2015

# An overview of bluetooth device discovery and fingerprinting techniques – assessing the local context

Maxim Chernyshev
*Security Research Institute, Edith Cowan University*, m.chernyshev@ecu.edu.au

DOI: 10.4225/75/57b3f8ebfb88c
This paper was originally presented at The Proceedings of [the] 13th Australian Digital Forensics Conference, held from the 30 November – 2 December, 2015 (pp. 77-84), Edith Cowan University Joondalup Campus, Perth, Western Australia.

# AN OVERVIEW OF BLUETOOTH DEVICE DISCOVERY AND FINGERPRINTING TECHNIQUES – ASSESSING THE LOCAL CONTEXT

Maxim Chernyshev
Security Research Institute, Edith Cowan University, Perth, Australia
m.chernyshev@ecu.edu.au

## Abstract

*The ubiquitous nature of portable communication devices presents a number of opportunities for automated device discovery, tracking and possible owner identification. Consumer devices such as smartphones, tablets, wearables, laptops and vehicle entertainment systems commonly support the 802.15.1 (Bluetooth) wireless communication protocol that enables a variety device discovery and fingerprinting techniques. We provide an overview of these techniques encompassing those native to the protocol as well as those that are possibly protocol-agnostic due to their inherently generic nature. We then introduce an opportunity for a comparison study that sets out to examine and quantify the effectiveness of selected techniques in the field. To assess the potential viability of such study in the local context, we employ location-aware inquiry scanning and discuss the results of the exploratory data collection. We conclude that in this context the simplest technique being inquiry scanning can be used to establish a baseline for comparison with other techniques.*

**Keywords**
Bluetooth, device discovery, device fingerprinting, Ubertooth One

## INTRODUCTION

Consumers are adopting electronic mobile devices such as smartphones, wearables and smart home appliances at a constantly increasing rate. The number of wearable device shipments alone is expected to exceed 90 million in 2016, meaning that more individuals will be expected to carry at least one device with them at all times (Gartner, 2014b). Moreover, Gartner (2014a) also predict that a third of all wearable devices in 2017 will be inconspicuous, listing smart glasses, contact lenses and jewellery as possible examples. Devices that are unobtrusive to the eye can still be detected, identified and tracked over time using non-visual methods. The open nature of the radio communications medium allows interested parties to capture, process, interpret and aggregate the emitted signals.

The 802.15.1 (Bluetooth) wireless communication protocol in use by many device classes can facilitate a variety of device discovery and fingerprinting techniques. While common techniques based on commodity as well as specialised tools have been documented extensively, alternative low-cost hardware and open-source software components have recently become available. This paper provides an overview of the relevant techniques and introduces an opportunity for a comparison study that sets out to examine Bluetooth device reconnaissance techniques using a mix of traditional and modern components.

## DEVICE DISCOVERY AND FINGERPRINTING TECHNIQUES

This section provides a categorised outline of works specifically related to tracking or fingerprinting Bluetooth devices. Two core categories are identified – native and specialised. The former encompasses techniques that can be achieved using standard consumer grade tools, whereas the latter covers those requiring access to specialised components.

### Protocol Background

The 802.15.1 (Bluetooth) specification was originally developed by the Institute of Electrical and Electronics Engineers (IEEE) to facilitate short range wireless communications for personal devices (IEEE, 2004). Depending on device class and Bluetooth stack type, the maximum theoretical Bluetooth range can be up to 1000 metres for classic Bluetooth and up to 250 metres for Bluetooth Low Energy (LE) (Dunning, 2010c). The standard utilises the unlicensed 2.4 GHz band split across 79 channels, and employs channel hopping scheme referred to as the *Frequency Hopping Spread Spectrum (FHSS)*, whereby devices change channels based on an agreed pseudorandom sequence every 625 μs or 1,600 times per second (Cache et al., 2010, p. 274). The master

device uses its clock to generate the hopping pattern. Connecting devices are referred to as slaves and device communication forms a basic network called a *piconet*.

**Native Techniques**

Whitehouse (2003) introduced the original set of native techniques including:

- Inquiry scan for locating discoverable devices;
- Vendor address range scan for locating non-discoverable devices, and
- Device fingerprinting via information extraction.

*Discoverable Devices*

Haase and Handy (2004) utilised inquiry scan using both fixed and mobile sensors and were able to identify over 5,000 unique devices at a crowded location over a one-week period. Given the inability of sensors to access the *Received Signal Strength Indicator (RSSI)* value as version 1.2 of the protocol was still being ratified, it was not possible to determine device proximity in relation to the sensors in order to perform more accurate tracking. Nevertheless, the authors discovered that at least 1% of identified devices contained real person names in advertised device names, presenting a potential device to person linkage opportunity.

Pels, Barhorst, Michels, Hobo, and Barendse (2005) used inquiry scan with fixed sensors across three train stations in two observation scenarios and were able to identify almost 4,000 unique devices. The paper highlighted a number of issues with being able to locate moving devices such as those carried by people on the train due to the speed of movement and architectural features of the train station. Thus, relevant considerations must be kept in mind when designing experiments in non-stationary scenarios – vehicular data collection being one possible case.

The emergence of a de-facto architecture for Bluetooth-based tracking can be observed through works by Callaghan, Harkin, and McGinnity (2006); Haase and Handy (2004); Jappinen, Laakkonen, Latva, and Hamalainen (2004); Pels et al. (2005). Jappinen et al. (2004) present a high-level architecture of a Bluetooth-based surveillance and tracking system. Callaghan et al. (2006) illustrate the architecture of their *Bluetrack* system, which relies on distributed sensors that send collected information back to the central data collection server also used to support the subsequent analysis and visualisation tasks. Another group used a modified version of an open-source trace monitoring script called *braces* also based on inquiry scan (Caldwell, Ekerfelt, Hornung, & Wu, 2006). The authors adopt an improved architecture by introducing offline data storage support and incorporating additional device information extraction capabilities. The specifics of the described hardware and software components reveal that one of the sensors was powered by a *Gumstix Waysmall* microcomputer, indicating a possibly unintentional desire to explore a distributed data collection model similar to those employed in modern Internet of Things (IoT) sensor deployments.

*Non-discoverable devices*

Whitehouse (2003, pp. 6-8) described a mechanism for defeating device non-discoverability using a self-developed tool called *RedFang*. The approach was based on the principle that non-discoverable devices would still respond to targeted inquiry requests directed at their BD_ADDR implying the possibility of brute-force scanning an arbitrary address range. However, scanned devices can take multiple seconds to respond, undermining the practical applicability of this method for large address ranges, which is even less effective in the case of non-stationary clients. Parallel processing can be employed to address the limitation to some extent, but it can result in additional hardware costs, increased power consumption and implementation complexity.

Despite the tool being mentioned in several subsequent works, no targeted attempts at quantifying its device discovery potential in the field appear to have been documented (Caldwell et al., 2006; Callaghan et al., 2006). One exception is the paper by Haataja (2005) where the author suggests that technique viability can be improved by assuming that part of BD_ADDR value representing the vendor OUI is known thereby allowing for a significant reduction of the address space. In 2008, Cross, Hoeckle, Lavine, Rubin, and Snow (2008) proposed an improved technique that required using 79 sensor devices (one per channel) at once, which the authors themselves labelled as impractical. Dunning (2010) suggested a potential method for narrowing down the address space using device address information collected from other devices in the area.

*Enumerating Device Service Information*

The discovery process can be complemented by additional information extraction, as originally discussed by Whitehouse (2003). In addition to the BD_ADDR value and device name, information extractable from the *Service Discovery Protocol (SDP)* profiles can be used to obtain these identifiers. The original concept was refined by Herfurt and Mulliner (2004), who aimed to set a standard for fingerprinting Bluetooth devices using a hash calculation algorithm called *Blueprinting*, which used the *RecHandle* and *RFCOMM Channel* values for each SDP service.

**Specialised Techniques**

*Visual Inspection*

Device discovery does not always involve equipment and signal capture. Cache et al. (2010, pp. 291-292) illustrate the effectiveness of basic visual inspection in a local supermarket where they were able to locate non-discoverable Bluetooth barcode scanners and determine their BD_ADDR values on the basis of attached device stickers. While this technique has practical potential, its applicability may be highly contextual.

*Sequential MAC and BD_ADDR Assignment*

MAC addresses of selected Wi-Fi clients can be used to identify BD_ADDR values (Cache et al., 2010, pp. 293-295; Yermalkar, 2012). In the case of some Apple, Windows and Samsung devices, MAC and BD_ADDR values are assigned sequentially meaning that the former can be used to infer the latter by incrementing or decrementing the MAC address by the value of one. The derived BD_ADDR is subsequently validated if response is received to a targeted scan. Unfortunately, the technique can be prone to false positives and false negatives as sequential address assignment is only used for specific device types.

*Specialised Equipment*

Product manufacturers need access to low level signal analysis and inspection during the product development cycles. In 2007, Cisco acquired a company called Cognio that provided a number of wireless spectrum analysis products (Wexler, 2007). The rebranded *Cisco Spectrum Analyzer* could then be purchased for around US$3,000 and was able to uncover the LAP component of BD_ADDR based on passive traffic inspection. A more capable sniffer by Frontline Test Equipment (FTE) could also be used for advanced packet interception and dissection, but would require an investment of over US$10,000 (PCM, 2015). Despite the immense usefulness of these tools, the associated costs would prohibit their application in multi-sensor collection scenarios.

Spill and Bittau (2007) laid the foundations for practical Bluetooth security research at a fraction of the cost. The resulting tool called *gr-bluetooth* can be useful in gaining the understanding of the lower level aspects of the protocol and raw signal demodulation approaches using *Software Defined Radio (SDR)*. Following on from the work done by Spill and Bittau (2007), the open-source community have been working on making Bluetooth security research more accessible (Ossmann, 2010, 2011). As the result, researchers can have access to protocol inspection capabilities on par with commercial tools for around US$100 with the arrival of *Ubertooth One*.

Huang, Albazrqaoe, and Xing (2014) examined the use of Ubertooth One to implement a novel device identification system called *BlueID*. The authors conducted an empirical evaluation using 56 commodity devices and identified individual device clock skew as unique differentiating feature that could be used to derive individual device fingerprints with up to 94.3% accuracy. The described approach was presented as extremely efficient, requiring only 25% of packets transmitted per second for successful identification.

### Cross-Protocol Approaches

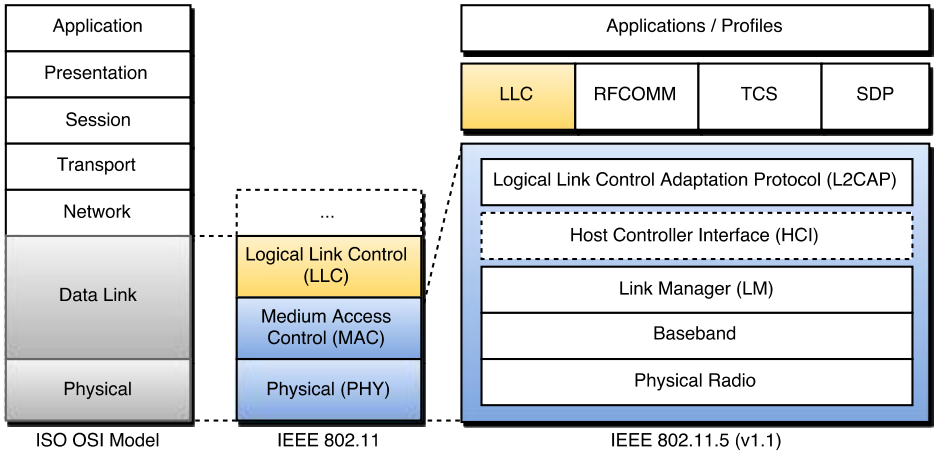


*Figure 1. Mapping classic Bluetooth (IEEE 802.11.5 v1.1) and IEEE 802.11 (Wi-Fi) to the Data Link and Physical layers of the OSI Model. Adapted from Marks, Gifford, and O'Hara (2001, p. 52); Patil (2003).*

Figure 1 demonstrates the relationship between the Open Systems Interconnection (OSI) model by Zimmermann (1980), selected 802.11 (Wi-Fi) layers and the components of the classic Bluetooth v1.1 protocol stack. The diagram shows that parts of the Bluetooth stack can be mapped to the Wi-Fi stack, primarily in the areas encompassing the Data Link and Physical OSI layers. Although the diagram does not include the Bluetooth LE stack for the purposes of simplicity, the same mapping principles would still apply. The depicted relationship is significant because it implies that techniques that have been evaluated as effective in the context of other protocols such as Wi-Fi may also be applicable to Bluetooth.

A survey of Wi-Fi device fingerprinting approaches by Xu, Zheng, Saad, and Han (2015) describes a number of observable features of interest found in the PHY and MAC layers of the 802.11. While features present in the MAC layer such as packet inter-arrival times and management frames are specific to Wi-Fi, generic features found in the PHY layer appear quite common, as both Wi-Fi and Bluetooth utilise radio communications at the lowest level of the protocol stack.

In the context of Wi-Fi, a number of studies into device fingerprinting using the PHY layer uncovered various distinct characteristics (Brik, Banerjee, Gruteser, & Oh, 2008; Polak, Dolatshahi, & Goeckel, 2011; Ureten & Serinken, 2007). Specifically, the authors explain that benign imperfections are likely to make their way into transmitter hardware as part of the manufacturing process, because production of an ideal transmitter would not be cost effective. As long as the resulting parameters are within defined deviation thresholds, there is no driver to invest into process and quality control refinements. As the result, signals emitted by seemingly identical transmitters generally contain subtle differences that can be leveraged for device identification and fingerprinting.

The cross-protocol applicability of *Radio Frequency Fingerprinting (RFF)* techniques is supported by the fact that that Barbeau, Hall, and Kranakis (2006) were able to capture high-accuracy fingerprints for various types of Bluetooth transceivers from different manufacturers using similar features. However, with the exception of Ureten and Serinken (2007), other authors generally do not discuss the specifics of the technical components used to conduct the experiments, making practical replication more difficult. Subsequently, the exploration of RFF techniques using modern SDR tools that provide low-cost access to the radio spectrum for around US$300 could be considered as a possible evaluation approach (SparkFun, 2015).

### Revisiting Inquiry Scan

A significant portion of previous research into Bluetooth device tracking is based on inquiry scanning (Callaghan et al., 2006; Ellersiek et al., 2013; Haase & Handy, 2004; Pels et al., 2005; Van Londersele, Delafontaine, & Van de Weghe, 2009). However, it is worthwhile recognising that associated findings were possibly developed on the basis of data representing a subset of observable clients that were configured as discoverable at the time of observation. There is a an opportunity to revisit Bluetooth device reconnaissance and quantify the advantages of using a modern platform such as *Ubertooth One* over basic inquiry scanning as well as examine and suggest more effective methods that employ a combined set of techniques using a hybrid approach. Subsequently, we aim to conduct a comparison study to realise this opportunity and fill the related gap. Having obtained the ethics approval, the initial step is aimed at examining the data collection potential

associated with the local geographical context. The developed understanding will feed into experimental design in areas such as sensor numbers and positioning and deployment models.

## CONTEXT EVALUATION

To gauge the viability of a techniqye comparison study, we conducted an exploratory data collection activity based on inquiry scanning in Perth, Western Australia. We used a sensor mounted in a vehicle driven alongside a predetermined route over a period of ten consecutive days. The sensor was based on a commodity tablet device (Asus Nexus 7) and used the freely available *Bluetooth 4.0 Scanner* app by Abraham, 2015a. While the app implements inquiry scan-based device discovery for both classic Bluetooth and Bluetooth LE, our experiment was limited to classic Bluetooth. As part of the scanning process, the instrument tracks user locations, attempts to capture friendly device names and performs vendor OUI lookups using a local database. Possibly due to the age of the bundled OUI database, vendor lookups in particular appeared to be only partially successful and we had to repeat the process manually using the most up-to-date version of the OUI reference file using a custom script. The scanner app is part of a crowd-sourced Bluetooth device location database project called *Eearthping* that at the time of writing contains just over 500,000 devices (Abraham, 2015b). Unfortunately, the project no longer appears to be active.

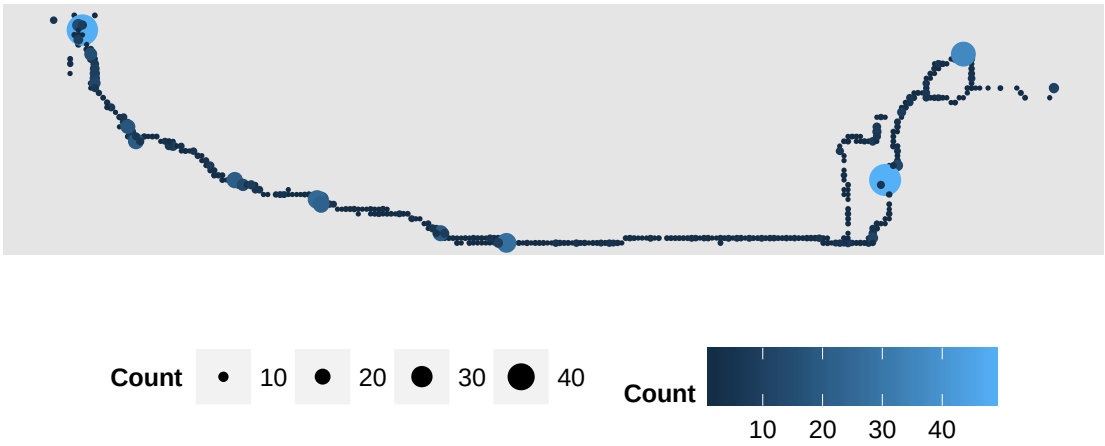


*Figure 2. Geographical representation of the route traversed as part of the experiment depicting density of unique device observations based on point size and colour gradient. Naive spatial clustering was applied for aggregation by rounding the latitude and longitude values to 3 decimal points.*

The data collection processed yielded 786 unique devices based on a total of 3,610 spatiotemporal observations. The outline of the travelled route and the associated observation density are presented in Figure 2. For added context, we note that the presented route is associated with minor and major arterial roads travelling across areas of varying urban density including two residential suburbs, an industrial area and a university campus. While we observe that unique device observation counts vary between 1 and over 40 devices, most of the observations are appear at the lower end of the spectrum. Using a physical map overlay, we determined that the majority of dense observation areas are associated with major road intersections where the sensor would remain stationary for prolonged periods of time surrounded by a larger group of stationary vehicles in close proximity. We could also examine and compare day-by-day observation accumulations, but at this point we are interested in establishing whether simple inquiry scanning alone can provide a viable basis for technique effectiveness comparison.

The number of observations, unique devices and newly observed devices for each day are shown in Figure 3. We note that due to issues with the data collection instrument, there is a significant drop in the number of observations on days 6 and 7. Nevertheless, we observe that the number of observations is not necessarily representative of the number of unique devices (see day 4 versus day 5 as an example). At the same time, the number of new devices is not significantly lower than the number of observed devices. This finding implies that (1) certain devices are seen on an ongoing basis across multiple observation days and (2) devices not previously observed are discovered on every subsequent observation day.

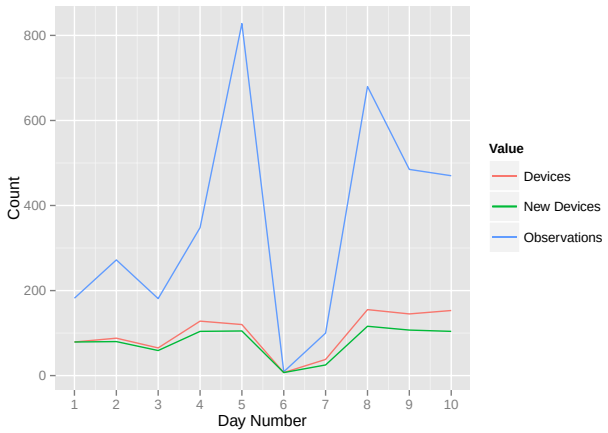


*Figure 3. Line chart that shows counts of spatiotemporal observations, devices and new devices (not observed during preceding collection days) by observation day number.*

The latter observation, however, does not necessarily imply that new devices are original and have not been observed previously. As shown in Figure 4, most of the observed devices are attributed to the *UNKNOWN* vendor meaning that no entity could be recognised based on their address. This finding possibility reveals common presence of devices running in *anonymity mode*, a Bluetooth privacy preservation feature designed as part of the version 1.2 of the specification (Gehrmann, Persson, & Smeets, 2004). On top of this, we also notice a diverse vendor mix dominated by *APPLE* devices – presumably, smartphones, as well as other vendors generally associated with in-car entertainment systems and portable navigation aids such as *PIONEER*, *ALPINE*, *GARMIN* and *TOMTOM*.

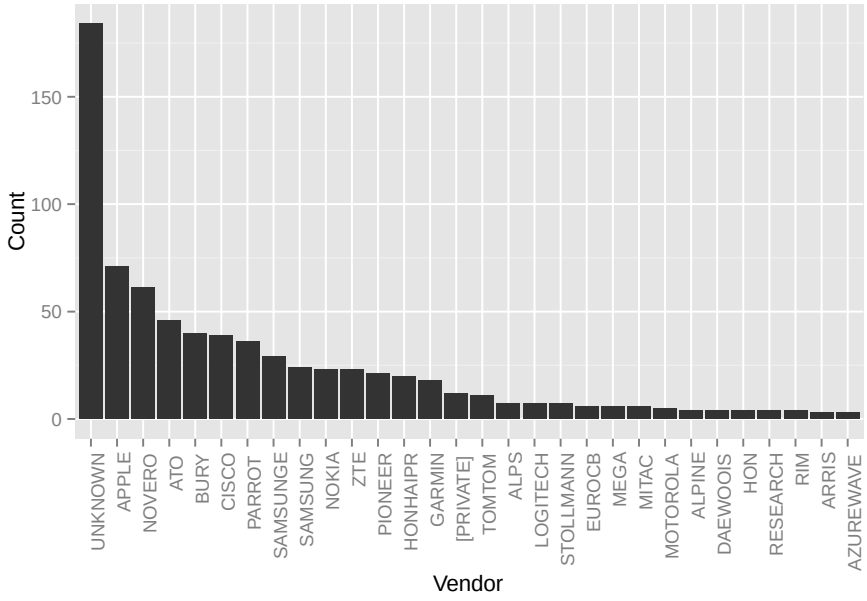


*Figure 4. Count of unique devices by vendor (top 30). OUI prefixes registered with IEEE anonymously are grouped under "[PRIVATE]".*

Furthermore, 12 devices were identified as *[PRIVATE]*, meaning that their vendors chose to register the respective OUI prefixes anonymously. The potential observation locations associated with these devices are presented in Figure 5. With the exception of device number 68, all other devices appear to have been seen in a single location. This finding could be used to infer that these devices are stationary and perhaps are associated with certain environmental and infrastructure elements, which could be useful if further analysis and assessment of this particular category would be of interest. We end our analysis at this point concluding that basic inquiry scanning could be used as a baseline observation method in a future comparison study.

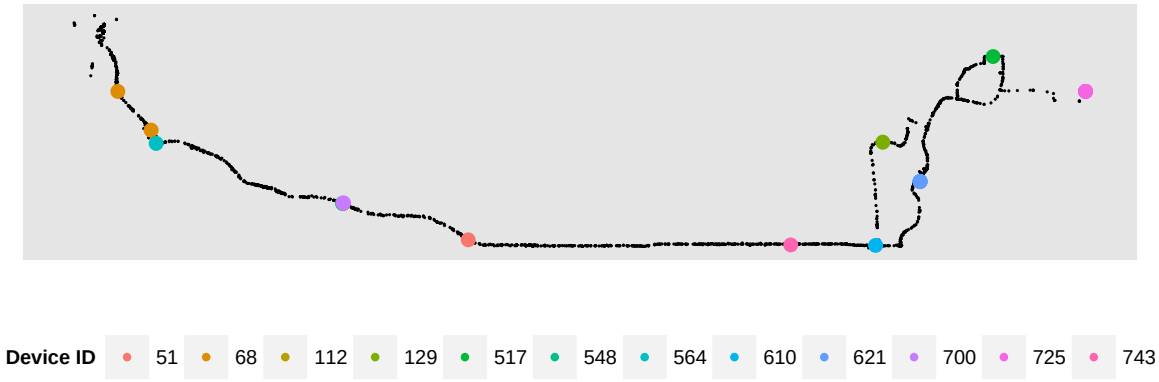


*Figure 5. Possible locations of devices identified as "[PRIVATE]".*

## DISCUSSION AND CONCLUSION

We presented an overview of various Bluetooth device discovery and fingerprinting techniques that can be realised using a range of software and hardware components. We identified the lack of practical technique comparisons in the same context as an existing research opportunity and assessed the potential for location-aware device discovery using simple methods in a local context. The presented set of preliminary observations has a number of implications.

First, the widespread presence of devices with unidentifiable OUI points to the need for other techniques that could possibly thwart the in-built anonymity preservation mechanisms. For example, combining RFF fingerprint values with the results of inquiry scan could possibly be used to attribute multiple BD_ADDR values to the same device. Second, the recurring visibility of some devices points to the continuing practical viability of inquiry scanning for device tracking purposes in a modern context, perhaps to a lesser extent than anticipated in earlier works. At the same time, the ongoing detection of new devices may indicate the need for a more effective discovery approach because it could be that some of these devices were also present on previous days but were not picked up by the sensor. Third, working on the premise that certain vendors could be aiming to achieve security through obscurity, the discovery of privately registered devices presents an opportunity for further examination aiming to uncover the class and purpose of these devices and possible motivations for anonymous registrations.

Finally, the context evaluation shows that inquiry scan can be used to establish a baseline for comparison with other techniques. We will pursue this direction in a future study and will aim to quantify the effectiveness of selected specialised techniques over the native ones. At the same time, we will aim to assess the viability of a hybrid fingerprinting approach based on low-level protocol-agnostic features.

## REFERENCES

Abraham, J. (2015a). Bluetooth 4.0 Scanner. Retrieved from https://play.google.com/store/apps/details?id=com.bluemotionlabs.bluescan

Abraham, J. (2015b). Earthping - Crowdsourced Bluetooth mapping project. Retrieved from http://www.earthping.com/

Barbeau, M., Hall, J., & Kranakis, E. (2006). *Detection of rogue devices in bluetooth networks using radio frequency fingerprinting.* Paper presented at the 3rd IASTED International Conference on Communications and Computer Networks, CCN.

Brik, V., Banerjee, S., Gruteser, M., & Oh, S. (2008). *Wireless device identification with radiometric signatures.* Paper presented at the Proceedings of the 14th ACM international conference on Mobile computing and networking.

Cache, J., Wright, J., Liu, V., Scott, E., Antoniewiecz, B., & Wang, C. (2010). *Hacking exposed wireless*: McGraw-Hill.

Caldwell, L., Ekerfelt, S., Hornung, A., & Wu, J. Y. (2006). *The art of Bluedentistry: Current security and privacy issues with Bluetooth devices*. University of Washington.

Callaghan, M., Harkin, J., & McGinnity, T. (2006). Case study on the Bluetooth vulnerabilities in mobile devices. *IJCSNS International Journal of Computer Science and Network Security, 6*(4), 125-129.

Cross, D., Hoeckle, J., Lavine, M., Rubin, J., & Snow, K. (2008). Detecting non-discoverable bluetooth devices *Critical Infrastructure Protection* (pp. 281-293): Springer.

Dunning, J. P. (2010). *Breaking Bluetooth By Being Bored*. Paper presented at the DEFCON 18, Las Vegas, USA.

Ellersiek, T., Andrienko, G., Andrienko, N., Hecker, D., Stange, H., & Mueller, M. (2013). *Using Bluetooth to track mobility patterns: depicting its potential based on various case studies*. Paper presented at the 5th ACM SIGSPATIAL International Workshop on Indoor Spatial Awareness, Orlando, Florida.

Gartner. (2014a). Gartner Predicts By 2017, 30 Percent of Smart Wearables Will Be Inconspicuous to the Eye. Retrieved from http://www.gartner.com/newsroom/id/2941317

Gartner. (2014b). Gartner Says in 2015, 50 Percent of People Considering Buying a Smart Wristband Will Choose a Smartwatch Instead. Retrieved from http://www.gartner.com/newsroom/id/2913318

Gehrmann, C., Persson, J., & Smeets, B. (2004). *Bluetooth Security*. Norwood, MA, USA: Artech House.

Haase, M., & Handy, M. (2004). *BlueTrack–Imperceptible tracking of bluetooth devices.* Paper presented at the 6th International Conference on Ubiquitous Computing (UbiComp).

Haataja, K. (2005). *Two practical attacks against Bluetooth security using new enhanced implementations of security analysis tools.* Paper presented at the IASTED International Conference on Communication, Network and Information Security (CNIS 2005), Phoenix, Arizona, USA.

Herfurt, M., & Mulliner, C. (2004). Remote device identification based on Bluetooth fingerprinting techniques. *Trifinite Group, White Paper*.

Huang, J., Albazrqaoe, W., & Xing, G. (2014). *BlueID: A practical system for Bluetooth device identification.* Paper presented at the IEEE INFOCOM 2014.

IEEE. (2004). IEEE 802.15 WPAN Task Group 1 (TG1). Retrieved from http://www.ieee802.org/15/pub/TG1.html

Jappinen, P., Laakkonen, I., Latva, V., & Hamalainen, A. (2004). Bluetooth device surveillance and its implications. *WSEAS Transactions on Information Science and Applications, 1*(4).

Marks, R. B., Gifford, I. C., & O'Hara, B. (2001). Standards in IEEE 802 unleash the wireless Internet. *IEEE microwave Magazine, 2*(2), 46-56.

Patil, B. (2003). *IP in Wireless Networks*: Prentice Hall Professional.

PCM. (2015). Frontline Test Equipment FTS4BT BLUETOOTH PROTOCOL ANALYZER & PACKET SNIFFER (FTSBLUE-2YR). Retrieved from http://www.pcm.com/p/Frontline-Test-Equipment-Utilities-Software/product~dpno~7121202~pdp.diiddeh

Pels, M., Barhorst, J., Michels, M., Hobo, R., & Barendse, J. (2005). Tracking people using Bluetooth–Implications of enabling Bluetooth discoverable mode. *Final report, University of Amsterdam*.

Polak, A. C., Dolatshahi, S., & Goeckel, D. L. (2011). Identifying wireless users via transmitter imperfections. *Selected Areas in Communications, IEEE Journal on, 29*(7), 1469-1479.

SparkFun. (2015). HackRF One. Retrieved from https://www.sparkfun.com/products/13001

Spill, D., & Bittau, A. (2007). BlueSniff: Eve Meets Alice and Bluetooth. *WOOT, 7*, 1-10.

Ureten, O., & Serinken, N. (2007). Wireless security through RF fingerprinting. *Electrical and Computer Engineering, Canadian Journal of, 32*(1), 27-33.

Van Londersele, B., Delafontaine, M., & Van de Weghe, N. (2009). Bluetooth tracking: A spy in your pocket. *GIM International, 23*(11), 23-25.

Wexler, J. (2007). Cisco grabs leading spectrum analysis company. Retrieved from http://www.networkworld.com/article/2285880/network-security/cisco-grabs-leading-spectrum-analysis-company.html

Whitehouse, O. (2003). *War nibbling: Bluetooth insecurity*.

Xu, Q., Zheng, R., Saad, W., & Han, Z. (2015). Device Fingerprinting in Wireless Networks: Challenges and Opportunities. *arXiv preprint arXiv:1501.01367*.

Yermalkar, S. D. (2012). Bluetooth Reconnaissance: Watching Over Invisible. Retrieved from http://www.chmag.in/article/oct2012/bluetooth-reconnaissance-watching-over-invisible