Large Scale Wi-Fi tracking using a Botnet of Wireless Routers

Pierre Rouveyrol, Patrice Raveneau, Mathieu Cunche

Large Scale Wi-Fi tracking using a Botnet of Wireless Routers

Pierre Rouveyrol
Inria
Grenoble, France
pierre.rouveyrol@inria.fr

Patrice Raveneau*
University of Lyon
Inria, CITI Lab
Lyon, France
patrice.raveneau@inria.fr

Mathieu Cunche
University of Lyon
Inria, CITI Lab.
Lyon, France
mathieu.cunche@inria.fr

ABSTRACT

Wi-Fi tracking is a method relying on signals emitted by portable devices to track individuals for commercial, security or surveillance purposes. Wi-Fi tracking has the potential to passively track a large fraction of the population [12] and is therefore an ideal population surveillance technology and a serious privacy threat. We argue that Wi-Fi routers make an ideal building block to create a large scale Wi-Fi tracking system. This paper first presents the interesting features of Wi-Fi routers for tracking and describes how they can be easily turned into Wi-Fi tracking devices through software modification. We then introduce the concept of a large scale Wi-Fi tracking system based on routers and we propose a design for such a system, including stealth communications and deployment. Finally we provide a first evaluation of the tracking capabilities of an hypothetical Wi-Fi tracking system through a set of simulations based on real-world datasets. Results show that the spatial distribution of Wi-Fi routers is such that compromising even a small fraction of Wi-Fi routers is sufficient to track people for a large fraction of the time.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection - Invasive software (e.g., viruses, worms, Trojan horses); K.4.1 [**Computers and Society**]: Public Policy Issues - Privacy

General Terms

Security

Keywords

Wi-Fi; surveillance; botnet; malware

*This work was supported by the LABEX IMU (ANR-10-LABX-0088) of Université de Lyon, within the program "Investissements d'Avenir" (ANR-11-IDEX-0007) operated by the French National Research Agency (ANR).

1. INTRODUCTION

Wi-Fi tracking is a technique that passively tracks individuals in the physical world by collecting identifiers periodically broadcast in cleartext by their Wi-Fi-enabled devices. It is used by commercial entities to track and profile customers, but it can also be used for security or surveillance purposes. Wi-Fi tracking has the potential to affect a large fraction of the population [12] and because of its passive nature, it is virtually impossible to detect. It is therefore an ideal population surveillance technology and a serious privacy threat. Military and surveillance agencies have started to exploit this technology [14], and the MAC address, the identifier used in Wi-Fi tracking, is one of the *selectors* used by the NSA[1]. IMSI-catchers [15] is another technology that can be used for identification and tracking of mobile phone owners. By mimicking cellular base stations, IMSI-catchers are able to collect mobile phone identifiers. However, as opposed to Wi-Fi tracking, cellular tracking technologies like IMSI-catchers are much more complex and costly to set-up and they can be easily detected[2].

Wi-Fi connectivity is in general provided by Wi-Fi routers. Those devices have become ubiquitous as they can be found in most homes, offices and public places. We argue that those already deployed Wi-Fi routers can be used to create a large scale Wi-Fi surveillance system. They embed the required hardware to monitor Wi-Fi channels and, by being connected to the Internet, they can easily report collected data. Through a proof-of-concept, we show that simple software modifications are enough to turn a Wi-Fi router into a Wi-Fi tracking device. We propose a design and the deployment of such a tracking system based on a botnet of Wi-Fi routers. The tracking potential of this system is then evaluated, first by discussing the spatial distribution of those Wi-Fi routers, then by simulating the reconstruction of mobility traces of a smartphone owner.

The paper is organized as follow. Section 2 introduces background and related work. Section 3 presents the suitable features of Wi-Fi routers highlighted with a proof-of-concept. The design of the router-based Wi-Fi tracking system is presented in section 4. Section 5 presents an evaluation of the tracking potential. Section 6 concludes the discussion.

[1] http://cryptome.org/2014/03/nsa-selector.pdf
[2] https://opensource.srlabs.de/projects/snoopsnitch

2. BACKGROUND AND RELATED WORKS

2.1 Wi-Fi tracking

Devices with an enabled Wi-Fi interface periodically broadcast (every 20-30 seconds) frames containing a unique identifier (the MAC address) even when they are not connected to a Wi-Fi network. This is caused by the active service discovery mechanism that requires Wi-Fi stations to send probe request frames in order to discover surrounding Access Points (APs).

As a consequence, Wi-Fi-enabled devices such as smartphones act as portable beacons, and it is trivial to track the device and its owner by collecting information available on Wi-Fi channels. This technique is already used by retail stores to implement physical analytics and advertisement campaigns [4]. It can also be used by any curious eavesdropper such as a criminal organization or a surveillance agency. In fact there are indications that surveillance agencies are already using Wi-Fi tracking [14].

By passively collecting signals emitted by most portable devices, Wi-Fi tracking systems can monitor the whereabouts of a large part of the population without being dectected. Those systems therefore represent a serious privacy threat and can be used as a powerful surveillance tool.

2.2 Wi-Fi routers

Wi-Fi routers (sometimes called Wireless routers) are embedded devices implementing a Wi-Fi AP as well as network routing functionalities. They can include a modem to connect to the Internet through ADSL or FTTH. Wi-Fi routers can be either owned by the customer or lent by the ISP to the customer. In the latter case, those devices have generally advanced functionalities and can be remotely updated by the ISP, whereas Wi-Fi routers owned by customers are rarely updated [13, 9]. Wi-Fi routers are the core element to provide Wi-Fi connectivity either in home, office or public places. As of today there are more than 450 million wireless routers deployed worldwide[3].

From a technical point of view, Wi-Fi routers could be considered as lightweight computers. Built around embedded processors using MIPS or ARM architectures seconded by a RAM of moderate size (generally around 32MB but sometimes up to 256MB and more), they are surrounded by multiple chipsets enabling network interfaces (Ethernet, ADSL and DOCSIS), most importantly a Wi-Fi interface. This Wi-Fi interface is built around a dedicated chipset which is coupled with one or several high gain antenna(s) in order to provide a good quality of service. They run Linux or BSD systems that have been customized for the specific needs of Wi-Fi routers. The file system (usually SquashFS) is read-only (except for the /mnt and /tmp partitions), therefore one needs to extract then repackage it in order to do any persistent change to the OS.

This OS generally provides a number of network services like a Web interface, Telnet and serial for administration, as well as typical file sharing services like NFS, Samba and DLNA. This number of services coupled with the tendency of users not to update them make Wi-Fi routers potentially vulnerable targets.

[3] `http://www.fiercewireless.com/tech/story/strategy-analytics-counts-25-global-households-wi-fi-2014-methods-differ-ip/2014-11-06`

2.3 Wi-Fi Routers' Malware

Wireless routers are infamous for vulnerabilities that allow remote exploitation and infection by malware. Such malware can have the ability to infect routers remotely and to spread like worms [7]. Reports about discovered vulnerabilities periodically appear in the news [7]. To make things worse, Wi-Fi routers are not always up to date and are therefore vulnerable to attacks for a long period of time.

Piggybacking on those vulnerabilities and the propagation vectors, botnets composed of Wi-Fi routers have started to appear These botnets can be used for various tasks such as DDoS attacks, or to infect connected computers`https://nakedsecurity.sophos.com/2012/10/01/hacked-routers-brazil-vb2012/`.

2.4 Related work

Malware affecting Wi-Fi routers has been the object of multiple studies. In particular, [11] and [13] investigated the propagation of a theoretical malware program spreading over the wireless channels, demonstrating that wireless channels are an ideal medium for the propagation of router malware, especially in dense areas. These works only considered classical applications of botnets and did not identify the potential for Wi-Fi tracking.

Malware using wireless capabilities of the infected host to track surrounding devices has been theoretically considered in [10], but has also been discovered in the wild [6]. It has been reported [6] that the *Flame* malware, allegedly developed as an espionage tool, has the capabilities to use the Bluetooth interface of the infected host in order to track Bluetooth devices of nearby individuals. In [10], Husted et. al. introduce a network of infected mobile devices that combine geolocation and signals collected by the Wi-Fi interface in order to track individuals coming in range. Using mobile devices has the advantage to cover some areas that are exempt of Wi-Fi routers, but on the other hand it provides a poor coverage in areas with a poor density. Finally, as opposed to Wi-Fi routers, the embedded antenna of mobile devices will imply a shorter reception range [10], and monitoring capabilities of mobile devices can be difficult to activate[4].

3. WI-FI ROUTER AS A TRACKING DEVICE

3.1 Suitable features

Wi-Fi tracking systems can be built on top of any device capable of monitoring Wi-Fi channels and reporting information to a central entity. Monitoring the channel requires a Wi-Fi interface supporting *monitor mode*, and information reporting requires Internet connectivity. Devices fulfilling those requirements include: Wi-Fi routers, computers (laptops and desktop computers) as well as mobile devices (smartphones and tablets). In the following, we enumerate a

[4] `http://bcmon.blogspot.fr/`

number of features that make Wi-Fi routers ideal candidates for a Wi-Fi tracking system to be built upon.

Ever-connected and powered: Wi-Fi routers are generally working without discontinuation, allowing them to monitor Wi-Fi channels around the clock. As opposed to mobile devices that have to rely on a battery, they can rely on a virtually infinite amount of energy. This is useful in our case since a wireless interface in monitor mode consumes a significant amount of energy.

Internet connectivity & traffic relaying: Wireless routers are directly connected to the Internet through a wired infrastructure allowing high quality connectivity. They also relay traffic from associated station to Internet. This genuine traffic can be useful to cover the reporting traffic.

High gain antenna and Wi-Fi-enabled chipset: Wireless routers embed high gain antennas and radio transceivers that cannot be fitted into other appliances, especially mobile ones. Most of them embed Wi-Fi-enabled chipsets that support monitor mode with publicly available drivers. Finally monitor mode does not disrupt the network connectivity of the interface.

Vulnerability: Rarely updated, off-the-shelf Wi-Fi routers often have vulnerabilities that remain exploitable for a long time. Those vulnerabilities can be used to install malware on those devices.

Those characteristics make Wi-Fi routers suitable elements for a large scale Wi-Fi tracking system. As we will see in the following section, turning a Wi-Fi router into a Wi-Fi tracking device is not a complicated task. As a matter of fact, Wi-Fi infrastructure resellers, such as Cisco, are providing updates of their appliances that turn them into Wi-Fi tracking devices for physical analytics[5].

3.2 Proof-of-concept

To demonstrate the feasibility of turning a genuine wireless router into a Wi-Fi tracking node, we present a proof-of-concept. We show how the software of a wireless router can be modified to enable Wi-Fi tracking and reporting capabilities. This proof-of-concept concerns the *NeufBox_V4*, a wireless router provided by the French ISP SFR.

This router has been selected because its firmware has been made open-source, making its alteration easier. However, it is important to note that closed-source software may not be a limitation for an entity disposing of important resources. Indeed, it has been recently revealed that the firmware of hard drives has been subject to modification even if the software is supposed to be closed source [5].

The *NeufBox_V4*: As other commonly used routers, the *NeufBox_V4* is built around a BCM6358 chipset that integrates a 32bits MIPS processor at 300MHz as well as various interfaces such as an ADSL transceiver, and Ethernet interfaces. It is also equipped with 32 MB of RAM and 8MB of flash memory to store the OS. The Wi-Fi connectivity is provided by the BCM4318 wireless chipset. As many Wi-Fi routers, the *NeufBox_V4* runs a custom Linux operating system, and it can be replaced with any system that can be compiled for the MIPS32 architecture, such as OpenWRT, Tomato, PF-Sense or even Arch Linux.

OS modification and installation: In order to preserve the original functionality of the Wi-Fi router, we chose to install a modified version of the original operating system (OS). This original OS can be obtained in several ways; for instance by gaining root access on the device or by dumping the flash memory after desoldering it. But in our case, it was simpler to directly download the OS since it is open source[6]. The following modifications were made to the OS in order to enable the Wi-Fi tracking and reporting capabilities. The network analysis tool `tcpdump` was added to allow the collection of useful data from the Wi-Fi interface, as well as an OpenSSH server to enable remote communication. Finally some scripts were installed in order to start the monitoring process at startup. After the required software (compiled for the MIPS architecture) has been added and the new OS has been repackaged, the latter can be re-flashed on the router. In our case this installation has been manually performed using a firmware update functionality through the Ethernet link, but any other OS update mechanism could have been used.

An operational Sniffing Wireless Router: After we installed the modified OS, the *NeufBox_V4* was able to collect MAC addresses from the Wi-Fi channels while performing its original functionality. We did not notice any alteration of the performances, suggesting that the load induced by the Wi-Fi tracking process was light compared to the router capabilities.

4. A WI-FI TRACKING BOTNET

This section presents a thought experiment in which we discuss the design of the Wi-Fi tracking system including its architecture, communication channel for data exfiltration as well as stealthiness of those communications.

4.1 System overview

The core elements of the considered system are a number of Wi-Fi tracking devices communicating with one central entity called server. Each participating device is infected by the malware and is running a modified OS.

This modified OS provides original services while allowing the device to run dedicated applications for Wi-Fi monitoring and data reporting. Each device is in charge of collecting and processing information from the wireless channel. Collected data includes MAC addresses of devices in range[7], a timestamp, and potentially a received signal strength indicator (RSSI) to estimate the remoteness of the device. To this will be added the identifier of the tracking node, which could be later resolved to a precise location by querying a public Wi-Fi Positioning Services with the BSSID of nearby

[5] `http://www.cisco.com/c/en/us/products/collateral/wireless/mobility-services-engine/white_paper_c11-728970.html`

[6] The source of the *NeufBox_V4* is available at `http://www.efixo.com/neufbox4/freesoftware/`

[7] Identifiers like cookies and login could also be considered.

APs[8]. A report will therefore contain the following information: `(MAC_ADDR,TIME,RSSI,TRACKER_ID)`. This data is then sent to the central server over the Internet. As for any botnet, this system can adopt a centralized topology or a decentralized one to reduce its detectability and increase its robustness [1].

4.2 Efficient and Stealthy Data Exfiltration

A core element of this system is the exfiltration of the data collected by the node to the server. The design of this data reporting must ensure that it will be efficient in terms of computation and communication but also stealthy. Efficient, because the extra load of Wi-Fi tracking functionality must not disrupt the original functionality of the system; and stealthy because network traffic generated by data reporting could reveal the existence of operating malware. Those objectives are tightly linked, since reducing the volume of reporting traffic will potentially reduce its detectability.

Methods such as temporal aggregation could significantly reduce the amount of transmitted information. Probe requests are usually received by bursts of several milliseconds every 20 or 30 seconds. This data report corresponding to a burst could be aggregated by averaging the signal strength for instance. Similarly, reporting events such as arrival and departure (i.e. when a device enters/leaves the range of tracking device) has also potential to reduce the load.

The stealthiness of those communications can be ensured by using covert communication channels [17]. A suitable covert channel should: (1) be capable of sustaining the data rate that a single node would produce, (2) look like genuine traffic typically originating from a set-top box. There are a number of proposals for covert channel that would be suitable for such communications, for instance by piggybacking on the DNS, ICMP or HTTP protocols [17], or even P2P file sharing systems. Finally, data reporting could be opportunistic by being activated only when genuine traffic is relayed by the Wi-Fi tracking device. This would prevent the generation of traffic without activity on the local network.

4.3 Deployment

Deployment of such a tracking system requires the infection of a large number of Wi-Fi routers. We review the potential methods that could be used to achieve this goal.

Physical Access: Installing custom firmware by getting a physical access to the target device for a short period of time is the easiest solution. This firmware can be installed by flashing the memory with a USB stick or by spoofing a server update through the Ethernet connection [16]. While not scalable, this method can be used for targeted monitoring.

Update server hijacking: Wi-Fi routers usually have a functionality that enables a software update by downloading the new version from the vendor servers. In most cases, this update must be manually initiated by the administrator, but it is sometimes automatically performed at boot time. The latter is the case for Wi-Fi routers owned by ISPs such as the *NeufBox_V4* of the ISP SFR and the Freebox. Compromising this update server to distribute modified firmware would be a convenient way to infect a large number of devices. Alternatively, using a Man-In-The-Middle attack, it could be possible to substitute a malicious update server to the real one [16]. Finally, we must also consider the eventuality of a malicious vendor distributing an official OS containing the Wi-Fi tracking malware.

Remote and Local Exploit: A third possible angle of attack is to use a worm that propagates in the routers through the network. This could be done by exploiting a remote code execution vulnerability [7] or more simply by using default credential [3]. Infected hosts on the local network could also be used as the last hop to attack the router.

Over the air propagation: With the increasing density of wireless routers in certain areas, *over-the-air* propagation of malware has become a valid hypothesis. This propagation mode has been explored from a purely theoretical point of view by several works that investigate the propagation speed and spread [11, 13, 9]. Such airborne malware exploits vulnerabilities in the device firmware after having bypassed the security protection of the wireless network (if any).

5. TRACKING POTENTIAL

This section considers the tracking potential of a Wi-Fi router botnet. Taking into account the geographical distribution of wireless routers, we first discuss the area covered by a hypothetical network deployed in France. Then, using real mobility and Wi-Fi traces, we provide a first estimation of its capability to track an individual's whereabouts.

5.1 Geographic distribution of Wi-Fi routers

The area covered by a Wi-Fi tracking botnet are those where Wi-Fi routers are usually operating, which are generally located in areas with high human activity like residential areas, commercial areas, or offices areas. On the other hand, there are a number of other areas that will not be covered by this system, for instance natural and agricultural areas as well as roads.

In order to estimate the geographical distribution of the potential elements of a Wi-Fi tracking system, we used the geographical coordinates of Wi-Fi routers belonging to the French ISP Free. By querying a Wi-Fi Positioning System (WPS) with two consecutive MAC address, we managed to obtain the location of more than 1.8 million Wi-Fi routers[9]. Geographical distribution of Freebox routers at the scale of the country is shown on Figure 1. As expected, the areas with the highest density correspond to those associated with human activity, while natural areas are empty. The highly uneven distribution of the routers mean that a tracking system based on Wi-Fi routers will only cover a small part of a country. However, this is in those locations that a majority of the population is located, which promises a high tracking potential.

[8] `https://developers.google.com/maps/documentation/business/geolocation/`

[9] This data could only be collected for Freebox routers. Indeed the WPS requires at leat two valid MAC address per query and, unlike the Freebox, other boxes do not have two consecutive BSSID on the same box.

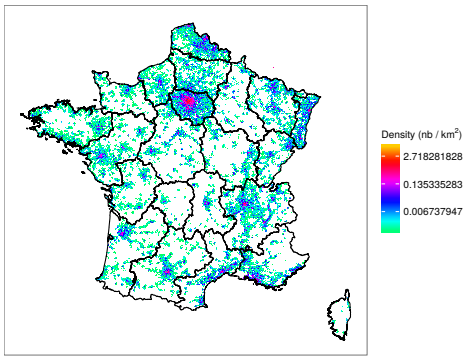


Figure 1: Density of Freebox routers in France.

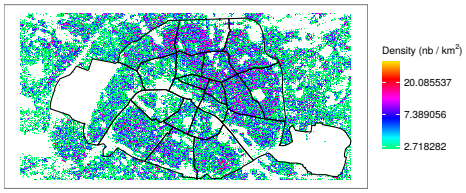


Figure 2: Density of Freebox routers in the city of Paris.

Figure 2 focuses on the distribution in the city of Paris. The density varies a lot inside the city. Areas with the highest density corresponds to residential areas, while the low density ones correspond to areas dedicated to other activities (parks and natural or industrial areas). It can be noted that those non-residential areas also contains Wi-Fi routers, but because our dataset is composed of home routers they appear as empty.

This means that a tracking network composed of such Wi-Fi routers would have a good coverage in urban areas. In some areas, the density is so high that the signals of a device could be received by several nodes, hence allowing for signal triangulation to further improve the geolocation of the device.

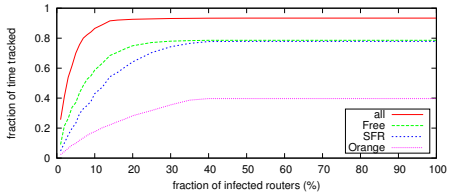
5.2 Temporal and Spatial Coverage

The geographical coverage alone is not enough to evaluate the tracking capabilities of such a system as the mobility of the subject will determine the amount of tracking. A more accurate representation of the tracking has been built from data collected on a smartphone . This dataset is composed of accurate mobility traces as well as results of Wi-Fi scans which are used to represent the detection of the mobile device by a set of routers. By using the result of Wi-Fi scans as a detection indicator, we make the assumption that the visibility is bi-directional: i.e. if the device can detect the AP, then the AP can detect the device. This assumption is reasonable since most portable devices use the active service discovery mode which involves a response from the AP upon reception of a request from the device.

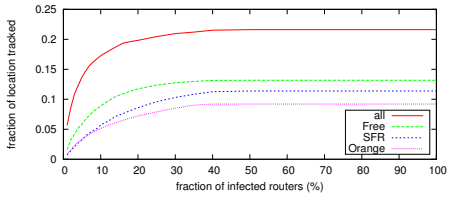
The dataset corresponds to 50 hours of daily life of one of the author and has been collected using a custom mobile application running on its smartphone and logging system events. In our particular context, the monitored events are a new Wi-Fi scan result and a the modification of the geolocation. The geolocation is either provided by the GPS chip or by the network.

From this dataset, the temporal and spatial coverage of a potential tracking network has been derived. The temporal and spatial coverage are respectively estimated by the fraction of time (time slots of 60 seconds) and location (square of 100 meters side) for which the device was visible by at least one element of the tracking system. Four categories of potentially infected routers have been considered: all the routers, and those belonging to one of the three main French ISPs: Free, SFR and Orange. Considering the possibility of a partial infection of the routers, we computed those coverage for a random fraction of routers. For each fraction, the coverage has been averaged over 1000 random subsets of routers.

Results of the spatio-temporal coverage evaluation are presented in Figure 3. Both spatial and temporal coverage rise quickly with the fraction of corrupted elements and then slowly converge toward a maximum value. Limiting the set of corrupted routers to those of an ISP reduces the amplitude of the coverage but does not change this trend. In these traces, an infection of only 10% of the routers is enough to cover 90% of the time and 17% of the locations. The significant differences between spatial and temporal coverage can be explained by travel along roads and train tracks that have a poor Wi-Fi coverage but accounts for a large number of locations and a relatively short duration.



(a) Fraction of time tracked



(b) Fraction of locations tracked

Figure 3: Fraction of time and location where a device is in range of a tracking device as a function of the fraction of compromised Wi-Fi routers.

An example of mobility traces that could be obtained by a Wi-Fi tracking botnet is provided on Figure 4. It presents the real mobility trace obtained from the GPS of the phone, as well as the set of locations where the phone was detected by one of the infected Wi-Fi routers. Despite the small fraction of infected routers (in this case 2%), the tracking system is able to build an accurate approximation of the real mobility trace.

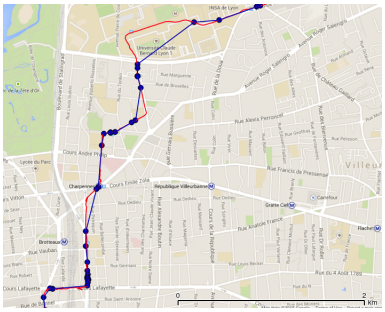


Figure 4: Mobility trace reconstructed from an hypothetical tracking system composed of 2% of the Wi-Fi routers (blue) vs. real mobility trace (red).

6. CONCLUSION

This work investigated the tracking potential of an hypothetical botnet of Wi-Fi routers. We argued that Wi-Fi routers can be easily turned into Wi-Fi monitoring devices. Because they can be massively infected, this type of devices has become the ideal core element of a large scale monitoring system. We presented design elements of such a system including efficient and stealth communication as well as options for its massive deployment. Using real-world data sets, we gave a preliminary evaluation of the coverage of such a tracking system.

Given the ubiquity of those devices, such a system could track most individuals a large fraction of the time. In fact avoiding such a tracking system would mean to stay away from places with Wi-Fi routers, i.e. most places with human activity. The system proposed by this paper is purely hypothetical and has not been deployed; however, given the quality of the data provided, and with the resources of a large surveillance organization, it is possible that this idea would be put in practice in the future, if this is not already the case. A surveillance organization could also cooperate with an ISP controlling a large fleet of Wi-Fi routers in order to deploy a Wi-Fi tracking system.

The most effective way to avoid Wi-Fi tracking is to prevent the leakage of the device MAC address, either by replacing it with a pseudo-random identifier [8], or by simply disabling the Wi-Fi interface whenever possible. Finally, the threat calls for the strengthening of Wi-Fi routers security, for instance through authenticated firmware updates [2] and in place firmware authentication.

7. REFERENCES

[1] Michael Bailey, Evan Cooke, Farnam Jahanian, Yunjing Xu, and Manish Karir. A survey of botnet technology and defenses. In *Conference For Homeland Security*, pages 299–304. IEEE, 2009.

[2] Jeff Bernstein and Tim Spets. CPE WAN Management Protocol - DSL Forum, Tech. Rep. TR-069, 2004.

[3] Carna Botnet. Internet census 2012-port scanning/0 using insecure embedded devices, 2013.

[4] Brian Fung. How stores use your phone's WiFi to track your shopping habits. `http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/19/how-stores-use-your-phones-wifi-to-track-your-shopping-habits/`.

[5] Eva Galperin and Cooper Quintin. Russian researchers uncover sophisticated NSA malware. `https://www.eff.org/deeplinks/2015/02/russian-researchers-uncover-sophisticated-malware-equation-group`, 2015.

[6] Dan Goodin. Spy software's Bluetooth capability allowed stalking of Iranian victims. `http://arstechnica.com/security/2012/06/spy-softwares-bluetooth-capabilty-allowed-stalk-of-iranian-victims/`, June 2011.

[7] Dan Goodin. Bizarre attack infects Linksys routers with self-replicating malware. `http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/`, February 2014.

[8] Marco Gruteser and Dirk Grunwald. Enhancing location privacy in wireless LAN through disposable interface identifiers: a quantitative analysis. *Mobile Networks and Applications*, 10(3):315–325, 2005.

[9] Hao Hu, Steven Myers, Vittoria Colizza, and Alessandro Vespignani. WiFi networks and malware epidemiology. *Proceedings of the National Academy of Sciences*, 106(5):1318–1323, 2009.

[10] Nathaniel Husted and Steven Myers. Mobile location tracking in metro areas: Malnets and others. In *Conference on Computer and Communications Security*, pages 85–96. ACM, 2010.

[11] Jonny Milliken, Valerio Selis, and Alan Marshall. Detection and analysis of the Chameleon WiFi access point virus. *EURASIP Journal on Information Security*, (1), 2013.

[12] A. B. M. Musa and Jakob Eriksson. Tracking unmodified smartphones using Wi-Fi monitors. In *Proceedings of the 10th ACM Conference on Embedded Network Sensor Systems*, 2012.

[13] Amirali Sanatinia, Sashank Narain, and Guevara Noubir. Wireless spreading of WiFi APs infections using WPS flaws: An epidemiological and experimental study. In *IEEE Conference on Communications and Network Security*, pages 430–437, 2013.

[14] Jeremy Scahill and Glenn Greenwald. The NSA's Secret Role in the U.S. Assassination Program. `https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/`, September 2011.

[15] Jennifer Valentino-DeVries. 'Stingray' Phone Tracker Fuels Constitutional Clash. `http://www.wsj.com/articles/SB10001424053111904194604576583112723197574`, September 2011.

[16] Bachy Yann, Nicomette Vincent, Alata Eric, Kaaniche Mohamed, and Courrège Jean-Christophe. Integrated access device security. Risk analysis and experiments. *Revue des sciences et technologies de l'information*, 19(6):63–88, 2014.

[17] Sebastian Zander, Grenville J Armitage, and Philip Branch. A survey of covert channels and countermeasures in computer network protocols. *IEEE Communications Surveys and Tutorials*, 9(1-4):44–57, 2007.