Wardriving and its Application in Combating Terrorism

Zeeshan Akram[1], Muhammad Anwaar Saeed[2]
Department of Computer Science & IT
Virtual University of Pakistan
Lahore, Pakistan
[1]zeeshan.137@hotmail.com, [2]anwaar@vu.edu.pk

Marriam Daud
Department of Computer Science
National University of Computer and Emerging Sciences
Lahore, Pakistan
marriamdaud@gmail.com

***Abstract*—Wireless local area network (WLAN) has changed the paradigm of communication and become ubiquitous. As the number of devices connected to wireless is increasing, the sensitive information broadcasted by WLAN can be utilized to collect important data about digital devices of criminals and terrorists. In this research war-driving was conducted to enumerate the sensitive data broadcasted by digital devices of WLAN in real time. Kali Linux version 2017.1, a laptop and a smartphone were used as a platform for war-driving. The results of war-driving showed that information about MAC addresses of digital devices, number of digital devices and manufactures of digital devices can be easily collected passively. This information can be useful for law enforcement agencies to plan a raid and make arrangements to seize digital devices of criminals and terrorists.**

Keywords—Wireless Network Security; Wardriving; Kali Linux; Security Set Identifer (SSID);

I. INTRODUCTION

The IEEE 802.11 Wireless Local Area Network (WLAN) standard is commonly used to provide internet connectivity to wireless and mobile devices. The elimination of wires makes WLAN a cost effective and easy to implement networking solution. IEEE 802.11 wireless LAN networks provide wireless connectivity in a range of roughly 300 feet from the AP. WLAN has changed the paradigm of communication and become ubiquitous. WLAN networks transmit important network related information in plain text [1][2].

WLAN uses authentication and encryption protocols to protect confidentiality, integrity and availability of data of its wireless clients. WLAN's security evolved over three major stages throughout its development. First, Wired Equivalent Privacy (WEP) was introduced as security protocol. However, researchers found vulnerabilities in cryptographic technique of WEP [3][4][5].

After the failure of the first stage, the second stage security standard, Wi-Fi Protected Access (WPA) was developed by WiFi Alliance. WPA was also known as WPA1. WPA used the Temporal Key Integrity Protocol (TKIP) encryption algorithm which provided an improvement in WEP security while utilizing the same WEP hardware. The third and currently used WLAN security stage is WPA2. WPA2 is also known as robust security network (RSN). WPA2 uses AES (Advanced Encryption Standard) and CCMP (Counter Mode CBC MAC Protocol), which provides stronger encryption than WPA [4][5].

WLAN broadcasts sensitive information despite the development in the security of WLAN. This information can be collected via war-driving. War-driving is recording name (Security Set Identifiers), location and security mechanism of AP with the help of a portable and on the move computer or smartphone [6].

Service Discovery Protocol (SDP) can be used to search Bluetooth devices and parse the search results [7]. Bluetooth data can be shared from a smartphone to a Linux based system by pairing the devices. The Bluetooth address of the smartphone can be easily viewed in Linux. In order to send specific data of an application via bluetooth, the bluetooth channel number is also required. The channel numbers used by different applications can be obtained by using sdptool command: 'spdtool browse [Bluetooth _address]' in Linux [8]. In order to communicate data the command: 'rfcomm bind [Device] [Bluetooth _address] [Channel#]' can be used to establish a link between Linux system bluetooth device and smartphone application via bluetooth [9].

A network scanner that recorded data like network names, the encryption status, and the number of users on the networks was implemented in [1]. The network scanner could be used to find the most vulnerable wireless networks and plan an attack that could affect most number of users. In this paper network scanning was performed using Linux Kali, a laptop and a smartphone. Authors in [1] have used Rasberry Pi hardware, WiFi dongle and GPS module to carry out wardriving. The configuration and integration of GPS module and WiFi dongle in Rasberry Pi is cumbersome. It also adds an extra cost of buying these components. In contrast, in this research wardriving was performed by using already available devices. The GPS sensor of smartphone was used to communicate GPS data with laptop via bluetooth.

978-1-5386-4427-0/18/$31.00 ©2018 IEEE

II. PLATFORM AND TOOLS

A laptop running Kali Linux 2017.1 was used as a platform for wardriving in real time. Kali Linux was developed by Offensive Security to provide penetration testing platform and to conduct security audits [10]. The laptop was connected to a smartphone via Bluetooth. The smartphone communicated GPS data with laptop which was recorded by Kismet tool of Kali Linux [11]. BlueNMEA application was used to send GPS data via Bluetooth from smartphone. It is an android application which can send location data via Bluetooth or TCP [12]. Giskismet tool was used to represent the data gathered by Kismet tool in a flexible manner. It can convert a database of wireless networks gathered by Kismet. It can also be used to generate KML files [13].

III. WARDRIVING

A. Initial Setup and configuration

The process of initial setup of laptop and smartphone for wardriving is shown in figure 1. Linux Kali was run in live mode on a laptop from a bootable USB. The wireless interface of the laptop was put in monitor mode to enable it to sniff wireless packets using airmon-ng tool as shown in figure 2 [14]. The Bluetooth and GPS sensor of smartphone were turned on. Smartphone was paired with laptop to communicate data via Bluetooth. The bluetooth address smartphone was obtained from Kali Linux as shown in figure 3. BlueNMEA was started on the smartphone. The MAC address of Bluetooth interface of smartphone was noted. The Bluetooth channel number of BlueNMEA application was found by sdptool command in Kali Linux as shown in figure 4. The laptop bluetooth device was binded to the smartphone bluetooth device on the channel of BlueNMEA application. Kismet was configured to get GPS data from bluetooth device. Kismet was started in Kali Linux to monitor WLAN interface. The laptop and smartphone were placed in a car which is driven in a residential area at 10-20 km/h.

B. Processing of Wardriving data

The captured packets were converted into wireless network database by using Giskismet tool of Kali Linux. The database was then converted into Keyhole Markup Language (KML) file by Giskismet so that it could be viewed in Google Earth [15]. The results of wardriving viewed in Google Earth are shown in Figure 6. The database of wireless networks was opened by 'DB Browser for SQLite' tool [16]. The 'wireless' and 'clients' tables were exported into comma separated values (CSV) format by 'DB Browser for SQLite'. These CSV tables were added to IBM SPSS tool as data sets for statistical analysis [17].

C. Results of Wardriving

A total number of 100 WLAN networks and 159 WLAN clients were found during wardriving. Table 1 shows frequency distribution of encryption mechanisms of WLAN networks collected during wardriving. It was observed that 97% of the WLAN networks were protected by WPA2. Table 2 shows the frequency distribution of manufacturers of WLAN APs.

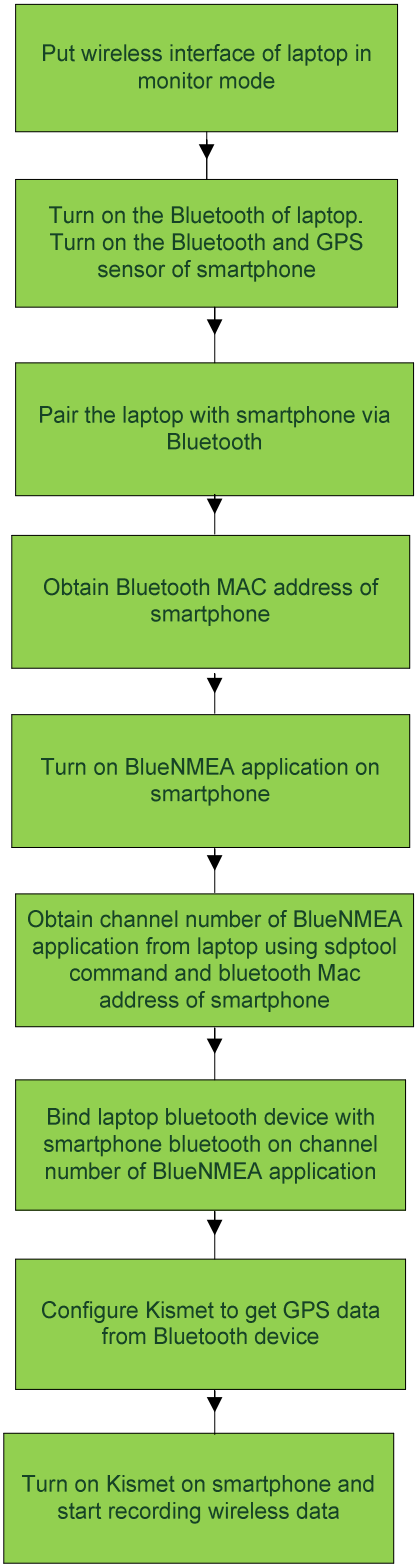

Fig. 1: The process of initial setup and configuration of wardriving.

Fig. 2: The output of airomon-ng tool to put the wireless interface 'wlan0' of the laptop in monitor mode.

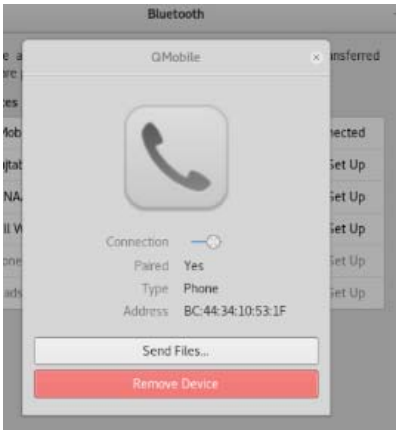

Fig. 3: Obtaining Bluetooth MAC address of smartphone from Kali Linux.

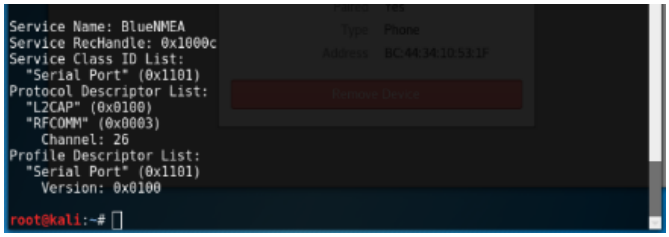

Fig. 4: Obtaining channel number of BlueNMEA application running on smartphone with spdtool tool in Kali Linux.

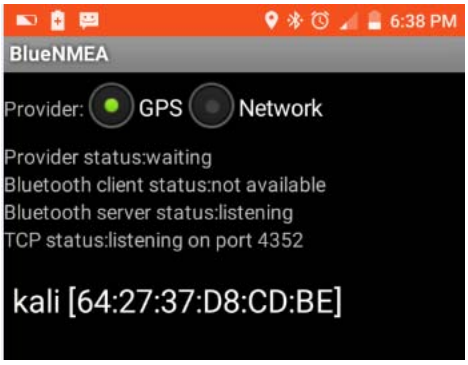

Fig. 5: Screenshot of BlueNMEA application upon binding of smartphone bluetooth device with laptop bluetooth device.

It was observed that 24% of APs were manufactured by Tenda, 14% by Huawei, 13% by KasdaNet and 11% by D-Link. Figure 7 shows the frequency distribution of channel numbers used by APs. It was observed that 29% APs used channel 11 and 23% APs used channel 1. Figure 8 shows the frequency distribution of WLAN clients against WLAN networks. The WLAN networks are represented by network ID (nid). It was observed that the maximum number of clients of a residential WLAN AP was 5. The average number of clients per WLAN AP was found to be 1.59. Figure 9 shows the frequency distribution of manufacturers of WLAN clients. It was observed that 18.2% of the clients were manufacturer by Tenda, 11.3% by KasdaNet, 10.7% by Huawei.

Fig. 6: The results of wardriving shown in Google Earth.

TABLE I. WLAN ENCRYPTION

Encryption Type	*Frequency*	*Percentage*
None	3	3
WPA+PSK WPA+AES-CCM	47	47
WPA+TKIP WPA+PSK WPA+AES-CCM	50	50
Total	100	100

TABLE II. ACCESS POINT MANUFACTURERS

Manufacturer	*Frequency*	*Percentage*
D-LinkIn	11	11.0
Fiberhom	6	6.0
HuaweiTe	14	14.0
KasdaNet	13	13.0
MurataMa	1	1.0
Routerbo	1	1.0
Sagemcom	2	2.0
SamsungE	1	1.0
Shanghai	8	8.0
TendaTec	1	1.0
Tp-LinkT	3	3.0
Ubiquiti	5	5.0
Unknown	5	5.0
Zte	2	2.0
ZyxelCom	3	3.0
Total	100	100.0

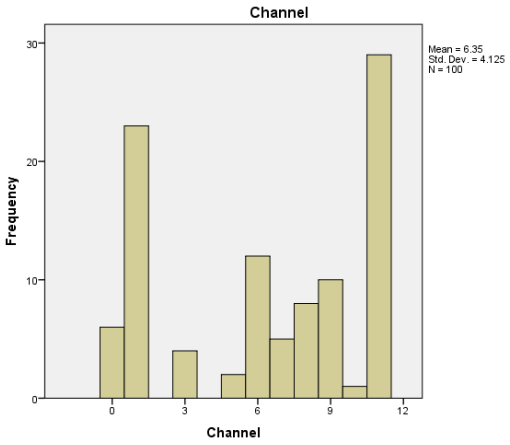

Fig. 7: The distribution of WLAN channels found during wardriving.

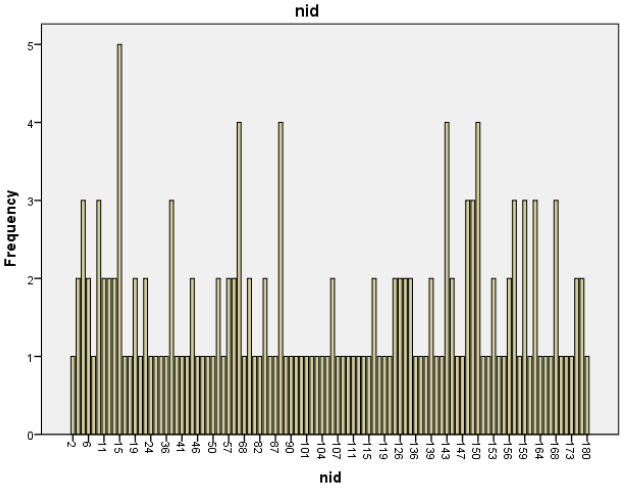

Fig. 8: The frequency distribution of WLAN clients against WLAN networks.

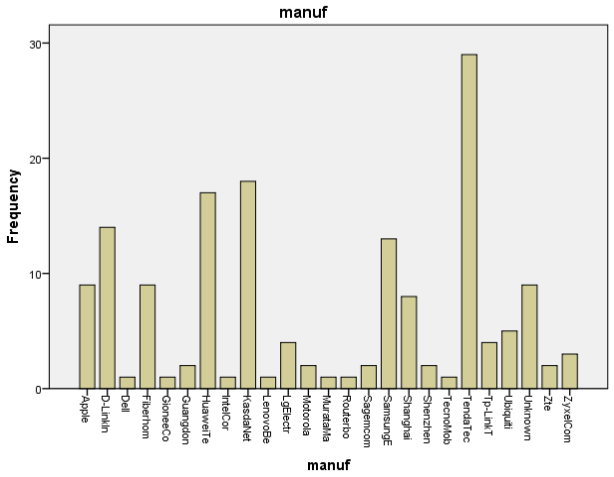

Fig. 9: The frequency distribution of WLAN clients manufacturers.

IV. APPPLICATION OF WARDRIVING

War-driving can be used to collect important information about the digital devices present in a location of interest. It can give details about the number of clients of an access point, their WLAN MAC addresses and also their manufacturer's information. War-driving can passively collect data related to WLAN connected digital devices which can give an additional insight to law enforcement agencies regarding an area of interest. This information can be fruitful in planning raid in such a way as to seize all these digital devices. War-driving can be used to collect data about the digital devices of criminals and terrorists. It can also be used as the first step in launching further wireless attacks on the WLAN of criminals or terrorists in order to collect more incriminating evidence regarding their activities.

V. CONCLUSION

In this paper war-driving was performed in real time to enumerate the sensitive data broadcasted by WLAN. Kali Linux was used as a platform to perform war-driving. The number of clients, manufactures of clients and access points, encryption mechanism of access points and geographic locations of access points were collected. This information can be useful for law enforcement agencies to provide an insight about an area of interest, the possible digital devices which can be seized and an approximate number of users. It can be utilized for collecting data before conducting raid on terrorists and criminals.

REFERENCES

[1] N. Domingo, B. Pearson, and Y. Jin, "Exploitations of wireless interfaces via network scanning," *International Conference on Computing, Networking and Communications (ICNC)*, pp. 937-941, 2017.

[2] M. Gong, B. Hart and S. Mao, "Advanced Wireless LAN Technologies", *ACM SIGMOBILE Mobile Computing and Communications Review*, vol. 18, no. 4, pp. 48-52, 2015.

[3] H. Boland and H. Mousavi, "Security issues of the IEEE 802.11 b wireless LAN", *Canadian Conference on Electrical and Computer Engineering, 2004*, vol. 1, pp. 333–336, 2004.

[4] H. Bulbul, I. Batmaz and M. Ozel, "Wireless network security: comparison of WEP (Wired Equivalent Privacy) mechanism, WPA (WiFi Protected Access) and RSN (Robust Security Network) security protocols", *In e-Forensics '08 Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, pp. 1-8, 2008.

[5] S. Wong, "The evolution of wireless security in 802.11 networks: wep, wpa and 802.11 standards", *Published by SANS Institute InfoSec Reading Room,* 2003.

[6] A. Etter, "A Guide to Wardriving and Detecting Wardrivers. *Published by SANS Institute InfoSec Reading Room,* 2002.

[7] https://people.csail.mit.edu/albert/bluez-intro/x604.html

[8] http://www.tutorialspoint.com/unix_commands/sdptool.htm

[9] https://unix.stackexchange.com/questions/92255/how-do-i-connect-and-send-data-to-a-bluetooth-serial-port-on-linux

[10] https://www.kali.org/

[11] http://max.kellermann.name/projects/blue-nmea

[12] https://tools.kali.org/wireless-attacks/kismet

[13] https://tools.kali.org/wireless-attacks/giskismet

[14] https://tools.kali.org/wireless-attacks/airomon-ng
[15] https://www.google.com/earth/download/gep/agree.html
[16] http://sqlitebrowser.org
[17] https://www.ibm.com/analytics/data-science/predictive-analytics/spss-statistical-software