Vehicle Identification Based on Secondary Vehicle Identifier - Analysis, and Measurements -

Markus Ullmann[*] [†] Tobias Franz,[†] and Gerd Nolden[*]
[*] Federal Office for Information Security
D-53133 Bonn, Germany
Email: {markus.ullmann, gerd.nolden}@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, tobiasfranz91@gmail.com

Abstract—**Increasingly, vehicles will be equipped with information and communication technologies, e.g., wireless communication technologies like IEEE 802.11x (Wi-Fi), Bluetooth, mobile communication, etc. These communication technologies enable identification based on identifier used in communication protocols. Today, the Vehicle Identification Number, and the license plate are regarded as vehicle identifier. With new communication technologies used in modern vehicles secondary vehicle identifier comes up. This paper analyzes identification of vehicles based on wireless communication interfaces and presents results of first real measurements of vehicular Bluetooth and Wi-Fi interfaces.**

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

I. Introduction

The IT architecture of vehicles has significantly changed during the last 10 years. This is shown by the increasingly availability of components for driving assistance: lane keeping support, traffic jam assist, automatic parking assistant, remote parking assistant and so on. This 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 able to establish a Wi-Fi hot spot to support internet access for vehicle passengers. Furthermore, the vehicle-2-vehicle communication technology (V2V) will be deployed based on IEEE 802.11p technology 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 identifier. This paper analyses vehicle identification capabilities of wireless communication interfaces, first, which can be used for vehicle identification and tracking. Next, first results of enforced measurements of vehicular Bluetooth interfaces and vehicular Wi-Fi hotspots are presented. The communication interfaces are built in the vehicle to support communication services for occupants. But we show that these services are available outside the vehicle and can be misused for unauthorized identification and tracking. We only use cheap measurement equipment (partially open source), which is publicly available. Especially, the applied smart phone measurement apps can be used by everyone with every modern Android compatible device for identification of vehicles based on Bluetooth. The analysis of Secondary Vehicle Identifier based on Bluetooth and Wi-Fi features is quite new and published here, first.

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 implemented wireless technologies in modern vehicles and analyzes identification capabilities. Aim of the performed tests, used test equipment and investigated test vehicles are presented in Section V. Results of real measurements of Bluetooth and Wi-Fi identifier are given in Section VI. Finally, we summarize our results, and mention open research issues.

II. Related Work

A classification of vehicle identifier is given in [1], which is applied in this paper, too. Hwajeng et al. supposed a vehicle identification and tracking system based on optical vehicle plate number recognition [2]. Tracking of devices based on Bluetooth interfaces is already discussed for a lot of applications, e.g., indoor localization [3] or wireless indoor tracking [4]. But only in [5], an analysis in Jacksonville, Florida, to capture vehicle traffic streams is described. Therefore, a set of Bluetooth receivers was located at the roadside on specific streets to capture the Bluetooth MAC ID of crossing vehicles. Besides Bluetooth, IEEE 802.11 compliant devices were suggested for real-time location tracking in indoor and outdoor environments [6].

Since the 1th of November 2014, vehicles and motorhomes have to be equipped with a Tire Pressure Monitoring System (TPMS) within Europe. They can be separated in direct and indirect TPMS. Direct TPMS means that specific physical sensors measure the air pressure of the tires. These sensors communicate wireless 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 [7].

Besides the identification of vehicles based on static identifiers used in communication protocols different feature based identification methods are suggested. One approach is the identification of vehicles based on noise features (individual noise spectrum) [8].

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 transmitter introduced at the manufacturing process. A good overview concerning the physical fingerprinting of different wireless communication technologies is given in [9].

III. ITS Vehicle Identifier

Here, we categorize the available identifiers of vehicles into two classes. Primary vehicle identifier represent such identifiers which will be typically regarded today, e.g., the Vehicle Identification Number (VIN). Secondary Vehicle Identifier come up with new information technologies used in modern vehicles.

A. Primary Vehicle Identifier

To date, each vehicle is identifiable based on the distinct 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 licence plate, which is already used for identification.

With the deployment of the V2V technology vehicles will be equipped with a long term ECC key pair and an appropriate certificate [10] [11]. This certificate will become an additional primary vehicle identifier.

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 MAC identifier. 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 equipped laptop, tablet or mobile phone to access the internet within the ITS vehicle station while travelling if the head-unit has mobile communications capabilities. But head-units configured as access point need a unique Service Set Identifier (SSID) or network name to connect devices. In addition, each head-unit needs an unique MAC address.

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

In [9], physical fingerprinting of wireless transmitter is investigated. So, a complete feature set for physical fingerprinting of a transmitter is a secondary vehicle identifier. So far mentioned vehicle identifiers are sufficient for identification all the time. Furthermore, vehicle identifier 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 licence plate or VIN. But it is technically very easy to capture Bluetooth and Wi-Fi identifiers of a vehicle shown in Section VI. So, attackers can misuse them for their purposes.

IV. Wireless Technologies

Here in this section wireless technologies, which are applied in vehicles are described, first. 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 like GSM, LTE, or 5G.

A. Bluetooth

The concept behind Bluetooth is to provide a universal short-range wireless communication capability using the 2.4 GHz band, available globally for unlicensed low-power uses. Bluetooth is specified by the Bluetooth special interest group [12].

1) 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 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 the 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 resistant to disturbance a frequency hopping spread spectrum (FHSS) is used. Bluetooth devices operate in the ISM band (2.4 to 2.485 GHz). This frequency range is divided into channels of a bandwidth of 1 MHz. There are 79 useable channels. Three classes of transceivers are available with different output power: 1 mW, 2,5 mW and 100 mW.

At first, Bluetooth devices have to establish a connection, termed pairing, to exchange data. This procedure is initiated by the master 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 exist a range of Bluetooth 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). LAP (24 bit) and UAP (8 bit) are assigned to the manufacturer of the device, and NAP (16 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 identifier. 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, too (Table I).

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 802.11 X.

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 send 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 equipped 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 used frequency band (2,4 GHz and/or 5 GHz), and communication speed (1 Mbit/s . . . 6,96 Gbit/s). The frequency band is splitted into channels (2,4 GHz: 13 channels with a bandwidth of 5 MHz, whereby 5 channels are needed to establish a network). In the 5 GHz frequency band a 455 MHz frequency bandwidth is reserved for Wi-Fi to establish 18 different Wi-Fi networks.

One of the management frames in IEEE 802.11 based Wi-Fis are beacon frames. 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 network beacon generation is distributed among the stations.

2) Identification Capabilities: Primary identifier 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)

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

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

V. MEASUREMENTS

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

A. Aim of the Measurements

With the measurements we investigate vehicular Bluetooth as well as Wi-Fi communication capabilities especially for identification purposes outside the vehicle. Therefore, 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 in the following measurements:

- Skoda Octavia 3: 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:

- 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 [13]
  - Standard antenna, LogPer Antenna and directional antenna WIFI-LINK WAVEGUIDE Antenna PN: WCA-2450-12, 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 playstore)

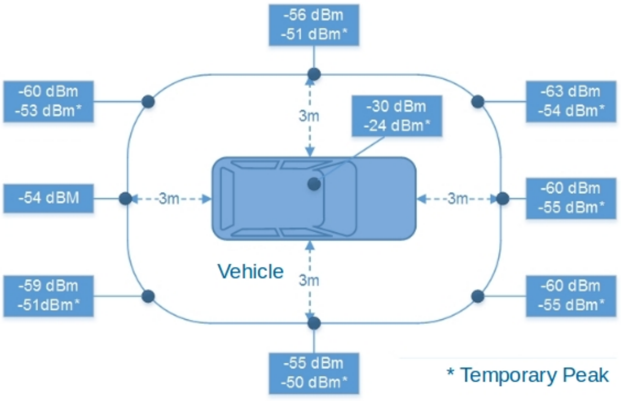

Figure 1. Radiation characteristic of the Octavia Bluetooth device

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

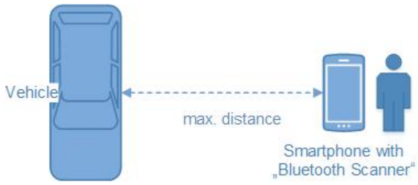

Figure 2. Test arrangement for the detection of Secondary Vehicle Identifier in stand still mode

2) 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 desribed.

A. Bluetooth Measurements for the Octavia (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 1. As we expected, the highest signal strength of -30 dBm has been detected inside the vehicle. But also outside the vehicle, a strong signal strengh has 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, as test equipment a Samsung Galaxy S6 with the Bluetooth scanner app is utilised. Figure 2 presents the test setting. The following information about the Bluetooth device of the head-unit can be captured with the mentioned test equipment:

```
 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. These information are 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 has already altered its SSID. “Skoda_TF” is not the factory setting).

The following information are 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):

```
 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 automaker is part of the SSID and that the number part “2058” of the SSID is chosen from the VIN of the Passat.

Next, as test equipment Lenovo ThinkPad X201, Ubertooth One with Ubertooth-RX is used to perform the same test case. Subsequent information can be captured if the test equipment is switched on and a Samsung Galaxy S6 will be 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
```

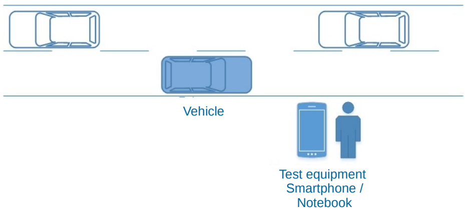

Figure 3. Test arrangement for the detection of secondary vehicle identifier in driving mode

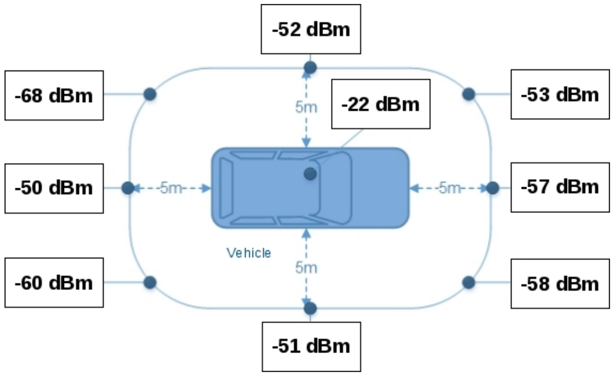

Figure 4. Radiation characteristic of the Opel Insignia Wi-Fi device

```
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: With the test equipment Samsung Galaxy S6 with the Bluetooth scanner app, subsequent information can be captured up to a speed of 30 km/h. Figure 3 shows the test case.

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

B. 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 fix point 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 4. As we expected, the highest signal strength of -22 dBm has been detected inside the vehicle. But also outside the vehicle, a strong signal strengh has 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 side and Samsung S7, and Wifi-Analyzer on the other side are used. With the TP-Link TL-WN722 and the Samsung S7 the signal strenght are measured in ascending distances to the vehicle, in direction to the right front door. The results are plotted in Figure 5. Only little 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.

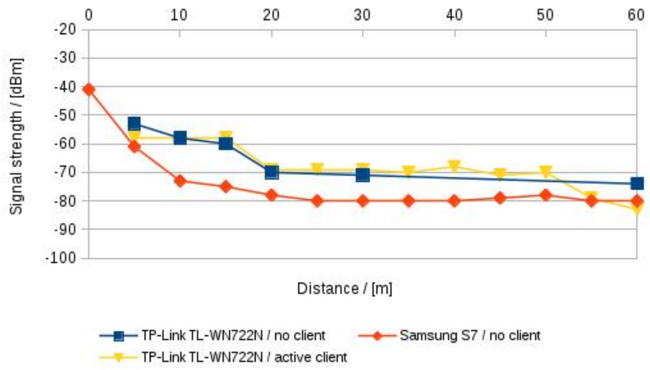

Figure 5. Radiation characteristic of the Opel Insignia Wi-Fi device

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

General Motor 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. An enabling or disabling of the Wi-Fi-AP is not possible by the driver, with the usage of the configuration menu implemented in the vehicle (disabling 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 side and Samsung S7, and Wifi-Analyzer on the other side are used. Figure 2 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.

```
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 Identifier. As test equipment a HP notebook, TP-Link TL-WN722N with standard antenna, and a LinSSID on the one side and a Huawei P8 lite 2017 with a Wifi-Analyzer on the other side are used. The results are presented in Table III for the Wi-Fi device of the Opel Astra.

TABLE III. 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

TABLE IV. 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

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 side and a Huawei P8 lite 2017 with Wifi-Analyzer app on the other side are used. Notebook with USB - Wi-Fi device and smart phones operate 1 m above the floor beside the roadway. Figure 3 shows the principle test case. The results for the Wi-Fi device of the Opel Astra are presented in Table IV. The maximum signal strenght 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 by 50 km/h and 27,8 m/s by 100 km/h).

VII. Conclusion

As shown in Section VI, it is technically very easy to capture Secondary Vehicle Identifier based on wireless interfaces of vehicles, especially Bluetooth and Wi-Fi (even with low cost equipment shown in this paper). Although, this interfaces are designed to connect devices of occupants, vehicle identifier can be detected far away from the vehicle (Wi-Fi 424 m with a TP-Link device) and high vehicle speed of up to 100 km/h. This enables the misuse of vehicle identifier for the tracking of vehicles.

In the context of the upcoming V2V communication our results are worrying concerning 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 future, each vehicle periodically broadcasts 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. Now, Secondary Vehicle Identifier can be misused to link captured CAM messages to a specific vehicle [14].

Besides the investigation of wireless Secondary Vehicle Identifiers, we noticed, that the security configuration of the Wi-Fi-APs in the examined vehicles should be improved. For example, neither MAC filtering, invisibility of the SSID identifier nor adjustable signal strengh, etc., can be set based on the Wi-Fi-AP configuration menues. A first improvement is to implement the security features suggested for WiFi-APs in generell. A comprehensive source for network security is the BSI IT-Grundschutz Catalogue [15].

Acknowledgement

The authors would like to thank our colleague Thomas Strubbe for detailed discussions. Also thanks to the anonymous reviewers for the valuable comments.

References

[1] Markus Ullmann, Thomas Strubbe, and Christian 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.

[2] 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.

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

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

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

[12] Bluetooth Special Interest Group, “Specifications,” 2017, https://www.bluetooth.com/specifications, access date: March 24, 2017.

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

[14] Markus Ullmann, and Thomas Strubbe, and Christian 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.

[15] Federal Office for Information Security, “IT-Grundschutz Catalogues,” 2013, https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html, access date: March 30, 2017.