iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** X **Month of publication:** October 2020

DOI: https://doi.org/10.22214/ijraset.2020.31981

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue X Oct 2020- Available at www.ijraset.com

The Security Risks of using Wi-Fi Hotspot

Haitham Daw Ammar Alfehri[1]
[1]*Assistant Lecturer at Higher Institute for Science and Technology – Sabratha, Libya.*

Abstract: ***The noticeable growth of uses for WiFi hotspots all over the most has been very significant in recent years, its use has occurred not only developed countries but also developing countries. The IEEE standard 802.11 stands out in this scenario. However, the protection mechanisms employed by this wireless network standard has not been effective in combating denial-of-charge attacks service.***
Intrusion detection systems are seen as an effective way to minimize these threats. In this research it was proposed to build three sets of data that significantly represents wireless network traffic. The generated sets have purpose of assisting in the evaluation of intrusion detection algorithms for wireless networks.
Keywords: **Network security, Wi-Fi hotspots, Man-in-the-middle attack, Wireless intrusion detection system**

I. INTRODUCTION

The use of wireless networks has become increasingly common and with an audience diversified. This preference encompasses a series of factors, among which the low implementation cost when compared to a wired network, mobility and diversity of existing devices.
The variety of devices that have wireless connectivity is huge, among them: notebooks , tablets , smartphones , televisions and others. This diversity makes the use of wireless networks, especially the IEEE 802.11 standard are more used today [1]. They are present in the most varied environments, such as corporate, media academics, buses and even planes.
However, the IEEE 802.11 standard has security problems in relation to security mechanisms. Over the years, there have been updates tosecurity amendments to IEEE 802.11 wireless networks, this occurred as follows: first amendment was Wired Equivalent Privacy - WEP. WEP uses RC4 algorithm and key shared, its purpose is to protect data frames.
However, it was not shown effective, presenting several vulnerabilities [2]. In 2004, the IEEE 802.11i security amendment or commercially called WiFi Protected Access Version 2 - WPA2. Its main improvements are related to confidentiality, integrity and authenticity data transmitted on the network. However, it does not present protection to control panels and management. The ultimate security mechanism presented is the IEEE 802.11w amendment. The protocol offers protection to some management frameworks [3]. This allows devices to exchange frames management systems securely. The IEEE 802.11w amendment does not provide protection for control boards.
The updates introduced by security amendments have corrected some flaws and showed improvements for some types of threats, this reduced the risk for certain types of threats attacks. However, a major exploiter of wireless network vulnerabilities is attacks denial of service, also called Denial of Service - DoS. Denial attacks service aims to affect the availability of network resources and services[4], in wireless networks they exploit the lack of protection in management and control of the WEP and IEEE 802.11i protocols. In the IEEE 802.11w standard use the lack of protection of control boards. An alternative to reduce incidents caused by this type of threat would be to use a protection mechanism with the security amendments.
A system that presents itself effectively in combating DoS attacks on networks wireless are intrusion detection systems - IDS. IDS can be based on signature or anomaly. The subscription-based IDS analyze the monitored traffic from a set of attack signatures. In the anomaly-based method, IDS builds models of normal behavior and characterizes as an intrusive event all traffic thatdiffers from this model. For each model there are different techniques proposed for its implementation, generally these approaches have specificities according to the type network. This is due to the fact that each type of network has different characteristics of operation. The main objective of the IDS is to identify anomalous events, this without compromising the functioning of the network.

II. TECHNOLOGY BEHIND WI-FI HOTSPOT

Wireless transmission over computer networks began to be disseminated through the initiative of companies and research institutions. With this, the IEEE seeking to make possible the technology created a research group called IEEE 802.11 to create open standards, but at the proposed data transfer rate, the standard was not validated. Only in 1997 did IEEE publish the standard for Wireless Local Area Networks - WLANs. The WLAN is a system that interconnects several devices, both mobile and fixed using radio frequency - RF as a means of transmission.

The architecture of the IEEE 802.11 standard is composed of multiple components; these perform interaction to provide mobility at stations so that it is transparent to the upper layers. The main components of this technology are:

1) *Basic Unit (Basic Service Set - BSS):* It is the main building block of the IEEE 802.11 architecture, defined as a group of stations, which fall under the direct domain of the same coordination function. This determines the sending and receiving data through the wireless transmission medium used by the stations;
2) *Distribution System (Distribution System - DS):* Logical component for the send frames between stations belonging to different BSSs and a wired local network (LAN);
3) *Wireless Station (Wireless Station - STA):* Any device that accesses the medium wireless; and
4) *Access Point (Access Point - AP):* It is a STA station that provides connectivity between multiple STAs and between STAs and DS.

Wireless networks follow a modular architecture, in which the system is partitioned into cells. Each of these cells is called BSS, which is composed of one or more stations and the AP. The AP performs all the control of the stations connected to this cell.
Wireless networks can be constituted through a single cell, with only one AP, however, for the construction of networks with a coverage area greater than one cell, it is used a DS, where the APs are connected via an Ethernet or wireless backbone. Being so the DS represents the communication infrastructure that interconnects the cells constituents of the network.
The union of a set of STAs and APs from different BSS interconnected to a DS it is termed as an extended set of services. The Extended Service Set - ESS is seen over the Internet Protocol - IP upper protocol layer as just an IEEE 802.11 network.

III. RISKS INVOLVED IN WI-FI HOTSPOTS

Wi-Fi has dramatically changed the world we live in, making it even easier than ever to access the Internet. Free public Wi-Fi networks can be found everywhere: public parks, coffee shops, churches, shopping malls, libraries and on public transport, such as buses and trains. While this technology has greatly improved convenience for notebook and smartphone users, it has also opened up a significant number of security risks. Here we will show you why public Wi-Fi can be dangerous and how you can protect yourself from these threats.

A. Encryption breaches

To understand some of the most common types of attacks, you need to know how Wi-Fi works. This technology is a type of wireless LAN that exchanges data with your device using radio waves. A device called an access point communicates with your phone, tablet or computer and then connects to the Internet with a network router. The exchange of data between your device and the router is encrypted using a pre-shared key (PSK).
Unfortunately, since everyone in a Wi-Fi hotspot can connect to the same network, it is possible for everyone in one area to see the data being exchanged on the other devices. A common method, called network spying, occurs when an attacker intercepts visible traffic on a Wi-Fi channel. In some cases, the attacker may be able to intercept the PSK, allowing you to decrypt all data sent to a specific device, until the connection is broken or the PSK is changed. Even if he is not fortunate enough to intercept the PSK, he can use a “brute force application” to try to guess it, which allows attackers to test millions of combinations per second. This means that if the network administrator has selected a simple PSK, the attacker can obtain it relatively quickly. This threat can be reduced, Some places, however, don't even bother to encrypt the data. Many locations display nothing more than an ad or contract page, before allowing users to connect. Although these companies generally restrict the use of Wi-Fi to regular customers (for example, by printing the password on the consumption bill) their data may still be visible to any other customer present. Some attackers even passively collect data, decrypting it later.

B. Page Spoofing and Fake Networks

There are other possible risks for anyone trying to connect to public Wi-Fi. One type of attack involves setting up an entirely new Wi-Fi network, causing users to connect to it. Thus, the owner of the network can view all the data sent. This practice is especially dangerous for all users who connect to any open network.
Another strategy used by hackers is to create a fake access point in an area that may have, in a totally plausible way, free Wi-Fi. For example, they can set up a network at a bus station that does not offer Wi-Fi and label the hotspot as “Internet by bus”. Or a hacker can create a second network in a location that already offers Wi-Fi. If you are in a library with a hotspot called “Library1”, he can create another hotspot called “Library 2”. Regular users of the library who do not suspect anything can choose a network based only on the name and when they connect to the hacker's Wi-Fi, the hacker can easily see all the information.

While some hackers are happy to collect any data that you may accidentally provide, others may try to collect specific information, such as account logins or email addresses. Some malicious access points have a practice called page spoofing to obtain this type of desirable data. When a page is spoofed, hackers will create a fake Web page that looks exactly like the real page, to get you to enter your information. For example, they may ask to share something on social media to access the Internet. You will be directed to a fake login page that looks exactly like the real page. After you have entered your account information, you will receive an error message, possibly stating that you entered the password or username incorrectly and will be directed, without knowing it, to the legitimate page, where you will be able to login, but this time, with an audience. In this scenario, you can give access to your social media account without even realizing it.

C. Owners Privacy

Even in situations where the public Wi-Fi network is safe from hackers, you may still face privacy breaches, but this time it will be the establishment itself that will offer the hotspot. While most companies aren't trying to steal your identity, they can use your information in ways you don't want them to use. Many Wi-Fi owners collect data from their users for advertising or statistical purposes. They may also ask you to leave an email or phone number in exchange for access to the network or to share their company on their social media profiles. Some companies triangulate your physical location using Wi-Fi signal strength to determine if your stores are overcrowded or find out about the paths you use to reach a store.

IV. WIRELESS INTRUSION DETECTION SYSTEM

Wireless networks have been experiencing dramatic growth in virtually allsectors of society. This increases the concern with the vulnerabilities presentedfor them, security has become a mandatory requirement. Figure 20 presents data obtainedby the company specialized in antivirus Symantec, it is noted that in 2013 Brazil occupied theeighth in the world ranking of attacks on computer networks.

This situation highlights the need to implement protection mechanisms against attacks on networks. IDS are applications that prove to be effective for this task; they act as a second layer of defense. This helps to reduce the effectiveness of attacks.

IDS is a tool capable of evaluating the content of packets carried on the network, identifying them as normal or anomalous, or categorizing an attack. The purpose of IDS consists of providing instruments that reduce the possibility of intrusion. This can occur in anticipation of attacks.

Intrusion detection metrics predict that parameters or behavior presented by legitimate users are different from those presented by an attacker. With this is possible to recognize patterns of activities performed in the monitored environment, and so report the results of the detection process.

Architectures for IDS can be defined in three categories: host- based, network-based and distributed.

The host- based architecture consists of monitoring a device, with the purpose of identifying intrusive events. This architectural model defines that for each monitored element there must be an IDS. In this way each device has its IDS host- based , there is no interaction between the IDS present in the devices arranged on the network.

The network-based architecture consists of monitoring a specific segment network, where the IDS is strategically positioned. In this way, IDS has the responsibility to monitor and analyze all traffic belonging to this network. In case of any unauthorized access IDS issues alerts.

The distributed architecture allows modular monitoring of the network. This can be carried out by positioning several modules at strategic points in the network. The data collected by these modules are directed to a central controller that performs themonitoring and analysis.

Another important feature present in IDS is that of data collection. The process of Intrusion detection is divided into two stages: data collection and analysis. Data collection is a very important step, an IDS needs information that enables the recognition of intrusive events. Therefore the collection of data is responsible for storing and providing such information to IDS. The process of formation of these data sets consists of capturing security information carried out at the perimeter of the network [5]. As Spafford and Zamboni[6]describe (2000), the good performance of an IDS is related to the information in which based on their decisions.

The detection method used by IDS directly influences its performance. The method used to identify events defines how data sets are analyzed. IDS can use different ways of analysis to identify traffic intrusive. There are two main classes, these are: subscription-based and subscription-based in anomalies.

Signature-based IDS recognize an intrusive action through the association between the audited records and the pre-established characterization of the intrusive behavior. Each event identified as an intruder is recognized through ansignature, this is a series of attributes that identifies it. This makes it possible for IDS identify known attacks quickly and with a low error rate.

This detection method is based on building and updating database knowledge of attacks. However, the behavior of an intrusive event can change constantly. This can lead to the non-recognition of certain intrusions, if are not specified in your knowledge base. To reduce this problem it is it is necessary to carry out constant updating of the database However, this action is very laborious and demands a high computational cost. It is necessary to generate specifications that have the greatest number of attacks and are not associated with any non-intrusive event [7].

V. METHODOLOGY

The entire perimeter of the selected environment has radio signal coverage; this is done through the four access points. The access points are all interconnected; this allows all users are connected on a single network. The diversity of devices and multiple user profiles generates various types of traffic categorized as normal. The monitoring carried out in the previous phase did not identify any type of anomalous traffic. THE monitoring as in the previous scenarios was performed by a wireless station, with Linux Ubuntu operating system and Wire shark software. The attacks were employed by two wireless stations; the stations were not associated with the network were allocated in strategic locations to obtain only radio frequency signal.

VI. FINDINGS

The WEP protocol presented several vulnerabilities, with this the work group of the IEEE 802.11 has started a search for the creation of a new security standard that could correct all the flaws presented by the WEP. This new standard was called as IEEE 802.11i. However, due to market pressures, the Wi-Fi Alliance used a number of specifications proposed for the new IEEE 802.11ie protocol and developed the WPA protocol. WPA has a number of mechanisms that address some security issues linked to WEP. Following is a set of features implemented in the WPA protocol:

1) The WPA protocol sends and exchanges keys used for encryption and data integrity Dice. Resolving the issue of using the WEP static key;
2) Does not support ad-hoc networks ;
3) A new message checking code has been implemented, using a new 64-bit field, the Message Integrity Code - MIC. This performs a check of the content of the data frame analyzing whether or not there was a change or errors in data transmission; and
4) The reduced WEP IV made it possible to repeat in a short period of time; already with WPA a 48-bit IV was implemented.

There are two distinct authentication methods in the WPA protocol. One designed for small networks, ie home networks, and another more robust method used in large network that uses a RADIUS 802.1x / EAP authentication server.

Personal WPA - authentication method used for home networks. THE authentication in this method is performed by the AP, is shared between the AP and the client station a WPA- Pre Shared Key - WPA-PSK which is a passphrase. This is manually configured on each equipment belonging to the network ranging from 8 to 63 ASCII characters; and Corporate WPA - all authentications is performed by an authentication server, regardless of whether it is requested by a user or device. This occurs through the use of a server that uses IEEE 802.1x associated with a type and extensible authentication protocol - EAP. This protocol is used between the AP and the authentication server. It works as follows: a customer requests a authentication, just after the server checks its database if the requester has valid credentials. If the credentials are valid, the client is authenticated and sent a Master Session Key - MSK. The channel logic of secure communication generated between the client station and the authenticator is made by EAP, it is in this environment that credentials will be trafficked.

VII. CONCLUSION

There are a large number of IDS proposals for networks, but fair evaluation between the different approaches is an arduous task, after all, it is very difficult to reproduce the same scenario employed by the author of the proposal, mainly with the behavior profile of the users. One way to carry out the comparison is through the application of IDS in a data set. However, most data sets come from simulation or wired networks. Thus, it is not feasible to use these data sets in evaluation of IDS for wireless networks based on the significant differences between networks.

With the use of some classification and pattern recognition algorithms, good results have been obtained in identifying denial of service attacks. You can conclude that the MAC layer header fields were sufficient for detection. The type, subtype, duration and address fields made a significant contribution to this process, mainly in the identification of de-authentication, and EAPOL- Start.

The scenario was not repeated with other types of attacks: fragmentation, beacon flooding, fake authentication, and fake AP. The contribution of these fields was notimportant, in fact, the detection of these attacks was poor.

The different results allow us to conclude that some fields of the MAC header are more significant for some types of attacks. Therefore, it is important to capture all header fields and their use in the data set. And to increase the accuracy of detection, data from other layers can be used.

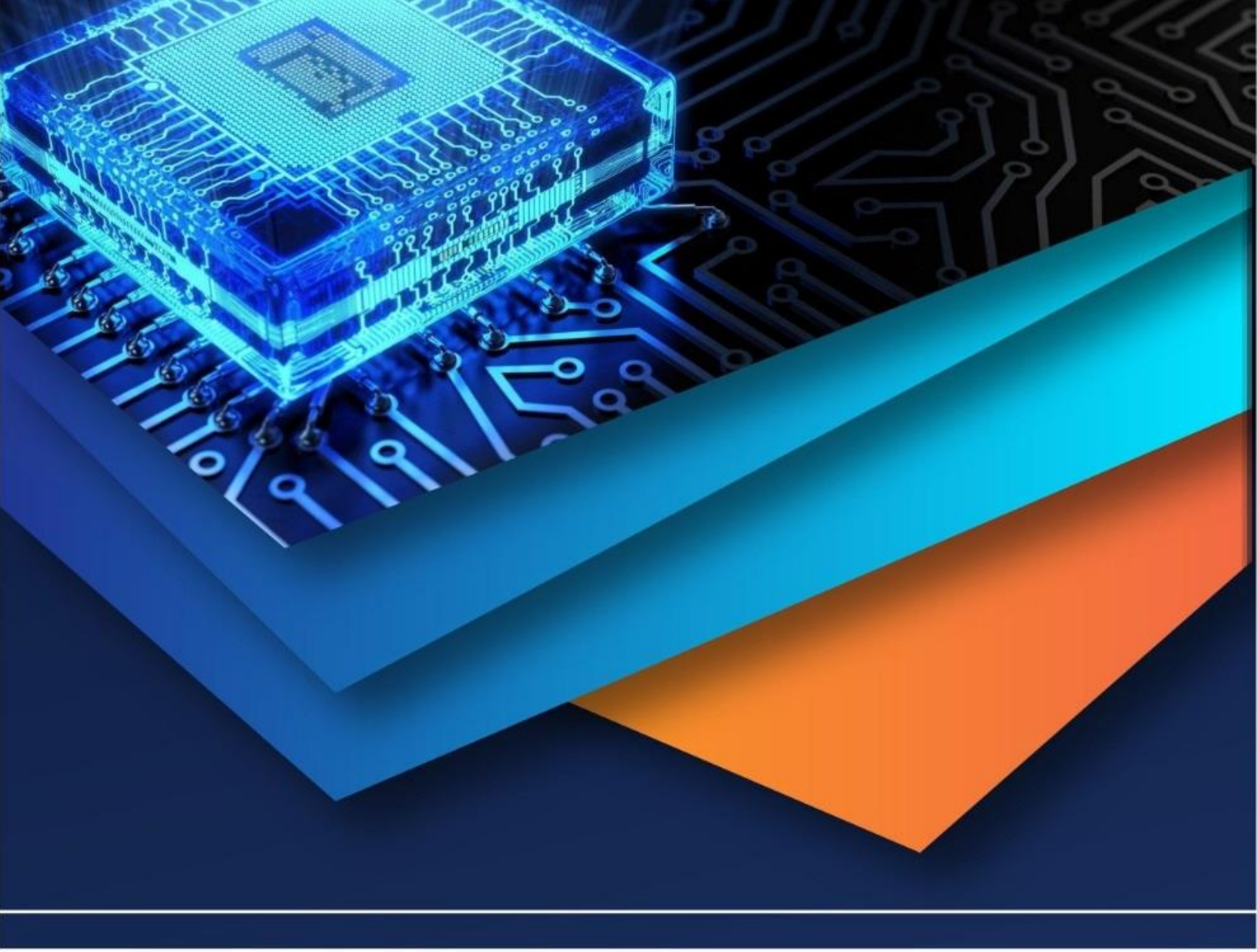
However, in the evaluations carried out in the scenario in which the IEEE amendment was employed 802.11w, good results were obtained, mainly due to the duration field, which helped to identify the attacks.

The continuation of this research, with future works, can be carried out through

A. Insert new categories of attacks in order to generate other traffic profiles anomalous;
B. Compare assessments with other intrusion detection methodologies;
C. Check fields from other layers (application, transport, network and physical) of network that can be representative in the wireless network scenario; and
D. Creation and analysis of repositories to evaluate intrusion detection algorithms for other types of networks, such as mobile telephony.

REFERENCES

[1] Feng, P., 2012, June. Wireless LAN security issues and solutions.In 2012 IEEE symposium on robotics and applications (ISRA) (pp. 921-924).IEEE.
[2] Tews, E., 2007. Attacks on the wep protocol.Cryptology ePrint Archive, Report.
[3] Ahmad, M.S. and Tadakamadla, S., 2011, June. Short paper: security evaluation of IEEE 802.11 w specification. In Proceedings of the fourth ACM conference on Wireless network security (pp. 53-58).
[4] Sandstrom, H., 2001. A survey of the denial of service problem.BSc Programmes in Engineering Computer Engineering.
[5] Peddisetty, N.R., 2005. State-of-the-art Intrusion Detection: Technology, Challenges, and Evaluation.
[6] Spafford, E.H. and Zamboni, D., 2000. Intrusion detection using autonomous agents. Computer networks, 34(4), pp.547-570.
[7] Sobh, T.S., 2006. Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art. Computer Standards & Interfaces, 28(6), pp.670-694.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY