NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 8, ISSUE 9, Sep. -2022

STUDY OF SECURITY IMPROVEMENTS IN WIRELESS NETWORK

Haroon Rashid Hammood Al Dallal
Bachelor's degree, Department Engineering in Communication Techniques,
Al-Furat Al-Awsat Technical University, Najaf, Iraq.
Master's degree, Department Infocommunication Technologies and
Communication Systems, Saratov State Technical University, Saratov, Russia.
haroonra1994@gmail.com

Thimar Falih Yasir Al Sharify
Bachelor's degree, Department Engineering in Communication Techniques,
Al-Furat Al-Awsat Technical University, Najaf, Iraq.
Master's degree, Department Electrical Engineering-
Systems Communication, Imam Reza International University,Iran.
Construction and Projects Department -Presidency Of Wasit University - Wasit - Iraq.
thimarfalih85z@gmail.com

ABSTRACT
Wireless security can be defined as the inhibition of unlawful access or intrusion of devices operated on wireless networks. The global community has witnessed a rapid increment in the distribution of wireless networks due to the rigorous advancement in technology that calls for the intensive use of wireless network systems. Wireless networks are broadly clustered into four major categories, namely, Wireless personal area network (WPAN), wireless Local Area Network (WLAN), Wireless Metropolitan area network (WMAN), and Wireless wide area network (WWAN). The wireless network system is distinct from the contemporary wired system in that communication through this medium is through electromagnetic radiation, not wires, as is the case with wired networks. The nature of the wireless networks makes them more susceptible to threats, and their unique transmission system makes securing the network quite intricate. Although a wireless network comes with enhanced flexibility and portability and a reduced budget for the users, its security features need to be improved to cushion its users from potential threats. This paper focuses on assessing existing and new threats, possible areas of vulnerability in the wireless network system, and probable solutions to curb the threats.

INTRODUCTION

Wireless networks, also known as WI-FI, have gained dominance due to their ability to meet advanced technical requirements and their affordability compared to other networks. The network also allows for flexible installation due to its lack of cabling, which further endeared it to users. The introduction of wireless network technology in any organization or setup creates loopholes for unauthorized users to gain entry into the data transmission systems, intercept conversations and introduce malicious software that could corrupt information. Wireless networks are pervasively available, and extensive usage globally calls for developing more robust security systems to prevent data vandalism, privacy violation, and message distortion due to unauthorized intrusion. Currently, there exists Wired Equivalent privacy and Wi-Fi Protected access as the two major wireless security systems. The existing IEEE 802.11 Security standard has attracted numerous critics due to its porous nature [1].

The standards have numerous loopholes that pose serious security threats to individuals using wireless networks. Thus, it is crucial to work on the improvement of these standards.

IEEE 802.11 is anchored on two primary network architectures: the Ad-Hoc Network and the Infrastructure Network. IEEE.802.11 began its official operation in 1997 to design Medium Access Control (MAC) and Physical Layer (PHY), whose purpose was to aid the wireless connectivity to fixed stations, portable stations, and moving stations of a specified boundary [2]. The initial design of the standards comprises three physical layers, Frequency Hopping Spread Spectrum, Direct Sequence Spread Spectrum, and Infrared. The MAC layers include a channel access mechanism providing two channel access controls: the Distributed Coordination Function and the Point Coordination Function. The two have distinct roles.

RESEARCH QUESTION

The primary purpose of this research paper is to highlight the threats directed at the wireless networks, provide a detailed analysis of the existing flaws in the current security measures and provide suggestions on how to improve the security of wireless networks. Wireless networks are taking over globally with the recent invention of the 5G network. The rapid change, however, brings severe challenges that may choke the whole concept of wireless networks. The main concerns regarding wireless networks are data breaches that violate privacy and integrity and leakage of private information.

METHODOLOGY

Assessment of wireless network performance and identification of potential threats employs two methodologies that work in a complementary manner. The two methods are manual assessment and automated assessment. The manual assessment method is used to analyze the wireless network environment physically. The method may also be used to countercheck the functionality of the computerized assessment method. This method is renowned for identifying potential threats when used frequently. The method, however, is limited to the fact that it only examines the security of a given wireless network at a certain point beyond which it does not guarantee its safety. Automated assessment is a comprehensive, intuitive security mechanism implanted in the wireless network system. It provides prompt feedback on any potential threats to the network.

This research paper will use the qualitative research technique to bring a deeper view of wireless network security. The report will combine various online materials using the random sampling model to gather the required data. The qualitative aspect will help unravel the human understanding of wireless security and the multiple reasons behind the many decisions made concerning the security of wireless networks. The observation and statically evaluation of the numerical data will help in the understanding of the trends as well magnitude of the security threats associated with wireless security networks. The observation and proper interpretation of this data will help predict possible future trends, which can be used to formulate countermeasures. Since our research will confine itself to secondary information already published in journals, books, and articles that best address the research question, we will heavily rely on the qualitative methodology. Our research will therefore revolve around an in-depth analysis of informative secondary data to understand the topic and develop clear recommendations.

RESULTS

Security Threats on Wireless Networks

Based on our research findings, Wireless security threats are grouped according to their nature for easier understanding. The grouping is equally applicable when finding solutions to the existing threats. Firstly, we have the wireless integrity threats, where attackers, in this case, create and send falsified data, control, and management through the wireless networks, thus misdirecting the wireless devices to carry out DOS attacks. Secondly, the wireless confidentiality threat intercepts confidential information relayed through the wireless networks. Such threats can manifest in the form of Honey-pot AP, Evil Twin AP, Cracking WEP Key, or Session Hijacking. Thirdly, we have the wireless access control threats that aim to intrude on wireless network systems by bypassing the WLAN access control measures. Notable WLAN control measures include AP MAC filters and Wi-Fi port access control. We also have wireless authentication threats whose primary focus is to steal the Wi-Fi identity of clients, personal information, and login details. This threat leads to unauthorized network access over time via shared key guessing, VPN login cracking, LEAP cracking, and password guessing.

The preliminary data also shows that unsecured wireless networks are prone to piggybacking. Piggybacking is the aspect of unauthorized users being able to use the network as long as they have wireless-enabled devices and are well within the range of the network. Such unregulated users may be able to carry out illegal activities, monitor or even capture web traffic and steal personal files and data.

The evil twin attack is another well-known attack directed at wireless networks. This occurs when attackers clone the details of a public network access point. They then amplify the signal of the duplicate access point to surpass the signal strength of the authentic network, thus enabling unsuspecting users to connect to the rogue network [4]. The connectivity between the fake network and the victims' devices gives the attacks unfettered access to their data and file, which may lead to data theft, violation of data privacy, and distortion of information. Additionally, the technique can help the attackers to read crucial information such as credit card numbers, user names, and passwords, which can lead to further damage.

Wireless sniffing is also another problem facing the wireless network. Because many public networks are not secured, and communication alongside these networks is not encrypted, they are vulnerable to frequent attacks. Attackers target such networks using wireless sniffing tools to acquire sensitive data and information, including credit cards and passwords used to carry out authorized transactions or share or wrong data.

Lastly, individuals and companies should not overly focus on data breaches as attackers target stealing the gadgets used to access wireless networks such as computers and mobile phones. It is therefore essential for individuals to also focus on safeguarding these devices; if they get lost, it will be impossible for the attackers to access their data. Such measures may include the password on the devices.

Tools Commonly used by Hackers

To access wireless network systems, hackers use several freeware that is readily available on the internet. Understanding these tools and how they function can help wireless network users protect themselves against some attacks. We begin with the Kismet. Kismet is well known as an advanced freeware tool for passive eavesdropping. The device is used to monitor traffic, and data storage, sort

data, determine the connection speed, and graphical map the network and MAC addresses [3]. Hackers also used Airsnort, which helped them decrypt the WEP.

Global Statistics on Wireless Network Attacks

Based on our static findings, global data exhibits a relative rise in security threats over the wireless network systems due to increased users. The majority of these threats are attributed to human error. This is mainly because there is an acute shortage of cyber security experts, and not unless this is resolved, there is a likelihood of this trend persisting in the coming years. The global information security market is rapidly expanding because a more significant percentage of organizations are striving to safeguard their data against potential cyber threats.

An estimated 95% of cyber security breaches originate from human error due to the lack of relevant skills. Further research reveals that about 45 percent of the attacks experienced are due to inside jobs, either intentional or accidental [5]. A considerable number of these breaches are directly linked to financial motives that as data breaches for ransom. In 2021 the number of recorded data breach cases was 1862, with a majority of the attacks emanating from phishing at 40 percent, 22 percent hacking, and 11 percent malware intrusion. The 2021 data breach cases exposed about 22 billion data records containing personal, state, and company data. Additionally, available research data indicates that the top malicious email attachments that carried the malware are .doc and .dot, constituting 37 percent, followed by the .exe at 19.5 percent.

In 2021 LinkedIn experienced a data breach that exposed the personal information of about 93 percent of its users, representing about 700 million users. In the same year, Microsoft experienced an attack that took place in march affecting about thirty thousand organizations in the United States [5]. Among the affected organizations include private businesses and government agencies. Subsequently, the United States of America experienced another cyber-attack carried out on the colonial pipeline company that led to unexpected fuel shortages across the U.S.

In 2021 there was another attack on Twitter targeting access to crucial information on about 130 accounts that included the then U.S president, Tesla C.E.O Elon Musk. The attack resulted in the theft of Bitcoins valued at $120,000. The statistics of these recurrent cyber-crimes show how the topic of cyber security is crucial, especially in a world where almost everything is being digitized, thus creating avenues for cyber-attacks.

Trends Changing Cyber Security

The adoption of cloud computing and its attached services is gaining momentum as companies incorporate it into their operations. The massive adoption of cloud computing escalates the challenges experienced in the wireless network space. The rise in web applications in the cloud calls for the holistic evolution of the policy controls governing the cloud services and the web application to safeguard valuable data. Cloud has been cited for having higher growth potential, attracting significant security concerns that need to be urgently addressed.

There is an increase in the usage of encryption codes to safeguard data. Encryption can be defined as the process of encoding information in a way that locks out eavesdropping as well as hackers. The encryption process results in the transformation of easily readable data into a more complex text that is had to be read through an encryption algorithm. The end user will require a decryption code to access the encrypted data.

Drawbacks in Addressing the Wireless Network Security

The tendency of organizations to rely on other individuals to safeguard their wireless networks increases their vulnerability. With the global connectivity expected to rise to an all-time high of 27 billion devices due to the inception of the 5G network, many users will most likely operate in an environment that is quite uncertain and intricate for them to understand the surrounding threats. Therefore, organizations must work on understanding the breadth and magnitude of hazards likely to occur due to their continued usage of wireless networks.

The lack of adequate cyber security personnel has made the struggle to secure wireless networks futile. Companies, therefore, need to actively work on building their workforce through facilitated training and frequent seminars. This will help them gain the ability to detect possible threats and formulate proper rebuttals to evade further destruction of data or leakage of crucial information. Adequate planning for the mitigation strategies against threats directed at the wireless networks will determine companies' future growth and success.

The rise of general cyber-attacks, some directed toward wireless networks, is directly attributed to the fact that it is challenging to trace, arrest, and prosecute cyber criminals. The available statistics show that a meager 0.05% of such cases were solved conclusively by involving arrests and prosecution of culprits. Many attackers operate anonymously through the dark web, launching attacks on unsuspecting victims. It is tough to trace such individuals since they work in disguise. The availability of the dark web provides an avenue for the ready workforce to be hired at any time to launch attacks. Additionally, there is a need for the security agencies to work closely with the cyber security aspects to come up with the internationally accepted criteria for attribution, evidence, and synchronized efforts in the war against these criminals.

DISCUSSION

Protocols to Enhance Wireless Network Security

Upon understanding the various threats that wireless networks face, some proposals have been put forward to salvage the situation. It is crucial to restrict the number and type of users that can successfully log into a wireless network system. Every device connected to a network system automatically has q media access control. It is possible to lock out unwanted users to the wireless network by filtering their MAC addresses. Additionally, it is advised that while giving access to your visitors to the wireless network, use the guest feature, which allows your guest to access the web on a separate wireless channel, thus safeguarding the privacy of data on the main track. It is worth noting that the guest feature bares its unique password; hence, it does not affect the main channel.

Frequent password change has also been cited as one of the crucial mechanisms to safeguard wireless networks. Most of the used network devices come with a pre-configured default password that can easily be retrieved online. It is therefore very urgent that the users change these passwords upon purchase of the devices to limit the possibility of unwanted intrusion. Changing the original default password renders unauthorized users powerless and provides a formidable shield to the devices.

Consequently, Wireless Access Point (WAP) hardware substantively reduces the possibility of attacks on a wireless network. WAP facilitates wireless communication between mobile computers and PDAs, enabling them to connect to different wireless networks [6]. The WAP hardware provides connectivities between wired networks and wireless access points and safeguarding and links the data being transferred between wired and wireless gadgets.

Additionally, incorporating Service Set Identifier SSID offers configurable identification that limits communication within the specified wireless network to users with the appropriate SSID. SSID, therefore, serves as a co-shared password between specific clients and access points.

Wi-Fi Protected Access is another crucial element used to enhance wireless networks' security. Wi-Fi Protected Access is a command that identifies, fixes, and promptly addresses critical security issues raised within the WEP. Through its temporal key integrity protocol, WAP provides data security, thus giving users the assurance that their data is safe. Inventors have incorporated the 8002.1x to enhance the authentication of WAP. WAP 2 is also linked to the IEEE 802.11i and is actually one of the recent advancements in the safety of wireless networks. The WAP 2 security system only allows authorized users to access the wireless network devices, thus locking out intruders and potential threats. The WAP 2 also has unique features that support cryptography and offer more vital protection in terms of key management, authentication tools, replay attack protection, and data integrity.

Additionally, the introduction of the Wired Equivalent Privacy Protocol into the IEEE 802.11 standards has increased the confidentiality of data across wireless networks. The system operates through encryption of data and information being circulated across different endpoints of the wireless networks. WEP, however, is highly vulnerable to attacks as it can easily be cracked by hackers using several automated tools. Thus WEP needs to be combined with other safety tools to guarantee the safety of data and information. One of the most frequently used systems to compliment the WEP is the Open System Authentication, a default authentication protocol captured in the IEEE 802.11M standards. The open system Authentication comprises simplified authentication requests that feature the station ID and the authentication response. The WEP is often merged with the Open system authentication to offer enhanced security to the communication undertaken on the wireless networks.

Installing a firewall into the wireless devices also offers greater reproof in terms of security to the user. Both modem and host-based firewalls are essential in providing security across the wireless network. Host-based firewall units offer an additional protection layer to the user's data in the event that the attackers can gain entry through the modem-based firewall. A combination of the two, therefore, is considered more powerful.

Users of wireless networks are also encouraged to use Virtual private networks while connecting to the wireless networks. The virtual private network provides a secure environment for users to connect to wireless networks when away from their usual networks. The Virtual Private network safeguards the user by encrypting the data at the receiving and sending point, thus locking out all unauthorized users who do not have the proper encryption. Users are usually advised to log in to their respective Virtual Private networks before eventually connecting to the wireless networks.

Proper encryption of data on the wireless network consequently secures the data from being accessed by intruders. A number of data encryption protocols exist that the user can use to safeguard data. Wi-Fi protected access 3 (WAP 3) is highly recommended regarding the data encryption protocol. WAP 3 provides more robust encryption to the data transmitted across the wireless networks from the wireless router to the wireless devices. Users are advised to purchase equipment that is WAP 3 enabled for more accessible encryption of data to prevent a data breach.

Additionally, the cautious usage of file sharing and proper maintenance of the anti-virus software safeguards the users' devices while using the wireless networks. Anti-virus systems have programs that help detect and protect devices against the spywares and adware, thus securing the devices. Careful selection of file sharing prevents possible attacks that originate from unregulated data sharing. Users are advised to have default settings that only allow for data sharing over the home or

work networks and not public networks. Additionally, the use of password protection for data transmitted also provides additional safety to data preventing accessibility by unauthorized individuals should the information be mistakenly sent to the wrong recipient. Creating a dedicated folder for shared files and restricting access to other folders also prevents the spread of malware that can be introduced to the device through the shared data.

Regular updates of the access point software as directed by the manufacturer further augments the security of your devices. Manufacturers are constantly working on improving their software; among the items they emphasize is data security. The periodic updates initiated by the manufacturer come with improved security systems for the devices. Thus, regular updates can help secure your devices. Users are advised to regularly check the manufacturer's website for updates and promptly update their devices.

Secure Socket Layer and Transport Layer Security are majorly utilized by web resources to provide secure data transfer. A combination of HTTP with the TSL is referred to as the HTTPS and is gaining more popularity globally due to its success rate in combating cyber threats. TSL employs asymmetric cryptography to ensure connection privacy, and the integrated message integrity ensures that the integrity of the transmitted data is upheld. The two measures make the MITM attacks harder to be undertaken and provide a reasonable avenue to detect such attacks, thus making unlawful data extraction impossible. Although HTTPS does not eliminate the threats associated with MITM, it redirects their scope of attacks to dedicated targets such as corporate networks. Despite its demerits, HTTPS is still a viable security solution that should be used, especially when operating devices over public WLAN.

CONCLUSION

The wireless network's security is a crucial element that should not be overlooked. There are so many users of the wireless network whose personal data must be safeguarded. The is a need to upgrade different security protocols being used in the wireless network. Additionally, there should be intensified calls on training adequate cyber security personnel to aid in the traction, identification, and possibly prevent attacks. The amount of money and data lost through attacks on wireless networks need to be curbed to ensure proper advancement of the wireless networks.

Consequently, companies involved in the distribution and connection of wireless networks need to have appropriate structures to deal with potential dangers. The advancement of such technologies should equally tag along with improving security measures. For instance, the 5G network should be susceptible to the same threats that threaten to bring down the 4G networks. Data transfer and communication efficiency should be closely complimented by the security of the communication or data, thus enhancing data integrity and privacy.

There is also the need to conduct civic education specifically for individuals handling data in organizations such as banks and government agencies on the need to use the available security mechanisms to prevent attacks. Data encryption, use of VPN, and restriction of access to networks are among the key recommendations whose effects dramatically lower the possibility of being attacked while operating on a wireless network.

REFERENCES

1. "IEEE SA - IEEE Standard for Information Technology--Telecommunications and Information Exchange between Systems Local and Metropolitan Area Networks--Specific Requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications." IEEE Standards Association, https://standards.ieee.org/ieee/802.11/5536/.
2. DHINGRA, MADHAVI, et al. "Wireless Network Security Threats and Their Solutions: A Short Study." International Journal of Smart Sensor and Adhoc Network., 2013, pp. 205–210., https://doi.org/10.47893/ijssan.2013.1165.
3. Kismet, https://www.kismetwireless.net/.
4. Phungglan, Jeff. "What Is an Evil Twin Attack and How to Prevent It?" MacPaw, MacPaw, 5 Aug. 2022, https://macpaw.com/how-to/detect-evil-twin-attack.
5. Sobers, Rob. "166 Cybersecurity Statistics and Trends [Updated 2022]." Varonis, Varonis, 3 Aug. 2022, https://www.varonis.com/blog/cybersecurity-statistics.
6. Zhang, Peng, and Chuang Lin. "Security Threats in Network Coding." Wireless Networks, 2016, pp. 9–19., https://doi.org/10.1007/978-3-319-31083-1_2.