Tracking of Vehicles by Almost Everyone

Markus Ullmann* † Gerd Nolden,* and Timo Hoss*
* Federal Office for Information Security
D-53133 Bonn, Germany
Email: {markus.ullmann, gerd.nolden, timo.hoss}@bsi.bund.de
† University of Applied Sciences Bonn-Rhine-Sieg
Institute for Security Research
D-53757 Sankt Augustin, Germany
Email: markus.ullmann@h-brs.de

***Abstract*—Increasingly, vehicles will be equipped with information and communication technologies, e.g., wireless communication technologies like IEEE 802.11x, Bluetooth, mobile communication, etc. These communication technologies enable identification and tracking based on identifiers used in communication protocols. Today, the Vehicle Identification Number, and the license plate are regarded as vehicle identifiers. With new communication technologies used in modern vehicles, Secondary Vehicle Identifiers are coming up. This paper analyzes the identification of vehicles based on wireless communication interfaces and presents results of real measurements of vehicular Bluetooth and Wi-Fi interfaces. Moreover, countermeasures are introduced, which reduce the risk of being trackable.**

Keywords*–*Vehicle Identification; Vehicle Identifier; Wireless Vehicle Interfaces; Privacy; Vehicle Tracking

I. Introduction

Information technology in vehicles has significantly changed during the last 10 years. This is shown by the increasing availability of components for driving assistance: lane keeping support, traffic jam assist, automatic parking assistant, remote parking assistant and so on. This development is a prestage of automatic driving, which is one of the main challenges in automotive engineering at the moment. Besides driving assistance, modern vehicles are equipped with wireless interfaces, e.g., Bluetooth to connect devices (smart phones, tablets, etc.) to the multimedia component (head-unit) of the vehicle. In addition, head-units are more and more capable of establishing a Wi-Fi hot spot to support Internet access for vehicle passengers. Furthermore, the vehicle-2-vehicle communication technology (V2V) based on IEEE 802.11p technology will be deployed in the near future. V2V is one feature of Intelligent Transport Systems (ITS).

Today, only the Vehicle Identification Number (VIN), and the license plate are regarded and used as official vehicle identifiers. This paper analyses vehicle identification capabilities of wireless communication interfaces, called Secondary Vehicle Identifiers, which can be used for vehicle identification and tracking. This issue was first published in [1]. Next, results of further measurements of vehicular Bluetooth interfaces and vehicular Wi-Fi hotspots are presented. The communication interfaces are built into the vehicle to support communication services for passengers. We show, however that these services are also available outside the vehicle and can be misused for unauthorized identification and tracking. We only use cheap measurement equipment, e.g., external Bluetooth USB-Sticks (they cost only a few €) and partially open source tools (software components of the Kali Linux distribution for penetration testing), which are publicly available. The smart phone measurement apps applied can be used by everyone with every modern Android compatible device for the identification of vehicles based on Bluetooth. The aim of this paper is to highlight the issue of identification and tracking of vehicles based on Secondary Vehicle Identifiers. Therefore, we have only investigated selected vehicles instead of performing a study with lots of vehicles. Most of the measurements were already performed in November 2016. The Bluetooth tests presented in Section VI-B were conducted in August 2018.

We primarily investigated simple measurements of existing static Secondary Vehicle Identifier, e.g., static MAC IDs. We know that there exist further device identification capabilities as shown in [2] for Wi-Fi components, which we do not study, here. In comparison, we only propose simple countermeasures which avoid an easy tracking of vehicles.

The subsequent sections of this paper are organized as follows: Section II is a description of related work. Subsequently, identifiers for ITS vehicle stations are presented in Section III. Section IV describes wireless technologies implemented in modern vehicles and analyzes identification capabilities. The aim of the tests performed, test equipment used and test vehicles investigated are presented in Section V. Results of real measurements of Bluetooth and Wi-Fi identifier are given in Section VI. In Section VII, the problem of vehicular tracking is addressed. Section VIII depicts only simple countermeasures to avoid an easy tracking of vehicles. Finally, we summarize our results, and mention open research questions.

II. Related Work

A classification of vehicle identifiers which is also applied in this paper is given in [3]. Hwajeng et al. suggested a vehicle identification and tracking system based on optical vehicle plate number recognition [4]. Tracking of devices based on Bluetooth interfaces is already discussed for a lot of applications, e.g., indoor localization [5] or wireless indoor tracking [6]. In [7], an analysis in Jacksonville, Florida, to capture vehicle traffic streams is described. To this end, a set of Bluetooth receivers were installed at the roadside on specific streets to capture the Bluetooth MAC ID (BD_ADDR) of vehicles passing. A quite similar application is still performed in Bonn to analyse and detect mobility pattern of vehicles based on a network of stationary road side Bluetooth sensors [8].

Besides Bluetooth, IEEE 802.11 compliant devices were suggested for real-time location tracking in indoor and outdoor environments [9].

Since November 1st, 2014, vehicles and motorhomes have to be equipped with a Tire Pressure Monitoring System (TPMS) within Europe. These can be subdivided into direct and indirect TPMS. Direct TPMS means that specific physical sensors measure the air pressure of the tires. These sensors communicate wirelessly with the vehicle and transmit an identifier of 28 to 32 bit length. There are different wireless technologies available for 125 kHz, 315 kHz, and 433 MHz. A detection range of up to 40 m for direct TPMS is mentioned in [10].

Apart from the identification of vehicles based on static identifiers used in communication protocols different feature based identification methods are proposed. One approach is the identification of vehicles based on noise features (individual noise spectrum) [11].

Further identification techniques allow wireless devices to be identified by unique characteristics of their analog (radio) circuitry; this type of identification is also referred to as physical-layer device identification. It is possible due to hardware imperfections in the analog circuitry of transmitters introduced during the manufacturing process. A good overview concerning the physical fingerprinting of different wireless communication technologies is given in [12]. The discussion of device tracking based on static identifier of wireless communication interfaces started 15 years ago [13].

In [14], the privacy principles of Bluetooth low energy (BLE) are described and analyzed. It is shown that the privacy mechanisms in BLE are only applicable in connection mode but not during advertising. Moreover, privacy enhancements for advertising are proposed. BLE is widely applied for the connection of fitness trackers to smart phones. Though privacy is an important issue [15] shows that most of the analyzed devices do not implement the privacy mechanisms of the standard or, if they do, implement them in a wrong manner.

Mathy Vanhoef [2] et al. highlight the general difficulty of implementing anti-tracking solution for wireless devices. In particular, they analyzed proprietary Wi-Fi MAC randomization algorithms implemented in iOS (starting from iOS 8), Android (starting from Android 6.0), Linux (starting from Kernel 3.18) and Windows 10. They analyzed that probe requests included in their frame body under the form of Information Elements (IEs), also called tagged parameters, or tags (e.g., ordered lists of tag numbers, extended capabilities, etc.) can be misused for tracking. Besides that sequential frame numbers or predictable scrambling seeds can be used for device identification and device tracking [2].

III. ITS Vehicle Identifier

In this paper, we categorize the available identifiers of vehicles into two classes. Primary vehicle identifiers represent those identifiers which will be typically considered today, e.g., the Vehicle Identification Number (VIN). Secondary Vehicle Identifiers come up with new information technology used in modern vehicles.

A. *Primary Vehicle Identifier*

To date, every vehicle is identifiable based on its unique VIN. In some areas, the VIN is integrated as human readable information in the windscreen of vehicles.

Besides the VIN, vehicles are marked with a license plate, which is already used for identification.

With the deployment of V2V technology vehicles will be equipped with a long term ECC key pair and an appropriate certificate [16] [17]. This certificate will become an additional primary vehicle identifier in future.

B. *Secondary Vehicle Identifier*

Modern vehicles are equipped with multi-media components (head-unit), which are able to establish communications with electronic devices of drivers or passengers. Typically, wireless communication technologies, e.g., Bluetooth, are used for that purpose.

A Bluetooth multi-media device emits a static 48 bit Media Access Control address, named MAC ID. The MAC ID is composed of two parts: the first half is assigned to the manufacturer of the device, and the second half is assigned to the specific device. In addition, each Bluetooth device emits a “User-friendly-name” which is typically alterable. Bluetooth devices operate in the ISM band (2.4 to 2.485 GHz).

Moreover, vehicle head-units allow any Wi-Fi ready laptop, tablet or mobile phone to access the internet within the vehicle while travelling if the head-unit has mobile communication capabilities. But head-units configured as access points need a unique Service Set Identifier (SSID) or network name to connect devices. In addition, each head-unit needs a unique MAC address.

If vehicles are equipped with mobile communication capabilities an International Mobile Subscriber Identity (IMSI) is required. This is a unique ID to identify a mobile device within the network. In addition, a SIM card with a dedicated mobile phone number is needed for mobile communication.

In [12], physical fingerprinting of wireless transmitters is investigated. Here, a complete feature set for physical fingerprinting of a transmitter is a secondary vehicle identifier. Vehicle identifiers mentioned so far are sufficient for identification all the time. Furthermore, vehicle identifiers with a limited validity period, e.g., pseudonymous certificates (termed authorization tickets by ETSI) exist. Pseudonymous certificates come up with the V2V technology.

Initially, Secondary Vehicle Identifier have no formal character in contrast to a license plate or VIN. But it is technically very easy to capture Bluetooth and Wi-Fi identifiers of a vehicle as shown in Section VI. So, attackers can misuse them for their purposes.

IV. Wireless Technologies

In this section, wireless technologies, which are applied in vehicles are described. In addition an analysis concerning identification capabilities based on wireless communication technologies is given. We only address local wireless communication technologies, which are quite easy to detect and omit mobile communications according the Global System for Mobile Communications (GSM) or the Long Term Evolution (LTE).

A. Bluetooth

Bluetooth is specified by the Bluetooth special interest group. The information mentioned here is based on the Bluetooth Specification version 5.0 [18].

The concept behind Bluetooth is to provide a universal short-range wireless communication capability using the 2.4 GHz Industrial Scientific Medicine (ISM) bands, available globally for unlicensed low-power uses.

There are two forms of Bluetooth wireless technology systems: Bluetooth Basic Rate (BR) and Bluetooth Low Energy (BLE). During our measurements we detected only Bluetooth (BR) compliant devices in the head-sets of the vehicles investigated.

Both systems include device discovery, connection establishment and connection mechanisms. The Basic Rate system includes optional Enhanced Data Rate (EDR), Alternate Media Access Control (MAC) and Physical (PHY) layer extensions. The Basic Rate system offers synchronous and asynchronous connections with data rates of 721.2 kb/s for Basic Rate, 2.1 Mb/s for Enhanced Data Rate and high speed operation up to 54 Mb/s with the 802.11 AMP. The BLE system includes features designed to enable products that require lower power consumption, lower complexity and lower cost than BR/EDR. The BLE system is also designed for use cases and applications with lower data rates and has lower duty cycles.

1) Bluetooth (BR) Technology: Bluetooth provides support for three application areas using short-range wireless connectivity:

- Data and voice access points: Bluetooth facilitates real-time voice and data transmissions by providing effortless wireless connection of portable and stationary communications devices
- Cable replacement: Bluetooth eliminates the need for numerous, often proprietary cable attachments for connection of practically any kind of communication devices. The range of each radio depends on the output power (up to 100 m)
- Ad hoc networking: A device equipped with a Bluetooth radio can establish an instant connection to another Bluetooth radio as soon as it comes into range

In vehicles, Bluetooth is used for connecting a smart phone to the:

- Hands-free phone system
- Vehicular head-unit to use the loudspeaker of the head-unit to output music from the smart phone

The Bluetooth architecture is divided into different layers. It starts with the Radio Frequency (RF) Layer, also termed physical layer (PHY). To be resilient to disturbances a frequency hopping spread spectrum (FHSS) is used. Three classes of transceivers are available with different output power. Power class 1: 100 mW, power class 2: 2,5 mW and power class 3: 1 mW.

Bluetooth (BR) uses 79 frequency channels, spaced 1 MHz apart. Channel n uses (where n is in the range 0 - 78) a carrier frequency of 2402+n MHz. Each frequency channel is divided into 1600 time slots per second; each slot is 625 μs long. Each data packet may use between 1 and 5 slots and is transmitted on a different frequency channel, following a pseudo-random hopping sequence determined by the device address of the master device.

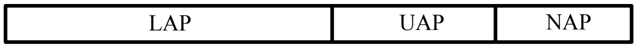


Figure 1. Structure of a Bluetooth Device Address

At first, Bluetooth devices have to establish a connection, termed pairing, to exchange data. This procedure is initiated by the host device based on the inquiry process. During this process Bluetooth devices respond with inquiry reply messages including BD_ADDR and clock rate (CLK), etc. During the pairing process the jump sequence for sharing the channels is calculated by the master device and synchronized with the slave devices.

There exists a range of Bluetooth Specification versions from Bluetooth 1.0a (published 1999) to Bluetooth 5.0 (published 2016).

2) Identification Capabilities: A Bluetooth multi-media device emits a static 48 bit MAC identifier (BD_ADDR). The MAC ID is composed of three parts: Lower Address Part (LAP), Upper Address Part (UAP), and Nonsignificant Address Part (NAP). NAP (16 bit) and UAP (8 bit) are assigned to the manufacturer of the device, and LAP (24 bit) is assigned to the specific device.

In addition, each Bluetooth device emits a "User-friendly-name" which is typically alterable. BD_ADDR and the "User-friendly-name" are the primary identifiers. In addition, the data set of a Bluetooth device: CLK, Bluetooth device profile, and the Host Controller Interface (HCI) can be used for identification purposes (Table I), too.

3) Bluetooth Low Energy: BLE is a low-power wireless technology for short-range control and monitoring applications. It operates in the 2.4 GHz ISM band as well. It uses 40 radio channels. 3 channels are primarily used for advertising. For BLE only one packet format is specified in the link layer. It consists of:
Preamble | Access Code | PDU | CRC.
The access code includes the 48 bit device address.

There are only two PDU formats in BLE, one for advertising packets and one for data packets.

The standard distinguishes between public and random device addresses. A public and a random device address are both 48 bits in length. To avoid tracking of a device, random device addresses should be used. But random device addresses can only be applied for data packets in a connection mode not for advertising packets.

The random device address may belong to either of the following two sub-types:

- Static address
- Private address

The term "Static address" means that the device initializes its static address to a new value after each power cycle. Private addresses are changed during operation at a fixed frequency.

As long as the Bluetooth device is not powered down and up, the static address has not changed and sniffed bluetooth advertising packets of one Bluetooth device can be linked. For privacy reasons private random addresses should thus be used.

hash(IRK, prand)	prand	1	0

Figure 2. Structure of a resolvable private Bluetooth device address

A private address may belong to either of the following two sub-types:

- Non-resolvable private address
- Resolvable private address

Resolvable private addresses have the positive side effect that already connected devices can be identified later on though the device address has changed in the meantime. Therefore, a specific device, namely, Identity Resolving Key IRK is needed, which is transmitted from the Bluetooth device to the Bluetooth component in the vehicle after a first paring procedure. The IRK is linked to an identity at the Bluetooth host. Figure 2 depicts the structure of a 48 bit resolvable private Bluetooth address. It consists of three different parts:

- bit mask '10' indicating a random resolvable private address
- 22 bit random value *prand* and
- 24 bit hash value $hash(IRK, prand)$

If a Bluetooth host receives a data packet with resolvable private address it calculates for all known IRK_i $hash'(IRK_i, prand)$ and compares this value with the current value of $hash(IRK, prand)$.

$$hash'(IRK_i, prand) \overset{?}{=} hash(IRK, prand) \qquad (1)$$

If this equation holds for one IKS the component is identified and pairing can again be established.

B. Wireless Local Area Network (Wi-Fi)

Primary, Wi-Fi is based on the communication standards which was made for cable based Local Area Networks (LAN), IEEE 802.11x.

1) Technology: Briefly spoken, Wi-Fi devices support two different modes:

- Ad hoc mode, termed independent BSS (IBSS): Wi-Fi devices communicate peer-to-peer. During the communication data pakets are sent to all devices of the network but discarded by the devices if the destination address does not fit
- Access point mode, termed Basic Service Set (BSS): All Wi-Fi devices are connected with the access point (hot spot)

Head-units of modern vehicles provide Wi-Fi hot spots. So any Wi-Fi ready laptop, tablet or mobile phone is able to access the internet within the vehicle while travelling if the head-unit has mobile communication facilities (GSM, LTE).

Different Wi-Fi Standards exist: IEEE 802.11b / g / a / n / ac. They differ in the frequency band used (2,4 GHz and/or 5 GHz), and communication speed (1 Mbit/s . . . 6,96 Gbit/s). The frequency band is split into channels (2,4 GHz: 13 channels with a bandwidth of 20 or 40 MHz, hence 5 channels are needed to establish a network). In the 5 GHz Wi-Fi frequency band channels have a bandwidth of 20, 40, 80 or 160 MHz.

TABLE I. TECHNOLOGY SPECIFIC IDENTIFICATION FEATURES

Technology	First Level Features	Second Level Features
Bluetooth	MAC ID (BD_ADDR) "friendly name"	CLK, Bluetooth device profil Host Controller Interface
IEEE 802.11 X (Wi-Fi)	MAC ID (BSSID) "SSID"	Information in Beacon Frames

One type of the management frames in IEEE 802.11 based Wi-Fis is a beacon frame. Beacon frames are transmitted periodically to announce the presence of a wireless LAN and contain information about the network. Beacon frames are transmitted by the access point in an infrastructure Basic Service Set (BSS). In IBSS networks beacon generation is distributed among the stations.

2) Identification Capabilities: Primary identifiers are:

- Basic Service Set ID (BSSID) or MAC address of the Wi-Fi device and
- SSID (primary name associated with an 802.11 wireless local area network with a maximum length of 32 characters)

In addition, information in Wi-Fi beacon frames could be used for identification, too (Table I).

3) Random Device Address: A common specification on Wi-Fi MAC address randomization does not yet exist. However, proprietary Wi-Fi MAC randomization algorithms are implemented in iOS (starting from iOS 8), Android (starting from Android 6.0), Linux (starting from Kernel 3.18) and Windows 10. Unfortunately, these mechanisms are only available if the Wi-Fi card and driver support it.

V. MEASUREMENTS

In this section, the test cases performed and the test equipment used are described.

A. Aim of the Measurements

By means of the measurements, we investigate vehicular Bluetooth as well as Wi-Fi communication capabilities especially for identification purposes outside the vehicle. Therefore, the following measurements, divided into test cases, are performed:

- Test case 1: Radiation characteristics
- Test case 2: Signal strength
- Test case 3: Activity of the transmitter
- Test case 4: Detection of Secondary Vehicle Identifier in stand still mode of the vehicle
- Test case 5: Detection of Secondary Vehicle Identifier in driving mode of the vehicle

B. Test Vehicles

The following vehicles were investigated during the measurements:

- Skoda Octavia III (two different models equipped with Bluetooth chips from Qisda Corporation or Alps Electronics Co. LTD are investigated): Only used for Bluetooth measurements
- VW Passat B8: Only used for Bluetooth measurements

- Opel Astra 2016 incl. OnStar: Only used for Wi-Fi measurements
- Opel Insignia Innovation 2016 incl. OnStar: Only used for Wi-Fi measurements

C. *Test Equipment*

1) Bluetooth Test Equipment for the Tests in Section VI-A:

- Notebook
    - ThinkPad X201 with Kali Linux (64 Bit, version 2016.2), BTScanner version 2.0, and Kismet version 2016-07-R1
    - Ubertooth One (firmware git-579f25) with Ubertooth-Specan-Ui, and Ubertooth-Rx version 201-10-R1 [19]
    - Standard antenna, LogPer antenna, and directional antenna WIFI-LINK WAVEGUIDE Antenna PN: WCA-2450-12, frequency range 2,4 - 2,5 GHz, 12 dBi
- Smart phone
    - Samsung Galaxy S6, Android 6.0.1, Bluetooth-Scanner app version 1.1.3 (from Google Play-store)

2) Bluetooth Test Equipment for the Tests in Section VI-B:

- Notebook
    - Lenovo ThinkPad T400 with Kali Linux (64 Bit, version 2018.2), BTScanner version 2.1-6
    - Ubertooth One (firmware-version: 2018-06-R1, API 1.03) with Ubertooth-Specan-Ui, and Ubertooth-Rx [19] and the following antennas are used: standard antenna, Ettus VERT2450 antenna, and WIFI-LINK WAVEGUIDE antenna PN: WCA-2450-12, 2,4-2,5 GHz, 12 dBi
    - USB Bluetooth stick: AVM BlueFritz! USB v2.0
- Smart phone
    - Sony Smartphone Xperia Z5 Compact

3) Wi-Fi Test Equipment:

- Notebook
    - Notebook Lenovo ThinkPad T400, Ubuntu 16.04 LTS and LinSSID version 2.7
    - USB-Wi-Fi-device: TP-Link TL-WN722N with standard antenna and directional antenna WIFI-LINK WAVEGUIDE Antenna PN: WCA-2450-12, 2,4-2,5 GHz, 12 dBi
- Smart Phone
    - Huawei P8 lite 2017, Wifi-Analyzer App (from Google Playstore)
    - Samsung S7, Wifi-Analyzer App (from Google Playstore)

VI. Measurements and Results

In this section the test results of the performed tests are described. In Section VI-A an Octavia III head-unit with a Bluetooth chip of the Qisda Corporation is examined, whereas in Section VI-B an Octavia III head-unit with a Bluetooth chip of Alps Electronic Co. LTD is considered.

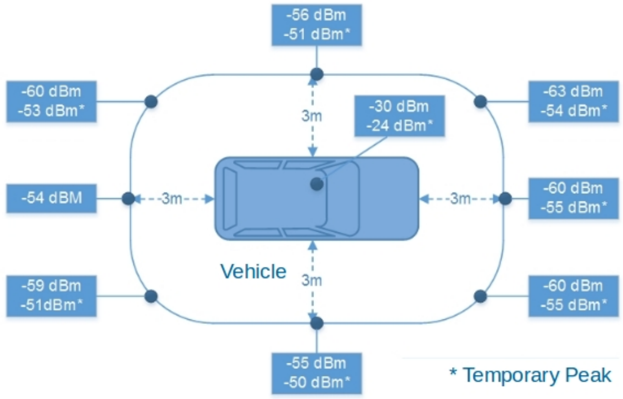


Figure 3. Radiation characteristic of the Octavia III Bluetooth device

TABLE II. SIGNAL STRENGTH OF THE OCTAVIA BLUETOOTH DEVICE

Distance	Standard Antenna	LogPer Antenna	Directional Antenna
3 m	-50 dBm	-56 dBm	-47 dBm
6 m	53 dBm	-60 dBm	-51 dBm
9 m	-63 dBm	-63 dBm	-54 dBm
12 m	-67 dBm	-65 dBm	-56 dBm
15 m	-71 dBm	-68 dBm	-60 dBm
18 m	-75 dBm	-69 dBm	-63 dBm
21 m	-78 dBm	-72 dBm	-65 dBm
30 m		-75 dBm	-68 dBm

A. *Bluetooth Measurements for the Octavia III equipped with a Bluetooth chip of the Qisda Corporation (and partly Passat)*

1) Test Case 1: As test equipment, a Lenovo ThinkPad X201, with Ubertooth One, Ubertooth-Specan-Ui and standard antenna is used. Measurements are performed at one position inside and 8 positions outside the vehicle. The positions and results are plotted in Figure 3. As we expected, the highest signal strength of -30 dBm has been detected inside the vehicle. But outside the vehicle, a strong signal strengh has also been measured.

2) Test Case 2: As test equipment a Lenovo ThinkPad X201, with Ubertooth One, Ubertooth-Specan-Ui and different antennas is used: Standard antenna, LogPer antenna and directional antenna WIFI-LINK WAVEGUIDE. The test results are presented in Table II. With all antennas the Bluetooth signal can always be detected, within a distance of 21 m.

3) Test Case 3: The Bluetooth module of the head-unit starts with scanning of Bluetooth devices which were already paired in the past and are registered in the pairing list of the head-unit after starting the ignition. Scanning is switched off after the deactivation of the ignition and removal of the key.

4) Test Case 4: First, a Samsung Galaxy S6 with the Bluetooth scanner app is utilised as test equipment. Figure 4 presents the test setting. The following information about the Bluetooth device of the head-unit can be captured with the test equipment mentioned:

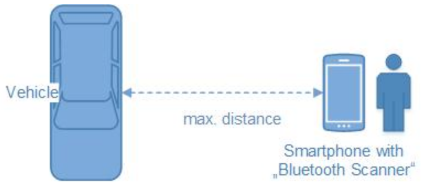


Figure 4. Test arrangement for the detection of Secondary Vehicle Identifier in stand still mode

Listing 1. BD_ADDR and "friendly name" of the head-unit of a Skoda Octavia

```
Skoda_TF
00:17:CA:D9:6B:77 (−65 dBm)
AUDIO_VIDEO_HANDSFREE
Scan Cycle 199 (20.11.16 15:01)
```

SSID “Skoda_TF”, BSSID “00:17:CA:D9:6B:77”, the service “AUDIO_VIDEO_HANDSFREE” and the “Scan Cycle 199 (20.11.16 15:01)” with date were captured. This information is readable up to a distance of 24 m (signal strength at this distance: -83 dBm) (it has to be mentioned that the owner of the Skoda Octavia III has already altered its SSID. “Skoda_TF” is not the factory setting).

The following information is captured from the Bluetooth device of the head-unit of the Passat up to a distance of 12 m (signal strength at this distance: -84 dBm):

Listing 2. BD_ADDR and "friendly name" of the head-unit of a VW Passat

```
VW BT 2058
A8:54:B2:FE:30:35 (−79 dBm)
AUDIO_VIDEO_HIFI_AUDIO
Scan Cycle 25 (02.11.16 13:15)
```

From a privacy perspective it is remarkable, that the name of the car manufacturer is part of the SSID and that the number part “2058” of the SSID is chosen from the VIN of the Passat.

Next, Lenovo ThinkPad X201, Ubertooth One with Ubertooth-Rx are used as test equipment to perform the same test case. The subsequent information can be captured if the test equipment is switched on and a Samsung Galaxy S6 is connected to the Octavia III head-unit:

Listing 3. Galaxy S6 connected to the Octavia head-unit

```
systime=1479652524 ch=39 LAP=d96b77 err=0
clkn=100728 clk_offset=1540 s=−35 n=−55 ...
systime=1479652571 ch=39 LAP=68dae3 err=0
clkn=250437 clk_offset=5596 s=−21 n=−55 ...
systime=1479652571 ch=39 LAP=68dae3 err=0
clkn=251217 clk_offset=5613 s=−16 n=−55 ...
```

This information can be captured up to 18 m with the standard antenna and up to 42 with the directional antenna.

5) Test Case 5: Using the test equipment Samsung Galaxy S6 with the Bluetooth scanner app, the subsequent information can be captured up to a speed of 30 km/h. Figure 5 shows the test case.

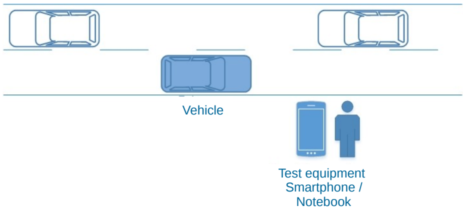
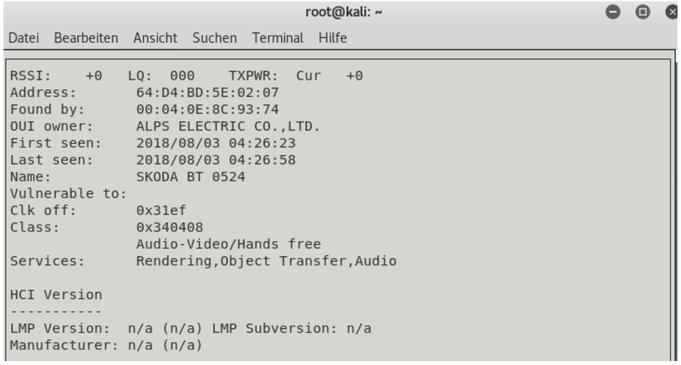


Figure 5. Test arrangement for the detection of secondary vehicle identifier in driving mode



```
RSSI:    +0   LQ:  000    TXPWR:  Cur   +0
Address:        64:D4:BD:5E:02:07
Found by:       00:04:0E:8C:93:74
OUI owner:      ALPS ELECTRIC CO.,LTD.
First seen:     2018/08/03 04:26:23
Last seen:      2018/08/03 04:26:58
Name:           SKODA BT 0524
Vulnerable to:
Clk off:        0x31ef
Class:          0x340408
                Audio-Video/Hands free
Services:       Rendering,Object Transfer,Audio

HCI Version
-----------
LMP Version:  n/a (n/a) LMP Subversion: n/a
Manufacturer: n/a (n/a)
```

Figure 6. Screenshot of the BTScanner during the measurement

Listing 4. SSID and BSSID in driving mode

```
Skoda_TF
00:17:CA:D9:6B:77 (−65 dBm)
AUDIO_VIDEO_HANDSFREE
Scan Cycle 199 (20.11.16 15:01)
```

B. Bluetooth Measurements for the Octavia III equipped with a Bluetooth chip of Alps Electronic Co. LTD

1) Test Case 4: As test equipment a Lenovo ThinkPad T400 with Kali Linux Version 2018.2, an USB Bluetooth stick AVM BlueFritz! USB 2.0 and a BTScanner version 2.1-6 were used to sniff information of the Bluetooth head-unit of the Octavia in stand still mode and with enabled ignition. Figure 6 presents the captured information. This information (BD_ADDR, “friendly name”) can be captured up to a distance of 67 m between vehicle and measurement device. The test arrangement is shown in Figure 4.

Next, the sniff distance of an existing Bluetooth communication between a paired smartphone (Sony Smartphone Xperia Z7 Compact) and the head-unit was investigated. As test equipment Lenovo ThinkPad T400 with Kali Linux Version 2018.2 and Ubertooth One with Ubertooth-Rx was applied. Table III presents the maximum detection distance with different antennas for a successful receiving of the BD_ADDR of the head-unit.

2) Test Case 5: Figure 5 depicts the test arrangement. As test equipment a Lenovo ThinkPad T400 with Kali Linux Version 2018.2, an USB Bluetooth stick AVM BlueFritz! USB 2.0 and BTScanner version 2.1-6 were used to detect the BD_ADDR of the head-unit of the Octavia III in driving mode.

TABLE III. DETECTION DISTANCE OF A PAIRED COMMUNICATION

Antenna	Detection Distance
Standard antenna	73 m
VERT2450	89 m
LogPer Antenna	112 m

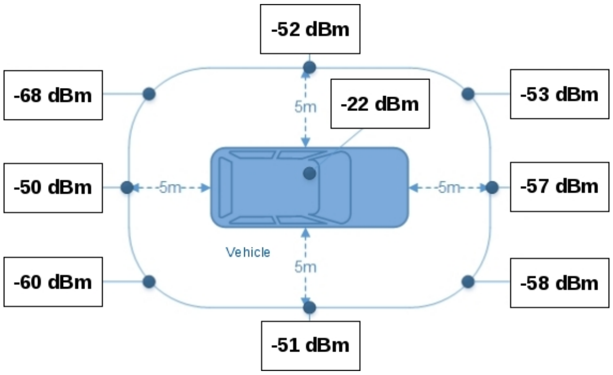


Figure 7. Radiation characteristic of the Opel Insignia Wi-Fi device

The test equipment was located at a distance of 10 m from the street to monitor the driving Octavia III. Up to a speed of 50 km/h we could identify the BD_ADDR of the head-unit. We stopped the investigation at this point. 50 km/h is the speed-limit inside cities in Europe.

C. Wi-Fi Measurements for the Opel Insignia (partly Opel Astra)

1) Test Case 1: As test equipment a Lenovo ThinkPad T400, TP-Link TL-WN722N with standard antenna, and LinSSID is used. The signal strength of the Wi-Fi access point (Wi-Fi-AP) has been measured at 8 fixed points outside and at 1 point inside the vehicle. The positions are equal to the Bluetooth test case. But in contrast to the Bluetooth measurement, the distance between the vehicle and the measurement tool is 5 m. The results for the Opel Insignia are plotted in Figure 7. As we expected, the highest signal strength of -22 dBm has been detected inside the vehicle. But outside the vehicle, a strong signal strengh has also been measured.

2) Test Case 2: As test equipment a Lenovo ThinkPad T400, TP-Link TL-WN722N with standard antenna, and LinSSID on the one hand and Samsung S7, and Wifi-Analyzer on the other hand are used. Using the TP-Link TL-WN722 and the Samsung S7 the signal strength is measured in increasing distance from the vehicle, in the direction of the right front door. The results are plotted in Figure 8. Only small differences in signal strength can be detected between an active connection and a non connection of a client to the Wi-Fi-AP of the Opel Insignia. The measurement sensitivity of the smart phone is about 10 dBm lower for distances greater 10 m in contrast to the measurements with the TP-Link. With both measurement devices the signal of the Wi-Fi-AP can always be detected, within a distance of 60 m.

3) Test Case 3: As test equipment a Lenovo ThinkPad T400, TP-Link TL-WN722N with standard antenna, and LinSSID is used.

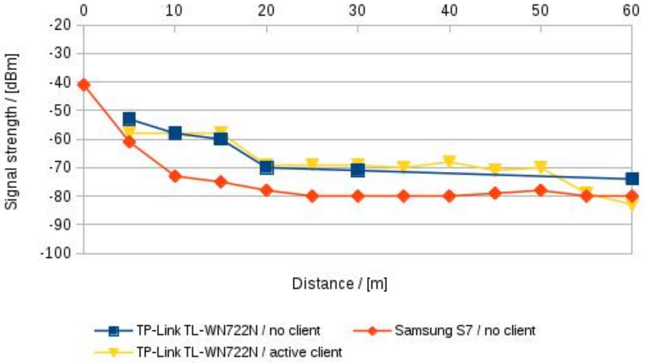


Figure 8. Radiation characteristic of the Opel Insignia Wi-Fi device

TABLE IV. SIGNAL STRENGTH OF THE ASTRA WI-FI DEVICE IN STAND STILL MODE

Distance	Signal strength Huawei P8 lite 2017	Signal strength TP-Link TL-WN722N
216 m	-82 dBm	-81 dBm
424 m	no signal	-91 dBm

General Motors and Opel provide vehicle online connectivity based on the OnStar service. Only if the OnStar service is enabled the Wi-Fi-AP of the Opel Insignia can be switched on. The Wi-Fi transmitter is activated when the ignition is started and deactivated when the key is removed from the ignition lock. Enabling or disabling the Wi-Fi-AP is not possible for the driver, using only the configuration menu implemented in the vehicle (disabling is possible with an appropriate smartphone app).

4) Test Case 4: As test equipment a Lenovo ThinkPad T400, TP-Link TL-WN722N with standard antenna, and LinSSID on the one hand and Samsung S7, and Wifi-Analyzer on the other hand are used. Figure 4 presents the test setting. In stand still mode the following Secondary Vehicle Identifier and additional information has been measured for the Wi-Fi device of the Opel Insignia, for all distances up to 60m with both test equipments.

Listing 5. SSID and BSSID of an Opel Insignia head-unit

```
SSID: WiFi Hotspot 1760
BSSID: C4:49:BB:21:91:DE
Frequency: 2437 MHz; 2448-2426 = 22 MHz
Channel: 6
Misc.: WPA2-PSK-CCMP+TKIP, ESS,
       MITSUMI ELECTRIC Co.,LTD
```

Next, we determine the maximum detection distance for the Secondary Vehicle Identifiers. As test equipment a HP notebook, TP-Link TL-WN722N with standard antenna, and a LinSSID on the one hand and a Huawei P8 lite 2017 with a Wifi-Analyzer on the other hand are used. The results are shown in Table IV for the Wi-Fi device of the Opel Astra. If a signal has been detected, then the SSID and the BSSID can always be extracted. The smart phone detected a signal up to 216 m, the USB-Wi-Fi-device up to 424 m.

5) Test Case 5: As test equipment a HP notebook, TP-Link TL-WN722N with standard antenna, and a LinSSID on the one hand and a Huawei P8 lite 2017 with Wifi-Analyzer

TABLE V. SIGNAL STRENGTH OF THE ASTRA WI-FI DEVICE IN DRIVING MODE

Speed	Maximum signal strength Huawei P8 lite 2017	Maximum signal strength TP-Link TL-WN722N
50 km/h	-60 dBm	-55 dBm
100 km/h	-71 dBm	-50 dBm

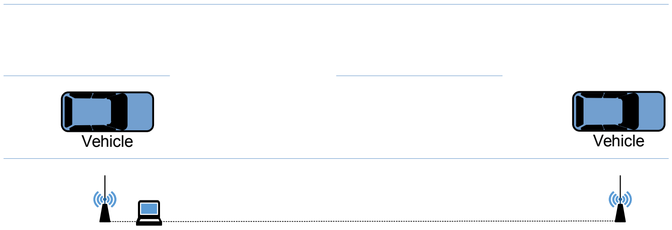


Figure 9. Attack scenario: Tracking of vehicles

app on the other hand are used. The notebook with USB - Wi-Fi device and the smart phones operate 1 m above the floor beside the roadway. Figure 5 shows the general test case. The results for the Wi-Fi device of the Opel Astra are presented in Table V. The maximum signal strength has been detected by the USB-Wi-Fi-device. The measured signal strengths with the TP-Link for 50 and 100 km/h are surprising. We assume that this issue is caused by the moving vehicle and the sample rate of the measurement devices of about 1 Hz (vehicle moves 13,9 m/s at 50 km/h and 27,8 m/s at 100 km/h).

VII. Tracking of Vehicles

We have shown that the identification and tracking of vehicles based on Secondary Vehicle Identifier can be performed with very cheap technical measurement equipment. This capability can be misused for tracking of vehicles. A technical measurement infrastructure to perform such kind of tracking is shown in Figure 9. Here, we consider only adversaries who passively sniff the communication.

To monitor vehicle motions in a specific geographic region a dense net of road side stations operating as sniffer would be needed. Due to current privacy regulations such an infrastructure for tracking of individual vehicles can be precluded in Western Europe [20]. It seems more realistic to be identified by scattered receivers of crucial neighbours monitoring vehicle motions in a street.

VIII. Countermeasures

A. Technology Independent Measures

In principle, wireless communication technology enables the identification and tracking of vehicles. One basic requirement to avoid privacy violations based on wireless interfaces or communication technologies is to avoid static identifiers in the whole communication stack. For example, communication technology for the vehicle-2-vehicle communication technology applies this rule [16].

Identification and tracking are completely excluded if the wireless communication components are powered down. But in vehicles Bluetooth (BR) is used for connecting a smart phone to the:

- Hands-free phone system
- Vehicular head-unit to use the loudspeaker of the head-unit to output the music from the smart phone

If drivers use this Bluetooth capabilities they will not quit the usage due to possible privacy risk.

The tracking problem can be reduced, however, if the antennas are located inside the vehicle and the field strength of the Bluetooth and Wi-Fi transmitters are limited. Especially during connection mode the field strength can be reduced to a necessary range to retain the data communication.

B. Technology Dependent Measures

1) Bluetooth: An alternative to Bluetooth (BR) to avoid simple tracking is the usage of Bluetooth Low Energy. BLE has specific privacy features, which are briefly described in Section IV-A3. In particular, private Bluetooth addresses should be used. This feature avoids the tracking of Bluetooth devices in connection mode. But the issue of tracking is still valid if BLE components are in advertising mode.

Obviously, private addresses have to be used for the Bluetooth interface in the head-unit als well as for the connected Bluetooth components.

2) Wi-Fi: A common standard for MAC ID randomization for Wi-Fi components is still missing. There are proprietary implementations for operating systems mentioned in Section IV-B3. The mechanism implemented in Windows 10 [21], [2]. Random MAC IDs are possible with Windows 10 if hardware and driver supports this issue. Interesting is that Windows 10 does not only use random device addresses during probe requests. It also employs a random address when connecting to a network. Further detailed investigations are needed to suggest adequate solutions for Wi-Fi MAC ID randomization for vehicles which are compliant with the Wi-Fi standard.

IX. Conclusion and Future Work

As shown in Section VI, it is technically very easy to capture Secondary Vehicle Identifiers based on wireless interfaces of vehicles, especially Bluetooth and Wi-Fi (even with low cost equipment as shown in this paper). Although, these interfaces are designed to connect the devices of passengers, vehicle identifiers can be detected far away from the vehicle (424 m for Wi-Fi with a TP-Link device) and high vehicle speed of up to 100 km/h. This enables the misuse of vehicle identifiers for the tracking of vehicles. At least, MAC ID randomization is needed for Bluetooth and Wi-Fi interfaces in vehicular head-units. BLE already supports random device addresses. For Wi-Fi only proprietary solutions are available. Altogether further investigations are needed to propose random MAC ID solutions which can be broadly applied in vehicular devices.

In general, vehicle manufacturer avoid to produce country specific vehicles. So we expect that our measurements hold for all instances of the analyzed car models at least in Europe.

In the context of the upcoming V2V communication our results are worrysome concerning the privacy of vehicles and drivers. The V2V communication is a short range communication technology with a communication range of about 800 m in open space.

In the future, every vehicle will periodically broadcast Cooperative Awareness Messages (CAM) with a packet generation rate of 1 up to 10 Hz. A CAM contains a lot of data about the sending vehicle: current geographic position, speed, driving direction, etc., at a specific time. One privacy requirement is that a receiver can not link a CAM to a specific vehicle. Secondary Vehicle Identifiers can be misused to link captured CAM messages to a specific vehicle [22].

Acknowledgement

The authors would like to thank our colleagues Christian Berghoff, Tobias Franz and Thomas Strubbe for detailed discussions. Also thanks to the anonymous reviewers for the valuable comments.

References

[1] M. Ullmann, T. Franz, and G. Nolden, "Vehicle Identification Based on Secondary Vehicle Identifier - Analysis, and Measurements -," in Proceedings VEHICULAR 2017: The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications. IARIA, 2017, pp. 32–37.

[2] M. Vanhoef, C. Matte, M. Cunche, L. S. Cardoso, and F. Piessens, "Why mac address randomization is not enough: An analysis of wi-fi network discovery mechanisms," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security. ACM, 2016, pp. 413–424.

[3] M. Ullmann, T. Strubbe, and C. Wieschebrink, "Technical Limitations, and Privacy Shortcomings of the Vehicle-to-Vehicle Communication," in Proceedings VEHICULAR 2016: The Fifth International Conference on Advances in Vehicular Systems, Technologies and Applications. IARIA, 2016, pp. 15–20.

[4] H. Lee, D. Kim, D. Kim, and S. Y. Bang, "Real-time automatic vehicle management system using vehicle tracking and car plate number identification," in Multimedia and Expo, 2003. ICME'03. Proceedings. 2003 International Conference on, vol. 2. IEEE, 2003, pp. II–353.

[5] R. Bruno and F. Delmastro, "Design and Analysis of a Bluetooth-Based Indoor Localization System," 2003, pp. 711–725.

[6] R. Zhou, "Wireless Indoor Tracking System (WITS)," Aktuelle Trends in der Softwareforschung, Tagungsband zum IT Software-Forschungstag. Dpunkt Verlag Heidelberg, Germany, 2006, pp. 163–177.

[7] C. Carpenter, M. Fowler, and T. Adler, "Generating Route-Specific Origin-Destination Tables Using Bluetooth Technology," Transportation Research Record: Journal of the Transportation Research Board, no. 2308, 2012, pp. 96–102.

[8] M. Mueller, D. Schulz, M. Mock, and D. Hecker, "Detecting mobility patterns with stationary bluetooth sensors: A real-world case study," in Proceedings of the 18th AGILE International Conference on Geographic Information Science, 2015.

[9] M. Emery and M. K. Denko, "IEEE 802.11 WLAN Based Real-Time Location Tracking in Indoor and Outdoor Environments," in Electrical and Computer Engineering, 2007. CCECE 2007. Canadian Conference on. IEEE, 2007, pp. 1062–1065.

[10] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in 19th USENIX Security Symposium, Washington DC, 2010, pp. 11–13.

[11] S. Astapov and A. Riid, "A Multistage Procedure of Mobile Vehicle Acoustic Identification for Single-Sensor Embedded Device," International Journal of Electronics and Telecommunications, vol. 59, no. 2, 2013, pp. 151–160.

[12] B. Danev, D. Zanetti, and S. Capkun, "On Physical-Layer Identification of Wireless Devices," ACM Computing Surveys (CSUR), vol. 45, no. 1, 2012, p. 6.

[13] T. Jiang, H. J. Wang, and Y.-C. Hu, "Preserving location privacy in wireless lans," in Proceedings of the 5th international conference on Mobile systems, applications and services. ACM, 2007, pp. 246–257.

[14] Wang, Ping, "Bluetooth Low Energy-privacy enhancement for advertisement," Master's thesis, Norwegian University of Science and Technology, Departement of Telematics, 2014.

[15] Andrew Hilts, Christopher Parsons, and Jeffrey Knockel, "Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security," 2016, https://openeffect.ca/reports/Every_Step_You_Fake.pdf access date: July 30, 2018.

[16] ETSI, "ETSI TR 102 893 V1.1.1: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA); Technical Report," 2010, http://www.etsi.org/, Access Date: June 02, 2017.

[17] ——, "ETSI EN 302 665 V1.1.1: Intelligent Transport Systems (ITS) - Communications Architecture," 2010, http://www.etsi.org/, Access Date: June 02, 2017.

[18] "Bluetooth Core Specification, v 5.0," 2011, https://www.bluetooth.com/specifications/bluetooth-core-specification, access date: July 25, 2018.

[19] Ubertooth Developer, "Ubertooth Bluetooth Sniffer," 2017, https://github.com/greatscottgadgets/ubertooth/, access date: March 24, 2017.

[20] European Commission, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," 2016, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en access date: August 03, 2018.

[21] C. Huitema, "Experience with mac address randomization in windows 10," in 93th Internet Engineering Task Force Meeting (IETF), 2015.

[22] M. Ullmann, and T. Strubbe, and C. Wieschebrink, "Misuse Capabilities of the V2V Communication to Harm the Privacy of Vehicles and Drivers," in International Journal On Advances in Networks and Services, vol 10 no 12. IARIA, 2017.