the existing IMSI / IMEI is that they can be cloned or assigned multiple times. It is not uncommon today that in an area where cheap phones exist, an IMEI is awarded multiple times, because the responsibility lies with the device manufacturer. It is also possible to clone an IMSI with little effort, but multiple entries in a base transceiver station are not possible.

A switch within the used IPv4 can host several 100 users. In the telecommunications records two IPv4 are stored, both are internal IPs. On the one hand an IP for the client itself, which in this case is in the IP range 10.XX.XX.XX and on the other hand the network identifier, which is located here in the range 192.168.XX.XX. Data that is not sent by the user-agent, does not leave any usable traces of equipment that can be directly assigned to the device in the network packets routed through the provider.

5.3 Monitoring Wi-Fi module

The Wi-Fi module was monitored during a highway journey of 07:59:25 and 12:42:24 by means of the command airodump-ng and existing data packets were recorded. The aim of this surveillance was to compare findings from the monitoring of stationary access points with this Wi-Fi hotspot to detect any investigation approaches and to continue to obtain an estimate of wireless networks during a motorway journey, as the number of stationary access points is relatively small. In the higher-level evaluation of the traffic on this interface, the following findings emerged (Table 1).

The hotspot acts with a BSSID, which indicates by default the vehicle brand, the intended use and a consecutive number. Because Wi-Fi is switched on by default in the vehicle, it can detect and monitor from a greater distance (more than 1000m depending on the antenna module and environment). A data reception is eliminated at greater distance, here we can from a maximum distance of about 200m.

Table 1. Wi-Fi- statistics - *mb_lang-hin.pcapng*

Description	Value
BSSID	9e:8d:7c:51:99:9c
Channel	5
SSID	MB Hotspot 38724
Percentage of packages	66.994378
Percentage repetitions	11.915921
Repetitions	5822
Beacons	40128
Data packets	190
Probe requests	0
Probe response	8462
Auths	2
Dauths	44
Further	33
Protection	Unknown

The channel used remained the same throughout the trial period, this is likely to be attributed to the fact that the bulk of the existing AP has channels 1,6,13 as the default and the company wanted to achieve a channel with as little access as possible to other access points for interference-free transmission.

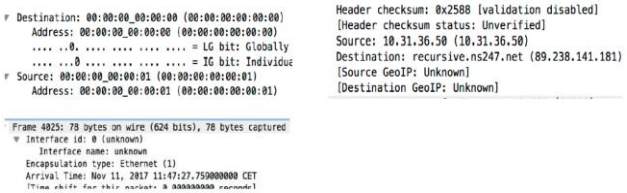
The number of beacons appears extremely high over a period of 4 hours, the test with an AVM router was about 1500 beacons per hour, a test with a VW T5 delivered 14000 beacons within one hour. Depending on the current state of knowledge, the transmission of the beacons is speed-dependent, the faster the vehicle was moved, the more beacons were sent.

The collected test responses show the high number of wireless network modules that can be found on motorways today and the associated possibilities and risks this poses for security authorities. Of course, observation and surveillance missions are possible, so that it would be possible to build up distance to the target without losing sight of it. Conversely security also poses a threat to security agencies. Units have Wi-Fi routers, hotspots, laptops and smartphones and can easily identify to their counterparts. A frame analysis using Wireshark showed that the communication was completely handled in the 2.4 GHz range. This seemed surprising at first glance, as the 2.4 GHz frequency band is being used by several other networks (e.g. Bluetooth). Reasons for the restriction to this Wi-Fi frequency range could be initial costs, the lower energy output (max 100mW) and the compatibility with older devices.

5.4 Information content of the network packets

With regard to the information provided in the network packets, it should be noted that there are major differences to normal packet captures. Entries are blank and aggravate or prevent automatic analysis of data packets. Especially in the field of network communication, this represents a barely surmountable data mountain. Within Wireshark, for example, there were no signs of RTP streams, they could not be captured by the existing analyses tools.

Analyzing path and looking at a connection



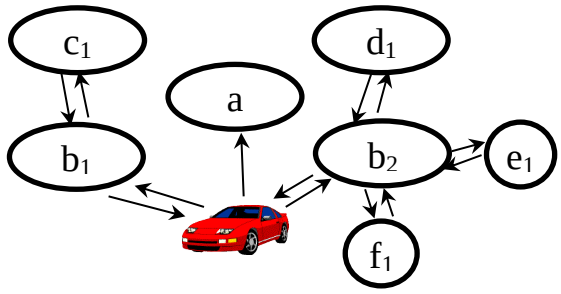
frame by using Dshell for (IP 10.31.26.50 -> IP 89.238.141.181) we can have the results as in Figure 2. We also noted that GeoIPs are missing. A device detection to connect the data packets with devices and close the evidence chain cannot be done. This also applies to the actually existing wireless traffic, which cannot be implemented as such due to missing frame contents.

Figure 2. Dshell analyzing of network packets

Because the MAC signature is not transmitted, this is the only known way to preserve the MAC of the network module. Since these are not available within the network communication of the data stream, a stream analysis within the network packets is not possible.

5.5 Insights into servers and impacts

In this topic communication lines in the areas of telemetry, InternetInTheCar and smartphone application were shown. It is an eSIM UMTS module with the IMSI of the Dutch provider Vodafone Libertel.



Legend:

a = recursive.ns247.net 89.238.141.181
b1= recursive.ns247.net 89.238.141.181
b2= recursive.ns247.net 89.238.161.35
c1= Hermes-if.dvb.corpinter.net 195.243.210.46
d1= Ssl-proxy-r55.dvb.corpinter.net 80.156.239.107
e1= Cep-ssl-win.dvb.corpinter.net 80.154.131.251
f1= Subs.snap.dvb.corpinter.net 80.154.131.207
Abnormalities within the connection
a= A one-off knock-on request; no response from the server
b1= Represents the main DNS platform that connects to servers d1, e1, and f1
b2= Connects to server c1; File contents of servers b1 and b2 are identical

Figure 3. Connection within the IP data network

Both IMEI and IMSI were not available at the vehicle branch upon request. This IMSI establishes its communication via an MSISDN with the country calling code +882 39, which belongs to Vodafone Malta and represents a catch-all for telephone services and is not dedicated to a single country.

In the field of telemetry, data transmission and communication are only possible within the German territory. Only the DNS server is operated by M247 in England. This is probably due to the fact that they are working with Vodafone UK and provide their services on this network. This would be the only server within the telemetry data communication outside of the scope of German law but currently subordinate to European law.

The integrated systems show that the (Figure 3) providers of telecommunications services are broadening their scope of activities and making their expertise available to car manufacturers. From participating servers, it can be assumed that the integrated systems of Deutsche Telekom AG: *hermes1-if.dvb.corpinter.net, cep-ssl-win.dvb.corpinter.net, vehicle-if.dvb.corpinter.net, ssl-proxy-r55.dvb.corpinter.net* and *subs.snap.dvb. .corpinter.net* save this data at least temporarily.

The cooperation between Mercedes-Benz and Telekom is also reflected in the fact that only two areas, belonging to the parent company Daimler, are fully integrated into this network structure.

Surprisingly, the eSIM Vodafone can be assigned outside the structure of Mercedes-Benz / Telekom. At the beginning of the investigation preparation, the question arises as to what extent Vodafone Libertel Netherlands would be involved in the data flow. The promising, yet globally, expected answer was "Not at all." The Internet Service Provider (ISP) is Vodafone US, which also receives all requests from the client. The Autonomous System (AS) belongs to Vodafone Italia, where the answers come back to the client. The AS is reported in Germany, Frankfurt / Main, presumably as a result of the eSIM being activated in Germany.

The MeConnect application from Mercedes-Benz is divided into its communication behavior. While the application within the server structure of the Deutsche Telekom AG has its information base, presumably due to the impact on facilities (such as auxiliary heating) and safety devices (such as locking system). The MeAccount has been connected to the Daimler network, as well as the Places and Production

Suite areas, which will guide him / her through Akamai Technologies.

5.6 Further discussion

The use of an IMSI catcher was chosen to capture the complete communication of the vehicle. Conducting monitoring by logging onto existing Wi-Fi would not have the desired outcome, because only the communication for the connected devices would have been detected.

By discharging directly from the provider Vodafone all transmitted data of the SIM card could be extended. These showed new problems in their evidential value and meaningfulness. By recognizing this problem, legal and technological measures can be taken by the legislator in cooperation with the provider and the Federal Network Agency.

Monitoring of the Wi-Fi module has shown that a large number of Wi-Fi beacons can be used in the field of reconnaissance and observation missions in the security regulatory environment.

Intrusion from outside by crackers of the password can be ruled out due to the length and variability (14 characters, Upper, Lower, Digit). However, it is also possible to create an Evil Twin and use it [12].

Finally, the localization of the server structure and the global use of individual country resources of a provider were discussed. Here we can still see approaches to receiving data that were not stored within Germany, but as in this case, a phone number. The provider recognized by the IMSI also had no influence or reference to communication processes and several globally branched distributions of the provider and their tasks within the service order InternetInthecar could be recognized.

6. CONCLUSION AND FUTURE WORK

The objective of this paper was to examine how data is generated by a car or routed through the car's network gateway. Knowledge of this data flow and its intermediate and final storage locations enables the security authorities to use it in preliminary investigations and to assess the risks of vehicle/technology use in their own operational procedures. Data of a vehicle were collected for this paper. This applies to both telemetry and remote application data, as well as the interconnection data of the mobile service provider. The vehicle data was analyzed and disseminated using various procedures / programs to provide a basis for assessing Internet of Things Mobility infrastructures. This paper has shown that contents and communication endpoints can be identified and further analysis approaches can be made, and under certain circumstances access and localization of the vehicle is possible. This also shows opportunities as well as risks which security authorities can have in dealing with the networked mobile areas of the Inter of Things [17]. In addition, a one-sided processing or forensic analysis will provide less and less useful information, only the way of holistic consideration will contribute to the investigation of criminal offenses or to the protection of one's own forces in the future. Several times during the paper it was shown that the generated data throughput leads to the use of the vehicle, the devices connected to the Wi-Fi or the smartphone application.

In terms of future work, in order to get a strong accentuated picture here, a fragmented data analysis for different vehicle manufacturers / groups should be conducted to evaluate them in context. Furthermore, consideration of the various domestic and foreign mobile service providers in this area would be an important consideration. In addition to the actual data

flow, the area of data (intermediate) storage would be of decisive importance here.

REFERENCES

Fleet Management System Using Novel GPS/GLONASS Tracker and Web-Based Software. 1st International Conference on New Research Achievements in Electrical and Computer Engineering (ICNRAECE), Teheran, Iran, May 2016.

How hackable is your car, Wired.com, August 6 2014, Andy Greenberg, retrieved online from https://www.wired.com/2014/08/car-hacking-chart/ on November 2018.

Berla.co https://berla.co

S. Checkowa et al. (2011), Comprehensive Experimental Analyses of Automotive Attack Surfaces, Retrieved online from http://www.autosec.org/pubs/cars-usenixsec2011 on August 2018

Miller and Valasek (2015), Remote Exploitation of an Unaltered Passenger Vehicle, IOActive, retrieved online from http://www.ioactive.com/pdfs/ IOActive _Remote_Car_Hacking.pdf on August 2018

BMW Connected Drive, BMW website, (2013), Retrieved online from http://www.bmw.com/com/ en/insights/technology/connecteddrive/2013/index. html on August 2018

My Car My Data, FIA, (2015), Retrieved from http://www.fiaregion1.com/download/mycarmydata/ covering_text_for_technical_study_final.pdf on August 2018

Briefing Note e-call, Big Brother Watch, (2014), retrieved online from https://www.bigbrotherwatch .org.uk/wp-content/ uploads/2014/07/Briefing-Note-eCall-PDF.pdf on August 2018

D. Tobin (2014), Officer are you tracking me?, The Sunday Times, January 26 2014, retrieved online from http://www.thesundaytimes.co.uk/sto/ingear/cars/article1366310.ece on August 2018

J. Daniel, et al. (2017). Volkswagen Car Entertainment System Forensics. In Proceedings of IEEE TrustCom/BigDataSE/ICESS 2017, pp. 699-70, Sydney, Australia, August 2017

N-A. Le-Khac et al. (2018). Smart vehicle forensics: Challenges and case study. Future Generation Computer Systems, June 2018, https://doi.org/10.1016/j.future.2018.05.081

Elektronikompendium,https://www.searchsecurity.de/definition/Evil-Twin-Boeser-Zwilling, 2018

https://www.kitploit.com/2018/07/devploit-v36-information-gathering-tool.html

A. Goudbeek et al. (2018), A Forensic Investigation Framework for Smart Home Environment, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18), New York, USA, August 2018, DOI: https://doi.org/10.1109/TrustCom/BigDataSE.2018.00201

L. Chen, H. Takabi, N-A. Le-Khac (Eds.) (2019) “Security, Privacy, and Digital Forensics in the Cloud”, High Education Press, Wiley Inc., April 2019, DOI: https://doi.org/10.1002/9781119053385

Miriam Cabo et al. (2014). Universal access to eCall system, 5th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting

Info-exclusion, Elsevier Procedia Computer Science 27 (2014) pp. 104-112

S. Alabdulsalam, et al. (2018) Internet of Things Forensics: Challenges and Case Study, In: Gilbert, Peterson; Shenoi Sujeet (Eds.). Advances in Digital Forensics XIV. New York: Springer Berlin Heidelberg. DOI: https://doi.org/10.1007/978-3-319-99277-8_3

