American Journal of Operations Management and Information Systems
2017; 2(1): 1-4
http://www.sciencepublishinggroup.com/j/ajomis
doi: 10.11648/j.ajomis.20170201.11

Wireless Network Security Threats, Vulnerabilities and Their Defences

Alex Roney Mathew*, Aayad Al Hajj

IT Department, College of Applied Sciences, Sohar, Sultanate of Oman

Email address:
dr.alex.soh@cas.edu.om (A. R. Mathew), aayad_hajj.soh@cas.edu.om (A. Al Hajj)
*Corresponding author

To cite this article:
Alex Roney Mathew, Aayad Al Hajj. Wireless Network Security Threats, Vulnerabilities and Their Defences. *American Journal of Operations Management and Information Systems.* Vol. 2, No. 1, 2017, pp. 1-4. doi: 10.11648/j.ajomis.20170201.11

Received: October 30, 2016; **Accepted**: November 22, 2016; **Published**: January 3, 2017

Abstract: Interchanges through PCs, laptops, tablets, and mobiles nowadays triggered the spread of remote systems administration to reach high levels throughout the globe. Security issues have risen considerably in Wi-Fi systems due to the unapproved clients and Wi-Fi programmers. Thus to eliminate conceivable security issues, WEP (Wired Equivalent Privacy) and WPA (Wireless Fidelity Protected Access) have been proposed in this paper. Both of these conventions are by large used to scramble the present information and data preventing unapproved clients and Wireless Fidelity (Wi-Fi) programmers from decoding the information and hacking the Wi-Fi systems. Anybody within the range of the Wireless Fidelity system can connect to it with the help the Access Point (AP). In addition the Universal Mobile Telecommunications System (UMTS) system is contrasted with Wi-Fi Network for better execution in security.

Keywords: Wi-Fi, WEP, WPA, WLAN, AP, UMTS, WSA, ICE

1. Introduction

The smart phones PDA's utilization progressively on the rise, places where individuals perform figuring are spreading. System network, then again, has turned into a vital piece of registering. It is anything but difficult to see why remote systems administration is being utilized on an inexorably bigger scale. As it is with wired systems, remote systems are as of now confronting various security challenges: defects and vulnerabilities can be misused by pernicious programmers to get entrance into remote framework designs. Wi-Fi system is confronting numerous security issues due to programmers and unapproved individuals. The Wi-Fi programmer utilizes Wireless Hacking instruments such as: AirSnort, Aircrack, WepAttack, WEPCrack and others over the system.

Remote neighbourhood Wireless Local Area Network (WLAN) has been generally utilized as a part of numerous divisions. The ubiquity picked up is because of numerous reasons, for example, simplicity of establishment, establishment adaptability, diminished expense of proprietorship and versatility. On the other hand, WLAN have some security dangers which individuals using it or mean to utilize it should recognize.

The basic segment of the paper gives brief description of WLAN parts and its design. With a specific end goal to analyse the WLAN security dangers, this paper will take a look at Denial of Service (DoS), Spoofing and Eavesdropping. The paper will then clarify how Wired Equivalent Privacy (WEP) functions, which is the IEEE 802.11b/WiFi standard encryption for remote systems administration. The discourse of WEP proceeds by inspecting its shortcomings, which result in it being a great deal less secured than what was initially proposed. This circumstance prompts further research with respect to down to earth arrangements in actualizing a more secured WLAN.

This paper will similarly cover the new benchmarks to enhance the security of WLAN, for example, the IEEE 802.1x standard, which contains three isolated segments: Point-to-Point Protocol (PPP), Extensible Authentication Protocol (EAP) and 802.1x itself. The 802.1x is really incorporated into 802.11i, a recently proposed standard for key circulation and encryption that will assume a major part in enhancing the general security abilities of present and

future WLAN systems. The 802.11i standard gives two enhanced encryption calculations to supplant WEP, which are Temporal Key Integrity Protocol (TKIP) and CBC-MAC Protocol (CCMP). This paper will likewise list down a few items that will help clients to shield their remote systems from assaults. Finally, this paper closes with the highlighted issues and arrangements.

2. Practical Solutions for Securing WLAN

In spite of the dangers and vulnerabilities connected with remote systems administration, there are absolutely conditions that demand their utilization. Indeed, even with the WEP imperfections, it is still workable for clients to secure their WLAN to a worthy level. This should be possible by actualizing the accompanying activities to minimize assaults into the primary systems.

2.1. Changing Default SSID

Administration Set Identifier (SSID) is a special identifier joined to the header of bundles sent over a WLAN that goes about as a secret key when a cell phone tries to associate with a specific WLAN. The SSID separates one WLAN from another, so all entrance efforts and all gadgets attempting to interface with a particular WLAN must utilize the same SSID. Thus, it is the main security component that the entrance directs requires toward empower relationship without actuating discretionary security highlights. Not changing the default SSID is a standout amongst the most widely recognized security botches made by WLAN directors. This is proportional to leaving a default secret key set up.

2.2. Utilize VPN

A VPN (Virtual Private Network) is a significantly more complete arrangement in a way that it validates clients originating from an entrusted space and scrambles their correspondence so somebody listening can't block it. Remote AP is put behind the corporate firewall inside a commonplace remote usage. This sort of usage opens up a major gap inside the trusted system space. A safe technique for executing a remote AP is to place it behind a VPN server. This kind of execution gives high security to the remote system usage without adding noteworthy overhead to the clients. On the off chance that there is more than one remote AP in the association, it is prescribed to run every one of them into a typical switch, then interfacing the VPN server to the same switch. At that point, the desktop clients won't need numerous VPN dial-up associations designed on their desktops. They will dependably be confirming to the same VPN server regardless of which remote AP they have related.

2.3. Utilize Static IP

Of course, most remote LANs use DHCP (Dynamic Host Configuration Protocol) to automatically assign an IP address to a client. One issue is that DHCP does not separate an honest to goodness client from a programmer. With an appropriate SSID, anybody executing DHCP will acquire an IP address naturally and turn into an honest to goodness hub on the system. By incapacitating DHCP and doling out static IP locations to every remote client, you can minimize the likelihood of the programmer acquiring a legitimate IP address. This constrains their capacity to get to network administrations. Then again, somebody can utilize an 802.11 parcel analyser to sniff the trading of edges over the system and realize what IP locations are being used. This helps the gatecrasher to think about what IP location to utilize that falls inside the scope of ones being used. In this way, the utilization of static IP locations is not trick confirmation but rather it is a hindrance. Additionally remember that the utilization of static IP addresses in bigger systems is extremely lumbering which may provoke system administrators to utilize DHCP to stay away from bolster issues.

2.4. Access Point Placement

WLAN access focuses ought to be set outside the firewall to shield interlopers from getting to corporate system assets. Firewall can be arranged to empower just true blue clients in view of MAC and IP addresses. This is in no way shape or form a last or perfect arrangement since MAC and IP locations can be parodied despite the fact that this makes it troublesome for a programmer to emulate.

3. Tools for Protecting WLAN

There are few items that can minimize the security dangers of WLAN; the following summarizes some of these tools.

3.1. Air Defense™

It is a business remote LAN interruption security and administration framework that finds system vulnerabilities, recognizes and shields a WLAN from interlopers and assaults and helps with the administration of a WLAN. AirDefense likewise has the ability to find vulnerabilities and dangers in a WLAN, maverick APs and specially appointed systems as examples. Aside from securing a WLAN from every one of the dangers, it additionally gives a powerful WLAN administration usefulness that permits clients to comprehend their system, screen system execution and uphold system approaches.

3.2. Minimize Radio Wave Propagation in Non-user Areas

Take a crack at arranging radio wires to abstain from covering zones outside the physically controlled limits of the office. By avoiding open regions such as: parking garages, halls, and contiguous workplaces, the capacity for a gatecrasher to take part on the remote LAN can be altogether diminished. This will likewise minimize the effect of somebody handicapping the remote LAN with sticking systems.

3.3. Isomair Wireless Sentry

It screens the air space of the venture constantly utilizing remarkable and advanced examination innovation to distinguish unreliable access focuses, security dangers and remote system issues. This is a committed machine utilizing an Intelligent Conveyor Engine (ICE) to latently screen remote systems for dangers and educate the security directors when they happen. It is a totally mechanized framework, halfway oversaw and will coordinate consistently with existing security base. No extra man-time is required to work the framework.

3.4. Wireless Security Auditor (WSA)

It is an IBM research model of a 802.11 remote LAN security inspector, running on Linux on an iPAQ PDA (Personal Digital Assistant). WSA systems managers to close any vulnerability via naturally review a remote system for legitimate security arrangement. While there are other 802.11 system analysers such as: Ethereal, Sniffer and Wlandump, WSA goes for convention specialists who need to catch remote parcels for basic investigation. In addition, it is expected for the broader group of onlookers of system installers and directors, who need an approach to effortlessly and rapidly confirm the security setup of their systems, without understanding any of the points of interest of the 802.11 conventions.

The general thought of WLAN was essentially to give a remote system base practically identical to the wired Ethernet systems being used. Since developed, it is still advancing towards offering quick association capacities inside bigger territories. Nonetheless, this expansion of physical limits gives extended access to both approved and unapproved clients that make it characteristically less secure than wired systems. WLAN vulnerabilities are basically brought about by WEP as its security convention. However, these issues could be resolved with the new principles such as 802.11i. For the time being, WLAN clients can ensure their systems by rehearsing the recommended activities that are said in this paper taking into account the expense and the level of security that they wish.

4. Problem Statement

Some sort of informal contact will totally hurt the PCs, cellular telephones and so on utilizing the remote systems. Indeed, even the Wi-Fi can be hacked by the programmers. So security is inadequate in the Wireless Fidelity innovation. To resolve this kind of issue a few strategies has been proposed.

5. Proposed Work

Individuals feel at ease to utilize the web office from the Wireless Access Point. For this sort of security issue, in this paper we have proposed two types of securities. One is known as Wireless Fidelity Protected Access (WPA) and the other as Wired Equivalent Privacy (WEP). To prevent information from meddling eyes, we need to consider encoding such information. Nowadays, the biggest share of the remote supplies comes from Wired Equivalent Privacy and Wireless Fidelity Protected Access. Wired Equivalent Privacy most critical powerless point is that, it makes utilization of static or altered encryption keys. Consider the possibility that you interface a Wi-Fi Router alongside a WEP encryption key and this must be used with every last gadget. At that point your framework or the specific system will scramble the parcels which it accepting and will be further transmitted.

This WEP is entirely considered to create a characteristic security and insurance in the remote correspondence system. Wired Equivalent Privacy (WEP) for securing remote systems is shown. Some sort of sensible WEP breaking can be basically confirmed with some gear like Air split and others. AirSnort have the astounding ability to break the Wired Equivalent Privacy (WEP) feeble keys. 802.11 is a Wi-Fi remote system correspondence standard and it is utilized as a part of quickly developing system. It is held in 802.11 arrangements.

General Universal Mobile Telecommunications System (UMTS) can be joined with the Wi-Fi systems for better correspondence aims in the world web system. This innovation is totally subject to the standard reach. UMTS is considered as a module of the International Telecommunications Union.

The past exploration has effectively demonstrated that the surrender time as of the UMTS system gave to the Wi-Fi system is around 1 to 10 seconds. In actuality, Universal Mobile Telecommunications System makes utilization of wideband guidelines division numerous contacts.

6. Conclusion and Future Work

In this paper, we have presented two wireless traffic encryption schemes namely Wired Equivalent Privacy (WEP) and Wireless Fidelity Protected Access (WPA). This sort of insurances and security strategies can be further more created by the most recent advancements in the field of Wi-Fi. Universal Mobile Telecommunications System can likewise be associated with the Wireless Fidelity (Wi-Fi) system. However, through these sorts of systems and conventions, just a portion of the security issues can be settled. In the future, many of the most recent advances will be instated making it anything but difficult to handle the inevitable Wi-Fi issues.

References

[1] Djabri Fahed and Rongke Liu (2013), “WiFi-Based Localization in Dynamic Indoor Environment Using a Dynamic Neural Network”, International Journal of Machine Learning and Computing, Vol. 3, No. 1.

[2] Gints Jekabsons, Vadim Kairish et al. (2011), "An Analysis of Wi-Fi Based Indoor Positioning Accuracy", Scientific Journal of Riga Technical University Computer Science. Applied Computer Systems, Vol. 47.

[3] Jiangfan Feng, Yanhong Liu (2012), "Wi-Fibased Indoor Navigation with Mobile GIS and Speech Recognition", IJCSI International Journal of Computer Science Issues, Vol. 9, No. 6, pp. 1694-0814.

[4] Kihun Kim, Younghyun Kim, Sangheon Pack and Nakjung Choi (2011), "An SNR-based Admission Control Scheme in Wi-Fi Based Vehicular Networks", EURASIP Journal on Wireless Communications and Networking.

[5] Beck, M., Tews, E.: Practical Attacks against WEP and WPA. In: Proc. 2009 Second ACM Conference on Wireless network Security (Wisec) 2009.

[6] Sriram, V. S. S, Sahoo, G., Agawal, K.K.: Detecting and Eliminating Rouge Access Points in IEEE-802.11 WLAN–A MultiAgent Sourcing Agent Methodology. Birla Institute of Technology, India (2010).

[7] P. Feng, Wireless LAN security issues and solutions, *IEEE Symposium on the Robotics and Applications (ISRA)*, 2012.

[8] Panigrahy, S. K, Jena, S. K, Turuk, A. K.: Security in Bluetooth, RFID and Wireless Sensor Network. In: Proc. 2011 ICCCS'11, India (2011).

[9] Andrew A. Vladimirov, Konstantin V. Gavrilenko and Andrei A. Mikhailovsky: Wi-Foo: The Secrets of Wireless Hacking, Pearson / Addison Wesley (2004).

[10] G. A. Mendez, L. C. D. Silva &A. Punchihewa, *Review of Present IEEE 802.11 "Wi-Fi" Security Issues and of Other Possible Vulnerabilities*, Institute of Information Sciences & Technology, Massey University, New Zealand.

[11] J. S. Park & D. Dicoi, WLAN security: current and future. *IEEE Internet Computing, 7(5)*, 2003, 60-65.