How Much Privacy Does $3,165 Buy You?
A Critical Look At Private IEEE Address Allocation Registration

Jeremy Martin[†*], Dane Brown[†], Kris Merrion[*], Lamont Brown[†], and Travis Mayberry[†]
[†]United States Naval Academy, Email: {jmartin, dabrown, m180636, mayberry}@usna.edu
[*]Center for Measurement and Analysis of Network Data

***Abstract*—Security and privacy are frequently linked for good reason; the more specific information an attacker can gather regarding a person or organization, the more devastating or surgical a targeted attack can be. Armed with this knowledge, many individuals and organizations focus too heavily on protecting privacy while under-emphasizing or entirely neglecting actions which will actually make their systems more secure, a practice known as *Security through Obscurity*. Such is the case with the Institute of Electrical and Electronics Engineers (IEEE) practice of selling *private* Organizationally Unique Identifier (OUI) registrations to companies. This feature hides the name and personal information of the company that owns an address block in the IEEE public registry. In this paper, we track the adoption of *private* address allocation over time and attempt to unmask some of the companies behind this veil. We perform a cursory assessment of collected unencrypted frames transmitted by the devices implementing this practice. We identify that ∼86% of observed devices reveal their associated provenance through the content of their unencrypted transmissions, thereby rendering the privacy protection moot. Furthermore, we posit that the practice itself is flawed, inherently drawing unnecessary attention by the public nature of IEEE allocations. Our research reveals the ownership details of private addresses used by critical law enforcement, emergency services, and a variety of physical security systems. The results of our findings have been disclosed with the goal of raising awareness of companies and consumers using products with unsubstantiated security guarantees.**

I. Introduction

Wireless-enabled devices are utilized for personal, commercial, government, and industrial applications. WiFi and Bluetooth-capable devices continue to grow in breadth and scope across an increasingly diverse Internet of Things (IoT) landscape [1], resulting in the parallel rise in associated security and privacy risks. Industry, academia, and government agencies have devoted immense resources towards securing this vast interconnected network of devices [2]–[4].

One such strategy, *Security Through Obscurity*, attempts to provide security or privacy by obfuscating traffic, device hardware or software information, or system designs. Such implementations rely on the premise that concealing or obscuring how a system is designed, or how it operates, provides enough ambiguity that an attack will be thwarted. As such, security through obscurity techniques are not designed to eliminate attacks or correct inherent vulnerabilities of a system. Debates on the intrinsic value of such implementations often include ridicule [5] and criticism [6], while others provide a balanced assessment [7].

In this paper, we explore a method of obfuscation offered by the IEEE in an attempt to implement privacy countermeasures. Specifically, the countermeasure is designed to prevent the trivial identification of a wireless device's manufacturer from its observed Media Access Control (MAC) address.

Preparations for network attacks commonly focus on the identification and enumeration of accessible hosts [8]. There exist both passive *sniffing* and a range of active techniques for exposing and eliciting granular device details such as the manufacturer, model, Operating System (OS), and running services. These details are integral pieces of information towards identifying vulnerabilities and executing targeted attacks.

Discovery that a specific manufacturer or model type is within observable range is all that is required to launch a variety of attacks [9]–[11]. The aforementioned Denial-of-Service (DoS) attacks specifically target Google Glass devices, WiFi-enabled Drones, and various surveillance camera manufacturers, initiated solely by the identification of the device MAC address. By matching a MAC address prefix, previously correlated to that of the targeted device type, an attacker simply listens for 802.11 frames matching the prefix and then launches the desired attack.

The fundamental catalyst for launching these attacks is the hardware identifier known as a MAC address. Every 802.11, 802.15, and Ethernet Network Interface Card (NIC) has a 48-bit layer-2 MAC address that uniquely identifies the wireless/wired radio. Significant research has been dedicated to the privacy concern related to wireless device tracking utilizing the globally unique MAC address [12]–[20].

The three byte prefix of a MAC address, commonly referred to as the OUI, is allocated by the IEEE to wireless device and hardware manufacturers [21]. The IEEE maintains a registry of all OUIs that have been purchased, providing a simple method for identifying the manufacturer of a wireless device by the associated prefix. Previously, further resolving the granular device model details from a MAC address was not possible, however Martin et. al. [22] illustrate multiple techniques to infer the device model from a MAC address. They decompose the MAC address structure of observed devices in order to build a capability in which a single wireless frame can elucidate a specific device model. The authors perform this granular MAC address decomposition by deriving manufacturer and model device details from: i) management frame Wi-Fi Protected Setup (WPS) data fields; and ii) discovery protocols such as multicast Domain Name System (mDNS).

The IEEE, in an effort to *obscure* the manufacturer ownership details, offers to list an OUI allocation as *private*, removing the company name and address from the listing [23]. This privacy motivated obfuscation is available for an additional registration and recurring annual fee of $3,165.

Naturally, we ask the question, how effective is this implementation of security through obscurity? We find that in practice this obfuscation method is fundamentally flawed, as it elicits unnecessary attention to an OUI. Quite simply, it serves to *alert* would be adversaries that a potentially sensitive device has attempted to hide from plain sight. Our analysis begins with this simple assumption which provides the starting point for our research. In this paper, we introduce targeted research efforts towards identifying the manufacturer, model, and category of devices with address blocks registered using the *private* nomenclature in the publicly available IEEE database.

We borrow from the techniques described in previous model inference research [16], [22] by extracting device details from 802.11 and 802.15 frames during network discovery as well as application and data-link discovery protocols.

Alarmingly, we show that in 18 of 21 instances in which we collected unencrypted frames we are able to reveal the manufacturer and model associations. Surprisingly, many of the revealed devices are in generally non-interesting categories such as mobile phones, mid-level branded tablets, mobile hotspots, and routers. However, we also uncover a group of more sensitive products. For example, we uncover a brand of biometric access control devices used for physical security systems. Additionally, we reveal that one allocated address block represents network-enabled camera and security systems. Finally we identify two address allocations owned by two separate companies that provide equipment utilized by local law enforcement and emergency services personnel. Due to the inherent personal security risks identified by the identification of the law enforcement devices we chose to disclose the findings prior to publication submission. These privacy and security implications highlight the impact of our findings, which is further amplified by the simplicity of our methodology.

Our contributions are as follows:

- We reveal the unintended information leakage flaw of listing a conspicuous minority of address blocks allocations as *private* within a public database.
- We highlight the fact that continued disclosure of granular device information derived from management frames during network scanning operations remains a privacy concern. We further call attention to the unintended privacy consequences of employing discovery protocols on an unencrypted wireless network.
- We systematically uncover the identity of sensitive and potentially critical systems and disclose our findings to respective entities.
- We provide recommendations for improving the IEEE allocation process.

II. Background

The 48-bit scheme of uniquely identifying devices under the IEEE 802 authority originated with Block Identifiers assigned by the Xerox Corporation during their early work with Ethernet. These Block Identifiers were identical in format to the MAC addresses seen today, where the first 24 bits universally identify a vendor and the last 24 bits uniquely identify a device sold by that vendor. The IEEE, while working to standardize Local Area Network (LAN) protocols, assumed responsibility for the universal addressing of devices under its Registration Authority Committee. The IEEE renamed Block Identifiers to OUIs, but maintained the existing allocations made by Xerox [24].

In recent years, the IEEE has expanded on the capabilities of the MAC address to meet the diverse needs of the modern marketplace and to more efficiently allocate the finite address space. The Extended Unique Identifier (EUI)-48 encompasses the traditional 48-bit identification of networked hardware as well as the unique identification of products that are not necessarily networked devices [25], [26]. The EUI-48 provides finer granularity on allocation of addresses by allowing organizations to choose MAC Address Block Large (MA-L), MAC Address Block Medium (MA-M), or MAC Address Block Small (MA-S) assignments in accordance with their needs.

The MA-L grants an organization a traditional 24-bit OUI with a 24-bit extension identifier, which can uniquely assign over 16 million devices. The MA-M grants a 28-bit organizational prefix with a 20-bit extension identifier, which can assign just over one million devices. Finally, a small company may opt for a MA-S which grants a 36-bit organizational prefix with a 12-bit extension identifier, allowing for just over four thousand product assignments.

The IEEE further encourages efficient use of EUI spaces by requiring a current EUI holder to utilize 95% of their allocation prior to applying for an additional EUI. For applications requiring more extensive addressing needs, the EUI-64 is an extension of the EUI-48 to 64 bits. All MA-L, MA-M, and MA-S prefixes are identical to the EUI-48 versions, just with longer extension identifiers. Current applications which derive addresses from EUI-64 include IPv6 [27] and Universally Unique IDentifiers (UUIDs) [26], [28].

One feature provided by the IEEE Registration Authority which deserves more attention is the *private* OUI. For a hefty additional, annual fee, this gives an organization the option to conceal its identity on the IEEE OUI listing, which is public by default [21]. The IEEE began to charge for this privacy service in December of 2003. In the time since, only a small fraction of customers have actually opted to pay for the concealment.

We were able to extract the number of *private* registrations over time based on historic snapshots of the IEEE OUI list maintained by the Wireshark project [29]. These snapshots go back to 2009, and even though the IEEE began offering the MA-M and MA-S in January of 2014, these services were not differentiated in the Wireshark database until well into 2015.

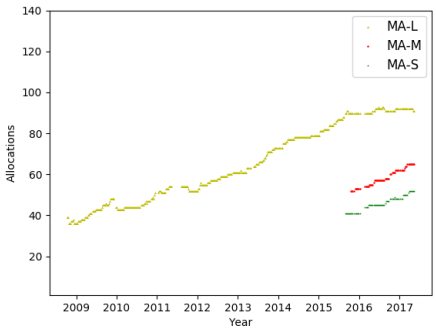

Fig. 1. *Private* Allocation Over Time [31]

As shown in Figure 1, the number of private registrations has steadily, but slowly increased since the offering. At present, approximately 200 of ∼32,000 prefix allocations have opted for *private* registration. Compare this to private or proxied Domain Name System (DNS) domain registration, which boasts an 18% share of total domain registrations (an estimated 18 million private registrations as of 2010) [30], and it becomes clear that the market as a whole places relatively little value in OUI privacy. We explore this further in Section III.

In this paper, we critically examine the secrecy provided by *private* OUIs by studying plain-text communications and other publicly available meta-data. This is not, however, the first time meta-data has leaked information that was intended to remain private. Information leaks are so commonly observed in applications, especially connected mobile applications, that "There's an app for that!" [32] Communications are bound to leak data, this is even more likely in an open, decentralized environment, like the Internet, where no one entity fully controls every aspect [33]. A commonly known example of this is leakage via request headers in Hypertext Transfer Protocol (HTTP) packets. Web servers need very little information about a browser in order to deliver an appropriate web page. However, HTTP request headers, in the form of user-agent strings, are loaded with superfluous information that are designed to help uniquely identify the connected client to the web server. This includes details of the operating system and version, the browser and version, installed plugins and fonts, cookies, language, referrer, and more [34]. This is before even considering dynamic forms of leakage and tracking, such as JavaScript, Adobe Flash, or Java applets.

Our methods, illustrated in Table I reveal information that is likely intended to remain private in much the same way. Data found in 802.11 management frames, such as Service Set IDentifiers (SSIDs) and WPS attributes, and data frames used for discovery protocols like mDNS are just as useful for identifying and tracking mobile devices as HTTP request headers are for identifying and tracking web clients. One item sometimes found in management frames is WPS data. WPS is a protocol created by the Wi-Fi Alliance to simplify the process of setting up and connecting to access points (APs) securely. This is done by allowing the user to provide

TABLE I
EXAMPLE - LEAKED DEVICE INFORMATION

Data Source	Leaked Details
SSID	Audi MMI
WPS	Motorola Nexus 6
mDNS	Samsung SM-G930AZ
HTTP	iPhone OS-9.3.1

some initiation signal (i.e. push button or PIN entry), then performing an exchange of credentials between the client and the AP without user intervention. Unfortunately, this convenience comes with drawbacks; in order for devices to identify each other without human interaction, they must transmit the required identifying information. Client devices that support WPS send data in additional Information Elements (IEs), frequently contain manufacturer and model information as well as enough information to uniquely identify and track the device [22].

Discovery protocols such as mDNS, Link-Local Multicast Name Resolution (LLMNR), and NetBIOS are present in client-based IEEE 802.11 data frames. Their main purpose is for advertising network services and capabilities through Domain Name System-Based Service Discovery (DNS-SD), thus making it feasible to use zero configuration protocols [35]. However, a significant drawback to the family of Zeroconf protocols is the inherent advertisement of granular manufacturer, model, and OS details. When client devices establish network connections on an unencrypted network the resulting automatic data traffic announces the device characteristics to anyone within range [16], [22].

Other protocols within the IEEE 802 family are prone to the same information leakage issues. Blutetooth, an 802.15 protocol, also utilizes EUI-48 addressing. When passively monitoring Bluetooth communication, it is possible to glean identifiable and trackable information from hostnames derived from plain-text packets.

III. METHODOLOGY

We set out to determine, through empirical data analysis of historical wireless collection, whether the *private* OUI service, provided by the IEEE Registration Authority, could be bypassed through passive collection. If so, there could be devastating consequences for organizations and end users relying upon that privacy for safety-critical or financial applications. It bears mentioning that this dataset of wireless collection was produced separately from our research efforts, further emphasizing the ease with which these techniques can be reproduced and expanded towards a targeted de-privatization effort.

Over the course of approximately two years, we captured unencrypted 802.11 device traffic using inexpensive commodity hardware and open-source software. We primarily used an LG Nexus 5 Android phone running Kismet *PcapCapture* paired with an AWUS036H 802.11b/g Alfa card. We hopped between the 2.4GHz channels 1, 6, and 11 to maximize coverage and employed several Raspberry Pi devices run-

ning Kismet with individual wireless cards each dedicated to channels 1, 6, and 11. Our collection effort spanned January 2015 to May 2017 and encompassed approximately 9,100 individual packet captures. The collection contained over 700 gigabytes (GBs) of 802.11 traffic, consisting of over 2.8 million unique devices. We then supplemented our 802.11 collection by retrieving the high-level metadata obtained via the publicly available online repository Wireless Geographic Logging Engine (WiGLE) [36]. Additionally, we captured unencrypted 802.15 Bluetooth device traffic using Sena Perani-UD100 USB adapters. Our dataset includes approximately 460 megabytes (MBs) of Bluetooth data and 137 individual packet captures.

A. Ethical Considerations

Our collection methodology is entirely passive. At no time do we attempt to decrypt any data, inject data, or alter normal network behavior while outside of our lab environment. Our intent is to show the ease with which one can build this capability with low-cost, off-the-shelf equipment. However, given the nature of our data collection, we consulted with our Institutional Review Board (IRB).

The primary concerns of the IRB centered on: i) the information collected; and ii) whether the experiment collects data "about whom" or "about what." Because we limit our analysis to 802.11 management frames and unencrypted data packets, we do not observe Personally Identifiable Information (PII). Although we observe IP addresses, our experiment does not use these layer-3 addresses. Even with an IP address, we have no reasonable way to map the address to an individual. Further, humans are incidental to our experimentation as our interest is in the manufacturer and model of the wireless device, derived from the layer-2 MAC addresses, or "what." Again, we have no way to map MAC addresses to individuals.

Finally, in consideration of beneficence and respect for persons, our work presents no expectation of harm, while the concomitant opportunity for network measurement and security provides a societal benefit. Our experiment was therefore determined to not be human subject research.

Due to the inherent privacy concerns related to this work, further impacted by the identification of law enforcement, emergency services, and a variety of access control and physical security devices we have chosen not to list the specific privately allocated prefixes nor the individual manufacturer and model information. We have worked with local law enforcement towards identifying a suitable solution.

B. Traffic Analysis

An overview of our findings is provided in Table II detailing each prefix and associated vulnerability observed in our datasets. It should be noted that the identified vulnerabilities are representative of the *in-the-wild* collection observations. We expect that additional vulnerabilities exist for the identified prefixes and likely for those not seen in our dataset. The simplicity with which we were able to extract associated device details should serve to emphasize the flaws in the IEEE's obscurity implementation. Furthermore, it highlights the more troubling concern that some manufacturers who chose to pay for obscurity fail to perform due diligence on software protocol design, inherently leaking critical granular details.

We begin our analysis by first reducing our WiFi corpus to include only unencrypted frames which contain privately allocated MAC addresses. From this merged subset of packet captures, we create individual capture files for each observed *private* prefix which allows us to obtain 21 unique files ($\sim$1.4GB), representing 21 *private* prefixes: 17 MA-L, three MA-M, and one MA-S. We systematically retrieve identifying information such as manufacturer, model, device nomenclature, operating system, and firmware using the following techniques previously described in Section II.

Table I highlights an exemplar case, the observed SSID indicates that the device belongs to an Audi vehicle's multimedia and navigation system. Six devices using private OUIs, leaked manufacturer and model information within their SSIDs name construct. As shown in Table II, detailed SSID-derived model information revealed emergency services related infrastructure as well as a variety of network connectivity devices such as APs, mobile hotspots, and client devices operating in hotspot mode.

Seven prefixes advertised WPS Information Elements when transmitting beacon, probe request, or probe response management frames, of which six provided detailed manufacturer and model information. Five of theses prefixes are tablet devices while the sixth is the aforementioned mobile hotspot designation derived from SSID analysis. A seventh prefix, typically contained blank WPS data attributes, however we occasionally observed WPS-derived manufacturer details indicating that these devices have improperly allocated addresses whereby the manufacturer has not followed the prescribed assignment policies for an MA-M block and instead has treated its prefix as if it was an MA-L. We draw this conclusion based on the observation that the identified manufacturer owns a publicly allocated block in close proximity to that of the MA-M. Due to the nature of the IEEE's randomly chosen assignment of prefixes, and specifically the inherently unlikely use of multiple contiguous MA-M blocks by a single manufacturer, it is unlikely that the observed WPS devices are associated with the privately listed block.

After reviewing the management frames, we proceed to inspect the unencrypted data frames for similar manufacturer and model attributes. We observe 12 prefixes transmit granular manufacturer and model characteristics allowing us to infer the prefix owner. We find that the tablet devices are particularly *noisy* while performing service discovery actions. Of note are two access control related prefixes; a manufacturer of biometric and physical security systems as well as a video surveillance company.

We then follow-up our analysis by retrieving from the public repository WiGLE [36], all datasets that contain a privately listed prefix. We inspect only the SSID fields, as this dataset contains limited attributes of use. From the observed SSIDs,

TABLE II
DEPRIVATIZED OUIS - COMPANY NAMES WITHHELD DUE TO RESPECT FOR PRIVACY CONCERNS

Prefix	Device Category	Data Source						
		WiFi (SSID)	WiFi (WPS)	WiFi (Data)	Bluetooth	WiGLE	IEEE	Confirmed
MA-L [a]	Mapping and Navigation Systems			✓	✓		✓	✓
MA-L	Law Enforcement					✓		✓
MA-S	Emergency Services	✓				✓		✓
MA-L	Access Control/Biometrics			✓			✓	✓
MA-L	Video Surveillance			✓				✓
MA-L	Access Point	✓				✓	✓	✓
MA-L	Printer			✓				
MA-L	Mobile Hotspot	✓	✓			✓		
MA-L	Proprietary Hardware/Protocol			✓				✓
MA-L	Mobility Support	✓				✓		
MA-L	Smart Phone	✓				✓		✓
MA-L	Tablet		✓	✓		✓		✓
MA-L	Tablet		✓			✓		✓
MA-L	Tablet		✓	✓	✓			✓
MA-L	Tablet	✓	✓	✓	✓			✓
MA-L	Tablet			✓				✓
MA-L	Tablet			✓				✓
MA-L	Tablet			✓				✓
MA-L	Tablet		✓	✓	✓			✓
MA-M [b]	Unknown							n/a
MA-M [c]	Unknown		✓					n/a
MA-M	Unknown							n/a

[a]The Garmin prefix allocated as Private for approximately 14 years has been removed from the *private* listing as of May 2017
[b]One frame observed in entire dataset
[c]Device assessed to be misused allocation

we corroborate the previous analysis of seven prefixes and identify one additional MA-L block. The newly identified prefix, related to devices operated by law enforcement entities was observed for 115 unique devices within the WiGLE dataset. This was particularly interesting as we never observed this address block in our corpus. After further review, we conclude that this was due to our dataset including only 2.4 GHz collection whereas the devices associated with this prefix are predominately transmitting on the 5GHz bands. To highlight the observations of the identified law enforcement devices we provide a geographical plot of the observed devices in Figure 2 [36].

Next we repeat the process for Bluetooth by creating individual packet capture files as previously defined. The resulting output, while minimal ($\sim$ 300 kilobytes (KBs)), identified four prefixes, all of which transmitted manufacturer and model details. The associated manufacturers for all four prefixes were consistent with the details derived from 802.11 analysis. Of note, the mapping and navigation-based device prefix has recently been publicly allocated after 14 years as a privately listed assignment, confirming our analysis that the OUI is owned by Garmin.

Lastly, we review the entire history of the Wireshark maintained `manuf` file used when performing name resolution for packet analysis [31]. Specifically, we examine instances where an OUI or prefix was temporarily publicly listed prior to a *private* allocation. We find two cases where a prefix was listed for a minimum of 12 months prior to becoming privately listed. In both cases we confirm our assumptions from packet analysis.

Using the `manuf` file, we identify that in addition to the previously mentioned Garmin prefix, two OUIs have transitioned from *private* to public since 2016 [31]. In each case the *private* listing was removed on the same date the public listing was made available.

Fig. 2. WiGLE-based Collection of Law Enforcement Devices [36]

C. Confirmation of Analysis

We attempt to provide confirmation of our assessments in Section III-B in the following ways: i) visual correlation via device settings, ii) visual correlation via affixed device label, iii) packet capture of device in lab environment, and iv) manufacturer produced reference manuals. For each assessment we confirm the manufacturer and device type, however, out of respect for the owners of the address blocks as well as the IEEE, we chose to list only the device category within our findings.

As depicted in Table II we make assessments for 19 of the 22 identified prefixes, of which we positively confirm 16 using the aforementioned confirmation techniques.

IV. Conclusions

We systematically decomposed historical 802.11 and 802.15 wireless packet captures, identifying the ownership and granular model details for 19 of the 22 *private* address blocks observed. We substantiated 16 for an ∼84% confirmation rate, with no false positives, all while performing no new collection to obtain additional prefixes of interest. As such, we posit that a sustained collection effort against devices listed as *private* will achieve a similar rate of success using our methodologies for device identification for a larger number of prefixes.

We found that the IEEE *private* registration implementation is fundamentally flawed and acts as a catalyst to spotlight a variety of manufacturer and OS privacy failures. Specifically, public listing of *private* allocations creates an enticing *Target Set* for would be attackers. When prepared with a focused list of potentially interesting targets, we found that the lack of due diligence in hardening the network and service discovery protocols serves to enumerate the *private* namespace, requiring little work by the attacker.

In an effort to improve upon the desired goal of obscuring the provenance of hardware we suggest the following:

1) We recommend that all future address allocations remain known only to the IEEE, inherently making all allocations private.
2) Encourage the use of MAC randomization for client devices while in an unassociated state.
3) Devices should not have SSID or hostnames that indicate manufacturer, model, or device information.
4) Device manufacturers should commit to removing granular details from network discovery [37] and service discovery protocols.
5) Proprietary data protocols should be encrypted, limiting the ability to infer the device type due to observation of unique protocol traffic.

V. Acknowledgments

We thank Erik C. Rye, Lucas Foppe, and Collin Donahue for early feedback and contributions. Views and conclusions are those of the authors and should not be interpreted as representing the official policies or position of the U.S. government.

References

[1] "Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated," http://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated, 2013.

[2] P. Levis, "Secure Internet of Things Project (SITP)," http://iot.stanford.edu/workshop14/SITP-8-11-14-Levis.pdf, Secure Internet of Things Project Workshop, Stanford University, Aug. 2014.

[3] US DHS, "Strategic Principles For Securing The Internet Of Things (IoT)," https://www.dhs.gov/securingtheIoT, Nov. 2016.

[4] R. H. Weber, "Internet of things–new security and privacy challenges," *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[5] "Why Security Through Obscurity Isnt," http://www.treachery.net/articles_papers/tutorials/why_security_through_obscurity_isnt/Security_Through_Obscurity_Isnt.pdf, 2001.

[6] S. M. Bellovin and R. Bush, "Security Through Obscurity Considered Dangerous," 2002.

[7] J. M. Johansson and R. Grimes, "The Great Debate: Security by Obscurity," https://technet.microsoft.com/en-us/library/2008.06.obscurity.aspx, June 2008.

[8] root9B, "Hacker Methodology," http://www.nibs.org/resource/resmgr/Conference2014/BI20140106_CS_Morris.pdf, 2014.

[9] J. Oliver, "glasshole.sh," Jul. 2014, https://julianoliver.com/output/log_2014-05-30_20-52.

[10] J. Oliver, "Cyborgunplug," Mar. 2016, https://github.com/JulianOliver/CyborgUnplug.

[11] S. Kamkar, "Skyjack," Dec. 2013, https://github.com/samyk/skyjack.

[12] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, and D. Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting."

[13] A. B. M. Musa and J. Eriksson, "Tracking Unmodified Smartphones Using Wi-fi Monitors," ser. SenSys '12.

[14] M. Cunche, "I Know Your MAC address: Targeted Tracking of Individual Using Wi-Fi," *Journal of Computer Virology and Hacking Techniques*, 2014.

[15] A. Musa and J. Eriksson, "Tracking Unmodified Smartphones Using Wi-Fi Monitors," in *Proceedings of the 10th ACM conference on embedded network sensor systems*. ACM, 2012, pp. 281–294.

[16] J. Martin, D. Rhame, R. Beverly, and J. McEachen, "Correlating GSM and 802.11 Hardware Identifiers," in *IEEE MILCOM*, 2013.

[17] J. Franklin, D. McCoy, P. Tabriz, V. Neagoe, J. V. Randwyk, and D. Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting," in *Proc. 15th USENIX Security Symposium*, 2006.

[18] M. Vanhoef, C. Matte, M. Cunche, L. Cardoso, and F. Piessens, "Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms," in *ACM AsiaCCS*, 2016.

[19] C. Matte, M. Cunche, F. Rousseau, and M. Vanhoef, "Defeating MAC Address Randomization Through Timing Attacks," in *Proceedings of the 9th ACM Conference on Security; Privacy in Wireless and Mobile Networks*, ser. WiSec '16. ACM, 2016, pp. 15–20.

[20] J. Martin, T. Mayberry, C. Donahue, L. Foppe, L. Brown, C. Riggins, E. C. Rye, and D. Brown, "A Study of MAC Address Randomization in Mobile Devices and When it Fails," *Proceedings on Privacy Enhancing Technologies, 2017(4), pp. 268-286.*, 2017.

[21] "OUI Listing," http://standards.ieee.org/develop/regauth/oui/oui.txt.

[22] J. Martin, E. Rye, and R. Beverly, "Decomposition of MAC Address Structure for Granular Device Inference," in *ACSAC 2016*, pp. 78–88.

[23] "IEEE Registration Authority," http://standards.ieee.org/develop/regauth/oui/.

[24] "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture," http://standards.ieee.org/getieee802/802.html.

[25] I. S. Association, "Guidelines for 48-Bit Global Identifier (EUI-48)," https://standards.ieee.org/develop/regauth/tut/eui48.pdf.

[26] IEEE Standards Association, "Guidelines for 64-Bit Global Identifier (EUI-64)," https://standards.ieee.org/develop/regauth/tut/eui64.pdf.

[27] R. Hinden and S. Deering, "RFC 4291: IP Version 6 Addressing Structure," 2006.

[28] P. Leach, M. Mealling, and R. Salz, "RFC 4122: A Universally Unique IDentifier (UUID) URN Namespace, 2005," vol. 4, 2013.

[29] "The wireshark project," http://www.wireshark.org/.

[30] "ICANN Study on the Prevalence of Domain Names Registered using a Privacy or Proxy Service among the top 5 gTLDs," https://www.icann.org/en/system/files/newsletters/privacy-proxy-registration-services-study-14sep10-en.pdf, Sep 2010.

[31] Wireshark, "Wireshark git repo," https://code.wireshark.org/review/gitweb?p=wireshark.git;a=history;f=manuf;h=1e5c26880c85384f980aa8f96712962f3711094e;hb=HEAD.

[32] Z. Yang and M. Yang, "Leakminer: Detect Information Leakage on Android With Static Taint Analysis," in *Software Engineering (WCSE), 2012 Third World Congress on*. IEEE, 2012, pp. 101–104.

[33] B. Greschbach, G. Kreitz, and S. Buchegger, "The devil is in the metadata - New Privacy Challenges in Decentralised Online Social Networks," in *2012 IEEE conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*.

[34] P. Eckersley, "How unique is your web browser?" in *International Symposium on Privacy Enhancing Technologies Symposium*. Springer, 2010, pp. 1–18.

[35] S. Cheshire and M. Krochmal, "Dns-based service discovery," Tech. Rep., 2013.

[36] "WiGLE (Wireless Geographic Logging Engine)," May 2017, https://wigle.net/.

[37] "Changes to Device Identifiers in Android O," https://android-developers.googleblog.com/2017/04/changes-to-device-identifiers-in.html.