International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Comparison of Wireless Lan (Wlan) Security Protocols Vulnerabilities

Igwe Chinedu S. & Okafor Obinna J.
Department of Information Management Technology, Federal University of TechnologyOwerri (FUTO), Nigeria.

ABSTRACT
Nowadays, due to the rapid proliferation of mobile devices, wireless local area network (WLAN) has been deployed in almost every possible sector of networking.WLAN provides wireless network communication over short distances using radio signals compared to the traditional LAN network cabling. It provides many advantages which include enabling access to computing resources for devices that are not physically connected to network (Rumale and Chaudhari, 2011). However, WLAN also is coupled with new security threats and alters the organization's overall information security risk profile. In order to secure the WLANs, there are currently three main security protocols available to WLAN communication: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and 802.11i (WPA2) standards. However, there still exist some levels of vulnerabilities among these protocols. In this paper, an in depth analysis of these protocols was presented. The security vulnerabilities that exist in them were analyzed and explained. This would be a guideline in terms of choosing the right and best possible security protocol and measures to be implemented to secure WLANs established in homes and business enterprises.

Keywords: **Wireless LAN, Vulnerabilities, Security, WLAN Technologies, Wi-Fi hack, WEP, WPA/WPA2, Threats.**

1.0 INTRODUCTION

Wireless local area Network (WLAN) provides wireless network communication over short distances using radio signals instead of traditional network cabling (Pratim Kar, 2013). WLAN enables access to computing resources for devices that are not physically connected to network (Rumale and Chaudhari, 2011). According to Jiang and Garuba (2008), wireless networking increases the flexibility in the home, work place and community to connect to the internet without being tied to a single location. Since its inception, the IEEE 802.11 Wireless Local Area Network (WLAN) has become one of the most popular means of setting up networking technology. It has been deployed in almost every possible sector of networking due to the rapid proliferation of mobile devices. One of the main reasons for its popularity is that it provides the support of a normal local area network and also allows the moving of any network device without the added complexity of cabling and costing within the coverage area of that Wireless LAN (Md Waliullah, A B M Moniruzzaman and Md. Sadekur Rahman, 2015). WLANs are increasingly used within home and business environment due to the convenience, mobility, and affordable prices for wireless devices. WLAN gives mobility and flexibility to users in homes and hot spot environments, such as airports and campuses. Today, the IT technology is mostly based on the wireless connection followed by the development of wireless network-enabled devices (Cache and Liu, 2010).However, security is one of the main problems that have been faced by the wireless network. Wireless LAN networks are generally designed with emphasis on convenience rather than security. This is exactly where the problem lies. On a wireless network almost anyone with a WLAN enabled device can easily connect to and penetrate other users systems (Misic, 2008). The problem with security can never be solved fully but it can be minimized. Depending on the business needs and requirements it is very much important to address wireless network security more efficiently (Bansal and Mahajan, 2013). The wide range of usage emphasizes the importance of having a secure network and protect from potential break in. In order to do so, mostly encryptions such as the Wired Equivalent Privacy (WEP) and the Wi-Fi- Protected Access (WPA/WPA2) are used (Kizza, 2011). This allows the transmitted data within the network to be encrypted. Research based and findings will illustrate just how easy it is to protect from malicious attacks by simply using a combination of strong encryption protocol and complex key.This paper looks at the security tools available for WLANs and their practicality in order to increase security awareness.

1.1 Overview of Computer Networks

According to Cisco systems (2007), a network is a connected collection of devices that can communicate with each other. A network can also be defined as a group of interconnected computers and other devices, such as printers. The interconnection between these devices take place using various media types; these media types could be wired or wireless (ACE, 2015). Computer networks offer lots of benefits, like carrying of data in many kinds of environments, including homes, small businesses, and large enterprises (Cisco Systems, 2007).

Networks can be classified based on geographical location of the network components, topology, and location of network resources. Based on the geographical distance, a network is classified as follows: local area network (LAN), campus area network (CAN), metropolitan area network (MAN), and wide area network (WAN). A local area network (LAN) provides connectivity in limited areas, such as a building or a small office. While CAN connects different LANs within the same campus, and is typically used by businesses or universities that have more than one building inside one campus. WAN covers regional and national boundaries, and is mostly used in organizations that operate in several branches at different locations (ACE, 2015).

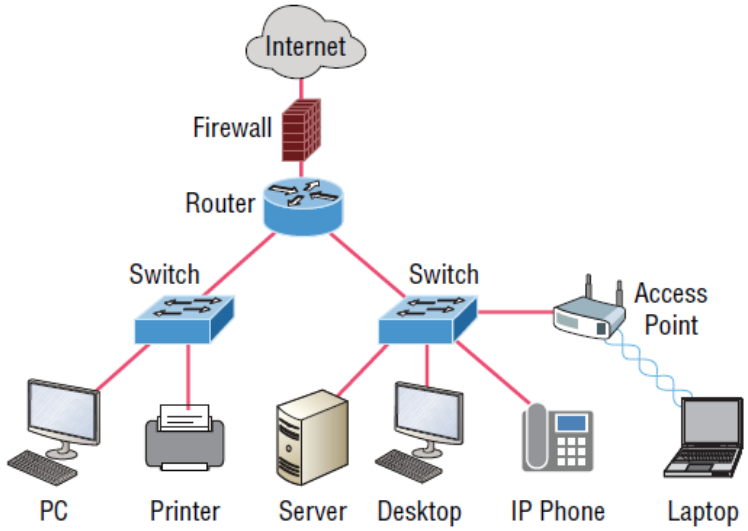

Figure 1.1 Physical Components of a Network (Lammle, 2016)

According to ACE, (2015), within a local area network (LAN), the interconnection between network devices takes places using various media types which can be either wired (LAN) or wireless (WLAN).

1.1.1 Wireless Local Area Networks (WLANs)

A WLAN is an extension of a wired LAN, connecting to it through a device called a wireless access point (AP). The access point relays data signals between all of the devices in the network, including file servers, printers, and even other access point -and wireless devices connected to them. Usually, APs are connected to an existing wired LAN infrastructure that provides connectivity to the network and to the Internet. Each computer on the WLAN has a wireless network interface card (NIC). This card performs the same basic functions and looks similar to a traditional NIC except that it does not have a cable that connects it to a network jack in the wall. Instead, the wireless NIC has an antenna built into it (Kumar and Gambhir, 2014). As shown in figure 1.2, implementing a wireless LAN involves setting up an infrastructure consisting of multiple access points. Computers that are equipped with wireless Network Interface Cards (NICs) would communicate with the nearest AP which provides simultaneous network connectivity to multiple computers (Kahai, P and Kahai, S., 2005).

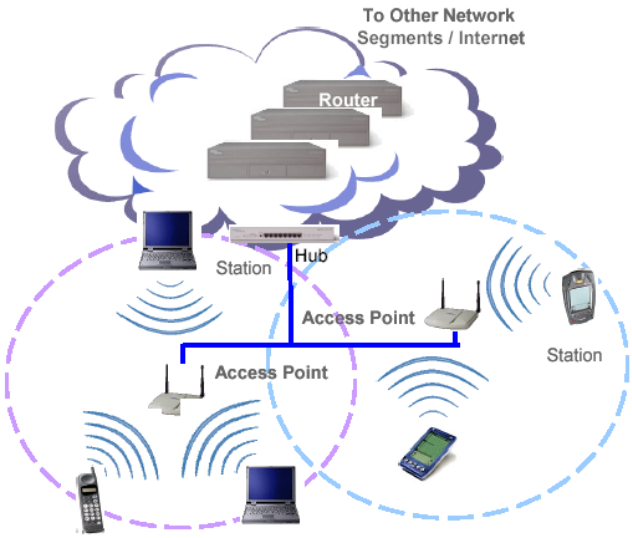

Figure 1.2 Wireless LAN Architecture (S. Kahai and S. Kahai, 2005)

One of the main reasons for its popularity is that it provides the support of a normal local area network and also allows the moving of any network device without the added complexity of cabling and costing within the coverage area of that Wireless LAN (Md Waliullah, A B M Moniruzzaman and Md. Sadekur Rahman, 2015). WLANs are increasingly used within home and business environment due to the convenience, mobility, and affordable prices for wireless devices. WLAN gives mobility and flexibility to users in homes and hot spot environments, such as airports and campuses. Today, the IT technology is mostly based on the wireless connection followed by the development of wireless network-enabled devices (Cache and Liu, 2010).

According to the Wi-Fi Alliance (2001), one of the major reasons for deploying WLANs is mobility. Users who are on the go or need to be mobile within an office complex generally would prefer to have access to their e-mail or resources on an Intranet for meetings or providing needed information to clients or customers. Such users equipped with a laptop that has a wireless NIC are able to get access to network resources and the Internet (assuming that wireless infrastructure is in place). Thus, wireless connectivity is always most beneficial for, and is most used by, mobile users (Wi-Fi Alliance, 2001).

A second reason is the high expenses of wiring buildings, both for access to the network and possibly for electrical outlets. It usually turns out to be less expensive to install wireless APs than it is to wire for network jacks. Network wiring involves laying cable either through available ducts in the floor or through ceilings and walls. Such cabling can involve a lot of effort and expense, both of which can be avoided if wireless infrastructure is used.

A third reason for WLAN deployment is the ability to provide network connectivity in places where providing wired connectivity is difficult. On university campuses that have older buildings which were not pre-wired for network connectivity, providing wall jacks becomes a difficult task. Also, in situations where network connectivity needs to be set up on a temporary basis, wireless connectivity can be provided relatively easily and less expensively.

WLANs operate base on networking standards established by the Institute of Electrical and Electronic Engineers (IEEE.) The WLAN developments, maintenance and standard creation is provided by the IEEE, which is the world's leading professional association for the advancement of technology (IEEE, 2011). The IEEE refers to WLAN by its technical name: IEEE 802.11. 802.11 standards cover all versions of WLAN technology. There are different types of 802.11 including B, G, and N, as the most common versions in use today (Burns, 2007). During further developments of 802.11, the IEEE Standards Board specified the types of security

2.0 WLAN Security/Encryption Protocols

Wireless Local Area Network Security is necessary because WLAN signals have no physical boundary limitations, and are prone to illegitimate access over network resources, resulting in the vulnerability of private and confidential data. Furthermore, the emergence of Wi-Fi as the primary access technology at home, the rising popularity of public hotspots, and the deployment of enterprise networks carrying sensitive and mission-critical data increased the security requirements for Wi-Fi. Network operations and availability can also be compromised in case of a WLAN security breech. To address these issues, various authentications, encryption, invisibility and other administrative controlling techniques are used in WLANs. Business and corporate WLANs in particular require adequate security measures to detect, prevent and block eavesdroppers and other intruders.Security is one of the main problems that have been faced by the wireless network. Wireless LAN networks are generally designed with emphasis on convenience rather than security. This is exactly where the problem lies. On a wireless network almost anyone with a WLAN enabled device can easily connect to and penetrate other users systems (Misic, 2008).

In order to mitigate the security vulnerability in WLANs, there are currently three main encryption technologies available to WLAN communication: WEP, WPA, and WPA2. These technologies attempt to provide Confidentiality, Integrity and Authentication. However, they do not all succeed at these tasks and introduce vulnerabilities into the WLANs.

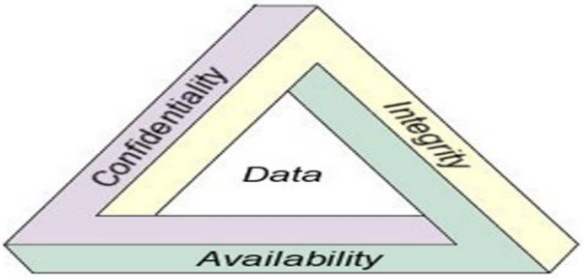

Figure 2.1 CIA Triad (I.S.S.W.G, 2011)

2.1 Technology Overview of WEP

Wired Equivalent Privacy (WEP) is a security protocol for IEEE 802.11 Wireless Local Area Networks (WLANs) introduced as a part of original 802.11 standard ratified in September 1999 (Vibhuti, 2005). Its intention was to provide data confidentiality comparable to that of a traditional wired network. As the name (Wired Equivalent) suggests, its intention has never been to make WLAN a 100 per cent secure, but to provide the same security as in a wired network. WEP was built for the encryption of the network traffic, the data integrity and station authentication. These 3 core elements attempt to satisfy the security objectives: Authenticity, Integrity and Confidentiality (Howard and Prince, 2010). However, Borisov et al. (2001) has proved that vulnerabilities exist for each of them; therefore none of the security objectives can be reached. Despite these issues, WEP is still widely deployed, thus it is necessary to explore further its vulnerabilities.

2.1.1 WEP Security Analysis

Leading research of the insecurity of WEP was done by Walker (2000) who concluded that the WEP was unsafe at any key size and that it could not meet its design goal which was to provide data privacy to the level of a wired network. Borisov et al (2001) presented the first serious paper on WEP insecurity receiving a high volume of controversy in the press. Only a month later Fluhrer, Mantin and Shamir (FMS) (2001) published a paper called “Weaknesses in the Key Scheduling Algorithm of RC4" describing an attack on the ‘key scheduling algorithm’ used by WEP. The FMS attack was only theoretical, yet it did not take long till it got adapted into the real world.

Nevertheless, it was FMS that started the downfall of the WEP. According to Gast (2005) it only took a week for his group of students, including the delivery of the WLAN Card, to crack the WEP key. However, these tests where purely experimental and no easy-to use tools were available to the public at the time. Yet,

this soon changed when an open source tool called AirSnort was released for Linux, allowing anyone with a computer and networking knowledge to hack into a Wireless LAN (AirSnort, 2011). The first attempt to counter this attack was made by Agere Systems, who developed more secure version of WEP called 'WEPPlus' or WEP+. It greatly reduces the amount of 'weak IV' produced by normal WEP implementations and was released as a firmware update for their own access points (Burns, 2007). Simultaneously, Cisco Systems (2001) decided to go for a different approach and introduced 'Dynamic WEP Keys' to their Aironet WLAN Products. Unfortunately, the issue with solutions discussed above is that they are vendor specific and incompatible with each other. Matters got worse for WEP in 2004, when a hacker known as 'Korek' replied to a thread on the Netstumbler forum about WEP security. The attack, he described, was no longer dependent on weak IV. The 'Korek attack' used statistical crypto-analysis and proved to be more efficient than the FMS attack (Beaver and McClure, 2010). In 2007, a new generation of WEP attacks was published by Tews, Weinmann, and Pyshkin. Their attack called PTW introduced new concepts, which allow breaking into WEP in less than a minute. The KoreK and PTW attacks were quickly integrated into WEP cracking and WLAN auditing tools and are now the standards for attacking WEP protected WLANs (Aircrack-ng, 2010).

2.1.2 WEP Mode of Operation

I. Authentication

According to Beaver and McClure (2010) process of authentication is used to verify that a valid user is trying to connect to the network. In WEP there are two approaches to do this: **open system authentication** and **shared key authentication.**

a.) Open Authentication is not really any authentication at all, because when a station wants to authenticate, the AP always accepts the request and allows a station to join the network.

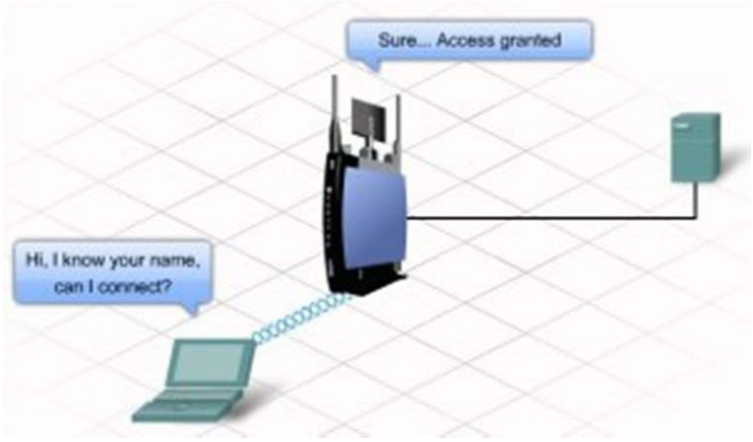

Figure 2.2 Open Authentication (Bel, 2009)

This is a device-based authentication scheme as the user does not need to provide a valid user ID or password. Instead, the MAC address of the connecting node is used to identify it. Borisov (2001) in his early research highlights the possibility to configure the MAC addresses of the permitted clients with their access points. However, this approach does not provide the desired security as it is easy to spoof an address.

b.) Shared key Authentication uses four messages (Figure 2-3). When a station requests Authentication the AP sends a challenge-text in the form of a 40 or 128-bit number. The Station encrypts this text with the WEP secret key, **sends** it back to the AP which decrypts the text, checks if it is the correct one and then grants access to the network.

Figure 2.3 WEP authentication process (Cisco Support, 2008)

This process only authenticates the station to the access point, not the other way around; therefore a malicious AP can simply pretend that the authentication was successful without knowing the secret key (Gast, 2005).

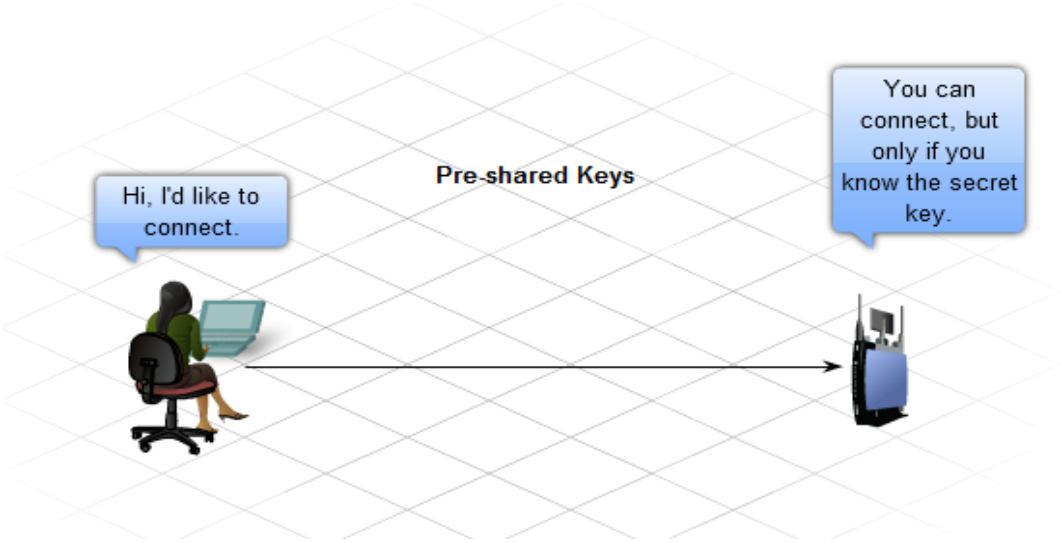

Figure 2.4 WEP one way Authentication (Bel, 2009)

WEP uses the RC4 algorithm to encrypt data messages. This algorithm uses a stream cipher meaning that every byte is encrypted individually with the WEP key. The decryption is the reverse of this process and uses the same key (Fluhrer et al, 2001). Usually the cipher key has 64 or 128 bit and consists of 24 bit initialization vector (IV and 104 bit key). An IV is used to produce a single key-stream for each frame transmitted. The IV is sent in plain text with the encrypted packet, therefore can be viewed by a packet sniffer (Lockhart, 2006). This is a major flaw of WEP encryption. As said by Flickenger (2006) the fact that the same key is used for all frames transmitted in the WLAN network it makes penetration test much easier. When WEP is active in a wireless LAN, each 802.11 packet is encrypted separately with an RC4 cipher stream generated by a 64-bit or 128 bit RC4 key. This key is composed of a 24-bit initialization vector (IV) and a 40-bit or 104-bit WEP key. The encrypted packet is generated with

a bitwise exclusive OR (XOR) of the original packet and the RC4 stream. The IV is dynamically chosen by the sending device and changes periodically so every packet won't be encrypted with the same cipher stream. The IV is sent in the clear with each packet. An additional 4-byte Integrity Check Value (ICV) is computed on the original packet and appended to the end. The ICV (be careful not to confuse this with the IV) is also encrypted with the RC4 cipher stream.

2.1.3 WEP Weaknesses

WEP has been widely criticized for a number of weaknesses. Some of the main weaknesses of WEP are discussed below (iLabs Wireless Security Team, 2011).

(I) Key management and key size

Key management is not specified in the WEP standard and, therefore, is one of its weaknesses, because without interoperable key management, keys will tend to be long-lived and of poor quality. Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access points and client stations must be programmed with the same WEP key. Since synchronizing the change of keys is tedious and difficult, keys are seldom changed.

In addition, the size of the key - 40 bits - has been cited as a weakness of WEP. When the standard was written in 1997, 40-bit keys were considered reasonable for some applications. Since the goal was to protect against "casual eavesdropping" it seemed sufficient at the time. The U.S. did not tightly control exports of 40-bit encryption, and the IEEE wanted to ensure exportability of wireless devices.The 802.11 standard does not specify any WEP key sizes other than 40 bits. Most vendors have implemented a de facto standard, simply extending the key size to 104 bits, with excellent interoperability. You will often see this called a "128-bit" WEP key (because it sounds better than a 104-bit key), but that is not a fair comparison. This is why you enter 13 characters (or 26 hexadecimal digits) instead of 16 characters when you set up a long WEP key. In either case (40 bits or 104 bits), the RC4 encryption key includes a 24-bit IV. Obviously, 104-bit keys are more resistant to brute-force attacks than 40-bit keys. For example, if it were to take on average of one week for a brute-force attacker to find a 40-bit key, that attacker would not be able to find a 104-bit key in a billion years (it's actually much, much longer than that). But brute-force attacks on 104-bit keys are not considered the primary weakness of WEP.

(II) The IV is too small

WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. Remember that the RC4 cipher stream is XOR-ed with the original packet to give the encrypted packet that is transmitted, and the IV is sent in the clear with each packet. The problem is IV reuse. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV or can forge packets. Since there are only 16 million IV values, how the IV is chosen makes a big difference in the attacks based on IV. Unfortunately, WEP doesn't specify how the IV is chosen or how often the IV is changed. Some implementations start the IV at zero and increase it incrementally for each packet, rolling over back to zero after 16 million packets have been sent. Some implementations choose IVs randomly. That sounds like a good idea, but it really isn't. With a randomly chosen IV, there is a 50% chance of reuse after less than 5,000 packets.Additionally, there are many methods for discovering the cipher stream for a particular IV. For example, given two encrypted packets with the same IV, the XOR of the original packets can be found by XORing the encrypted packets. If the victim is on the Internet, the attacker can simply ping the victim or send an e-mail message. If the attacker is able to send the victim packets and observe and analyze those encrypted packets, he can deduce the cipher stream.

(III) The ICV algorithm is not appropriate

The WEP ICV is based on CRC-32, an algorithm for detecting noise and common errors in transmission. CRC-32 is an excellent checksum for detecting errors, but an awful choice for a cryptographic hash. Better-designed encryption systems use algorithms such as MD5 or SHA-1 for their ICVs.The CRC-32 ICV is a linear function of the message meaning that an attacker can modify an encrypted message and easily fix the ICV so the message appears authentic. Being able to modify encrypted packets provides for a nearly limitless number of very simple attacks. For example, an attacker can easily make the victim's wireless access point decrypt packets for him. Simply capture an encrypted packet stream, modify the destination address of each packet to be the attacker's

wired IP address, fix up the CRC-32, and retransmit the packets over the air to the access point. The access point will happily decrypt the packets and forward them to the attacker. (The attack is slightly more complex than that, but to keep this short, we've skipped some of the details.)The biggest problem with IV- and ICV-based attacks is they are independent of key size, meaning that even huge keys all look the same. The attack takes the same amount of effort.

(IV) WEP's use of RC4 is weak

RC4 in its implementation in WEP has been found to have weak keys. Having a weak key means there is more correlation between the key and the output than there should be for good security. Determining which packets were encrypted with weak keys is easy because the first three bytes of the key are taken from the IV that is sent unencrypted in each packet. This weakness can be exploited by a passive attack. All the attacker needs to do is be within a hundred feet or so of the access point.

Out of the 16 million IV values available, about 9,000 are interesting to the most popular attack tool, meaning they indicate the presence of weak keys. The attacker captures "interesting packets," filtering for IVs that suggest weak keys. After that attacker gathers enough interesting packets, he analyzes them and only has to try a small number of keys to gain access to the network. Because all original IP packets start with a known value, it's easy to know when you have the right key. To determine a 104-bit WEP key, you have to capture between 2,000 and 4,000 interesting packets. On a fairly busy network that generates 1 million packets per day, a few hundred interesting packets might be captured. That would mean that a week or two of capturing would be required to determine the key.The best defense against this type of attack is not to use weak IV values. Many vendors are now implementing new algorithms that simply do not choose weak IVs. However, if just one station on the network uses weak keys, the attack can succeed.

(V) Authentication messages can be easily forged

802.11 define two forms of authentication: Open System (no authentication) and Shared Key authentication. These are used to authenticate the client to the access point. The idea was that authentication would be better than no authentication because the user has to prove knowledge of the shared WEP key, in effect, authenticating himself. In fact, the exact opposite is true: If you turn on authentication, you actually reduce the total security of your network and make it easier to guess your WEP key.Shared Key authentication involves demonstrating the knowledge of the shared WEP key by encrypting a challenge. The problem is that a monitoring attacker can observe the challenge and the encrypted response. From those, he can determine the RC4 stream used to encrypt the response, and use that stream to encrypt any challenge he receives in the future. So by monitoring a successful authentication, the attacker can later forge an authentication. The only advantage of Shared Key authentication is that it reduces the ability of an attacker to create a denial-of-service attack by sending garbage packets (encrypted with the wrong WEP key) into the network.Open system gives you better network security. Most network managers should turn off Shared Key authentication and depend on other authentication protocols, such as 802.1x, to handle the task of properly authenticating wireless users.WEP still provides basic security and it is integrated in most of the routers. A recent survey conducted for the purpose of this project on the Wireless security illustrates that an estimated one third of the Access Points have WEP encryption enabled (Chapter 4). Ziarek (2011) confirms these findings with a survey of the security situation in Poland where he found 21 per cent of the WLANs are still WEP encrypted.

2.2 Technology Overview of WPA

According to Halvorsen and Haugen (2009), Wi-Fi Protected Access (WPA) is a security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found in the previous system, WEP (Wired Equivalent Privacy). The WPA protocol implements much of the IEEE 802.11i (Halvorsen and Haugen, 2009) standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. TKIP employs a per-packet key (Halvorsen and Haugen, 2009), meaning that it dynamically generates a new 128-bit key for each packet and thus prevents the types of attacks that compromised WEP.

2.2.1 WPA Security Analysis

An improved level of security in WLANs can be implemented using WPA based on a similar acting as WEP. However, does not include most of the flaws of the previous system. The work on the WPA started immediately after the first reports of violation of the WEP and later on was deployed worldwide (Lowe, 2010).

In the article "Don't use WEP for Wi-Fi security" Sayer (2007) measures WPA encryption as a WEP replacement which is more secure and robust to attacks, yet it is able to run on the same hardware than WEP does. Nevertheless, the WPA shared more of the flaws of the WEP. McMillan (2009) concluded that Pre-Shared Keying (PSK) is not secure and short and/or unsecured passwords are almost as disadvantageous as the WEP. Based on similar thesis Takahashi (2004) developed a tool called WPA crack, a proof of concept which allows a brute force offline dictionary attack against the WPA. Author further concluded that the recommendation of the Wi-Fi alliance to use passwords longer than twenty characters would most likely not be executed in practice by the users of the WPA. Unfortunately, many people do not pay much attention to establishing long passwords and the consequences it may have in the future.

Kizza (2011) reviews the AES Protocol as "secure enough to meet the demands Federal \Information Standards (FIPS) 140-2", which is often demanded by institutions such as Police or Security Agencies. This new algorithm requires a separate chip for the encryption and therefore new hardware is needed (Misic, 2008). WPA is also subject to vulnerabilities affecting other 802.11i standard mechanisms such as attacks with 802.1x message spoofing, first described by Arbaugh and Mishra (2001).

2.2.2 How WPA works

WPA includes two types of user authentication. One named WPA Personal with a pre-shared key mechanism similar to the WEP and the WPA Enterprise, which uses 802.1x and derives its keys (Lockhart, 2006). Nonetheless, the main improvement of the WPA was introduction of Temporal Key Integrity Protocol (TKIP). Instead of using a pre-shared key, which creates a key stream, WPA uses a pre-shared key to serve as the seed for generating the encryption keys (Lammle, 2010). For data encryption, the WPA uses the RC4 stream cipher with a 128-bit key and a 48- bit IV, which is similar to the WEP. However, unlike the WEP, there is a major improvement for "WPA to use the Temporal Key Integrity Protocol (TKIP), which the heart of WPA" (Lammle, 2010). Due to the similarity of the encryption process to the WEP, implementation of the WPA can be as simple as upgrading clients' software and updating the firmware of older access points (Lowe, 2010). WPA adds features designed to address the deficiencies in the way that WEP uses the cipher. According to Jacobs (2012), some of the improvements found in WPA are:

(I) Stronger authentication: An 802.1x server, such as a Radius server, can be used to authenticate users individually.

(II) A longer key: WPA lengthens the Initialization Vector (IV) to 48 bits and the master key to 128 bits.

(III) Temporal Key Integrity Protocol (TKIP) generates different keys for each client and alters keys for each successive packet.

(IV) A message integrity code (MIC), or cryptographic checksum, verifies that messages have not been altered in transit and protects against replay attempts.

2.2.3 WPA Authentication (Jacobs, 2012)

WPA can be used in either of two modes: Personal or Enterprise.

(I) **Personal mode:** This utilizes manually configured keys in the same manner as WEP. All clients use the same initial master key.

(II) **Enterprise mode:** The AP uses Extensible Authentication Protocol (EAP) to negotiate a pair-wise master key with each client individually. The AP then verifies the identity of the client with an 802.1x server. The result is that each client that is permitted to use the network is validated against information configured in the 802.1x server and uses a key different from the keys used by other clients.

EAP, defined by RFC 3748, is an extensible protocol. It does not define a specific authentication protocol but simply specifies a set of functions and formats. A

large number of EAP methods have been defined. The Wi-Fi Alliance has chosen a subset of the available methods.

Cipher keys (Jacobs, 2012)

Reuse of keys provides a hacker with a great deal of data to use to determine the master key. With WEP, all stations used the same master key, and the 24-bit IV generated only 16 million possible values, so that on a busy network the same IV would be used within hours. It would take years to exhaust all of the values of a 48-bit IV.

In addition to increasing the length of the IV, TKIP solves the problem of weak IVs. Approximately 9,000 of the 16 million WEP IVs are called weak IVs because they reveal more about the master key than other IVs. The TKIP algorithm eliminates weak IVs.

In Enterprise mode, the 802.1x server supplies a different master key to each client, but in Personal mode, all master keys are the same. The TKIP algorithm combines the IV and the master key with the sender's MAC address and adds a sequence counter. Inclusion of the MAC address in the key means that the same combined key will not be used by all clients. Including the packet sequence number generates a different combined key for each subsequent packet. Use of the sequence number also provides a way to eliminate replay attacks. The receiving station can detect that the sequence number has not advanced as it should with each received packet.

Message integrity check (Jacobs, 2012)

The CRC32 checksum used in WEP did not provide adequate protection. A hacker can modify a WEP packet by changing one or more bits in the packet and making corresponding changes in the checksum. WPA uses a MIC algorithm called Michael. It provides much greater protection than CRC32, while requiring limited processor resources.

2.3 Technology Overview of WPA2

The IEEE 802.11i standard also known as Wi-Fi Protected Access 2 (WPA2) is an amendment to the 802.11 standard specifying security mechanisms for wireless networks. The draft standard was ratified on June 24th, 2004, and replaces the previous security specifications, Wired Equivalent Privacy (WEP), which was shown to have severe security weaknesses. Wi-Fi Protected Access (WPA) had previously been introduced as an intermediate solution to WEP insecurities. WPA implemented only a subset of IEEE 802.11i. WPA2 makes use of a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining- Message Authentication Code (CBC-MAC) protocol (CCMP). CCMP provides both data confidentiality (encryption) and data integrity. The use of the Advanced Encryption Standard (AES) is a more secure alternative to the RC4 stream cipher used by WEP and WPA (Ramchandran, 2011).

The WPA2 standard has two components, encryption and authentication which are crucial to a secure wireless LAN. The encryption piece of WPA2 mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware. The authentication piece of WPA2 has two modes: Personal and Enterprise. The Personal mode requires the use of a PSK (Pre-Shared Key) and does not require users to be separately authenticated. The Enterprise mode, which requires the users to be separately authenticated based on the IEEE 802.1X authentication standard, uses the Extended EAP (Extensible Authentication Protocol) which offers five EAP standards to choose from: EAP-Transport Layer Security (EAP-TLS), EAP Transport Layer Security (EAP-TTLS), Protected EAP vo/EAP-Microsoft's Challenge Handshake Authentication Protocol v2 (PEAPvo/EAPMSCHAPv2), Protected EAP v1/EAP-Generic Token (PEAPv1/EAPGTC) and EAP-Subscriber Identity Module of the Global System of Mobile Communications (EAPSIM).

2.3.1 How WPA2 works

Like WPA, WPA2 offers two security modes:

(I) Pre-shared key authentication based on a shared secret,

(II) Authentication by an authentication server

Pre-shared key authentication is intended for personal and small office use where an authentication server is unavailable (Lammle, 2010). Both the WPA and the WPA2 networks use a pre-shared key and are vulnerable to the dictionary attacks (Phifer, 2007). It

is significant to make the secret passphrase as long and as casual as possible (at least 20 characters long) with a mix of various random characters (numbers, uppercases etc.) (Lockhart, 2006.)

According to Jacobs (2012), WPA2 uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) protocol, based on the Advanced Encryption Standard (AES) algorithm for authentication and data encryption. TKIP greatly increases the difficulty of intercepting wireless traffic over WEP, but CCMP is more secure than the combination of RC4 and TKIP. Since CCMP requires more processor cycles than RC4, an upgrade to WPA2 may require replacement of APs or client wireless interfaces. Both Personal and Enterprise modes are supported. In Personal mode, the pre-shared key is combined with the SSID to create the pairwise master key (PMK). The client and AP exchange messages using the PMK to create the pairwise transient key (PTK). In Enterprise mode, after successfully authenticating -- using one of the EAP methods -- the client and AP receive messages from the 801.1x server that both use to create the PMK. They then exchange messages to create the PTK. The PTK is then used to encrypt and decrypt messages. In both cases, Personal and Enterprise, a group temporal key (GTK) is created during the exchange between the client and AP. The GTK is used to decrypt broadcast and multi-cast messages. WPA2 also adds methods to speed the handoff as a client moves from AP to AP. The process of authenticating with an 802.1x server and generating keys takes enough time to cause a noticeable interruption of a voice over wireless call. WPA2 specifies ways in which a client can pre-authorize with neighboring APs. APs and clients can also retain keys so that a client returning to an AP can quickly resume communication. WPA2 also introduces the authentication of Robust Security Network (RSN). "The RSN enhances the weak security of WEP and provides better protection for the wireless link by allowing the creation of Robust Security Network Associations (RSNA) only" (Cache and Liu, 2010). Through the improvements discussed above, WPA and WPA2 successfully provide more secure WLAN and make breaking into the network tougher. There are of course issues with TKIP (similarly to WEP) that allow small packets like ARP to be decrypted, yet there is no way to completely compromise a secure WPA key as well as it can be done with the WEP. If the WPA is appropriately implemented and sufficiently managed, it will be a very strong security and highly difficult task of breaking; especially with the implementation of the AES-CCMP, which is the most secure wireless network configuration in use today.

2.4 Comparing WEP, WPA, and WPA2

The relationship between WPA2, WPA and WEP is presented in table 2.1 below:

Table 2.1 Relationship between WPA2, WPA and WEP (Bansal and Mahajan, 2013)

	WEP	**WPA**	**WPA2**
Encryption cipher.	RC4	RC4	AES
Key sizes	40/104 bit	128 bit	128 bit
IV size	24 bit	48 bit	48 bit
Per-packet key	Key + IV	TKIP mix.fc.	CCM
Data integrity	CRC-32	Michael	CCM
Replay detection	None	IV seq.	IV seq.
Key management	None	802.1X	802.1X

Conclusion

The research approach aimed to raise the awareness of security issues, especially those related to the wireless LAN security. It is suggested that a reader will understand that every technology has its flaws and vulnerabilities, and often it is up to the users of technology to be aware and take actions to rectify and to use these technologies consequently.WEP encryption does not provide sufficient wireless network security and can only be used with higher-level encryption solutions. The research showed that WPA/WPA2 is more secured than WEP. The only time the pre-shared key of WPA/WPA2 can be cracked is if it is a dictionary word or relatively short in length. Equally, if there is a need for the unbreakable wireless network at home, the use of WPA/WPA2 and a 20 character password composed of random characters including special symbols is essential. If a weak pass phrase is used and it is included in the dictionary file, it takes no more than two hours to crack the key. However, depending on the capacity of the dictionary, it can take hours or days to break through large dictionary (millions of keys). WPA2 the latest encryption method, does not address the problem of dissociation and de-authentication attacks, but does address many of the issues with the WEP.

REFERENCES

[1] Abdalla, M., Pointcheval, D., Fouque, P. A. and Vergnaud, D. 2009. “Applied Cryptography and Network Security”
[2] Arbaugh, W., Mishra, A., 2001, “An Initial Security Analysis of the 802.1X Standard"[online] Available:http://www.cs.umd.edu/%7Ewaa/1x.pdf [accessed January 04, 2012].
[3] Berghel, H. and Uecker, J., 2004, “Wireless infidelity II”
[4] Barken, L. et.al. 2004. "Wireless Hacking: Projects for Wi-Fi Enthusiasts." Syngress [accessed January 04, 2017]
[5] Bayles, A. W. & Hurley, C. 2007. "Penetration Tester's Open Source Toolkit", Syngress Publishing. [Accessed March 20, 2017]
[6] Beaver, K. & McClure, S. 2010. "Hacking For Dummies", Wiley&Sons. [accessed]
[7] Beaver. K. and Davis, P. 2005. "Hacking Wireless Networks for Dummies." Wiley: Indianapolis [accessed March 20, 2017]
[8] Beck. M. and Tews.E., 2008. "Practical attacks against WEP and WPA" [accessed April 03, 2017]
[9] Bel., 2009. "Data Encryption, Enabling Authentication and Wireless Security" [accessed April 03, 2016].
[10] Borisov, N., Goldberg, I., and Wagner, D. (2001) "Intercepting Mobile Communications: The Insecurity of 802.11" [accessed December 01, 2016]
[11] Briere, D., Hurley, P. & Ferris, E. "Wireless Home Networking For Dummies", John Wiley & Sons. [Accessed November 02, 2016]
[12] Burns, B. 2007."Security power tools", O'Reilly. [Accessed May 10, 2012]
[13] Cache.J and Liu V., 2010. "Hacking Exposed Wireless: Wireless Security Secrets & Solutions - - McGraw-Hill Education" [accessed August 11, 2017]
[14] Cisco Support, [online]. Available: https://supportforums.cisco.com/thread/342246[accessed April 19, 2017].
[15] Coleman, D. D., Westcott, D. A., Harkins, B. E. &Jackman, S. M. 2009. CWSP: "Certified Wireless Security Professional Official Study Guide", John Wiley & Sons. [accessed July, 05, 2017]
[16] David B. Jacobs, 2012. "Wireless security protocols -- How WPA and WPA2 work" online].Available: http://www.searchnetworking.techtarget.com [accessed July, 05, 2017]
[17] Dowd, T., 2003. "Secure the network the same as a home: basic rules apply to keeping unwanted visitors out of prized possessions at home and at work.
[18] Flickenger, R. & Weeks, R. 2006, “Wireless hacks, O'Reilly. “
[19] Fluhrer, S., Mantin, I. and Shamir, S. 2001."Weaknesses in the Key Scheduling Algorithm of RC4" [online]. Available: http://www.crypto.com/papers/others/rc4_ksaproc.pdf [accessed November 02, 2016]
[20] Gast, Mathew S. 2005, "802.11 Wireless Networks, the Definitive Guide (2nd edn.)", USA, O'Reilly, Seabastopol [accessed January 20, 2017]
[21] Hatch, B. 2008. "Hacking exposed Linux: Linux security secrets & solutions", McGraw- Hill. [Accessed July 02, 2017]
[22] Howard, D. & Prince, K. 2010. Security 2020: "Reduce Security Risks This Decade", John Wiley & Sons. [Accessed June 05, 2017]
[23] Howard, R., Graham, J. & Olson, R. 2010. "Cyber Security Essentials", Auerbach Publishers, Incorporated. [Accessed August 09, 2017]
[24] Hurley, C, et.al. 2007. "WarDriving and Wireless Penetration Testing Syngress": Canada [accessed January 10, 2017]

[25] Hurley, C. & Thornton, F. 2004. "WarDriving: drive, detect, defend: a guide to wireless security", Syngress. [accessed March 03, 2017]
[26] I.S.S.W.G., 2011. "Information Systems Security Working Group: Security?" [online]. Available: http://www.isswg.org.uk/cia.php [accessed April 09, 2017]
[27] iLabs Wireless Security Team, 2011. "What's wrong with WEP?" [online] Available: http://www.networkingworld.com/wepflaws.com
[28] Kizza, J. M. 2011. "Computer Network Security and Cyber Ethics, McFarland & Co Inc Pub." [Accessed September 14, 2016]
[29] Krishnan, S. P. T., Veeravalli, B. & Wong, L. W. C. 2008. "Wireless LANs (WLANs): Security and Privacy. Encyclopedia of Wireless and Mobile Communications, 1392 - 1406." [Accessed April 19, 2017]
[30] Kumkum, G. 2010. "Mobile Computing: Theory and Practice", Pearson Education. [accessed December 05, 2016]
[31] Lammle, T. 2010. "CCNA Wireless Study Guide: IUWNE Exam 640-721", John Wiley & Sons. [Accessed May 05, 2017]
[32] Lockhart, A., 2006. "Network security hacks. 2nd ed." Sebastopol, CA: O'Reilly [accessed January 10, 2017]
[33] Lowe, D. 2010. "Networking All-in-One for Dummies", John Wiley &Sons. [Accessed August 21, 2017]
[34] Misic, J.andMisic, V. 2008. "Wireless Personal Area Networks: Performance, Interconnection, and Security with IEEE 802.15. 4". Wiley-Interscience:Chichester : [accessed September, 10, 2016]
[35] Raggi, E., Thomas, K., Channelle, A., Parsons, T. &Vugt, S. 2010. "Beginning Ubuntu Linux, Fifth Edition", Apress. [Accessed July 09, 2016]
[36] Sayer. P. 2007: Don't use WEP for Wi-Fi security. Computerworld [online] Available: http://www.computerworld.com/s/article/9015559/Don_t_use_WEP_for_Wi_Fi_security_researchers_say [accessed January 19, 12016]
[37] Simpson, M. T., Backman, K. & Corley, J. 2010."Hands-On Ethical Hacking and Network Defense", Cengage Learning. [Accessed 12 May 16, 2017]
[38] Takahashi, T. 2004, "WPA Passive Dictionary Attack Overview" [online] Available:http://www.tinypeap.com/docs/WPA_Passive_Dictionary_Attack_Overview.pdf [accessed November 10, 2016]
[39] Vladimirov, A. A., Gavrilenko, K. V. &Mikhailovsky, A. A. 2004."Wi-Foo", Addison-Wesley. [accessed Febuary 25, 2017]
[40] Vladimirov.A, Konstantin. V, Gavrilenko. A., 2010. Wi-Foo, "The Secrets of Wireless Hacking." Addison-Wesley Buch [accessed June 11, 2017]
[41] Wi-Fi Alliance. "Securing Wi-Fi Wireless Networks with Today's Technologies [security whitepaper]" http://www.wifi.org/files/uploaded_files/wp_4_Securing%20Wireless%20Networks_2- 6-03.pdf [accessed February 19, 2017]
[42] Wirelessdefence.org."A step by step guide to breaking WEP" [online].Available:http://wirelessdefence.org/Contents/802.11%20Basics.htm [accessed November 21, 2016]
[43] Yasir, Z. and Yang. T., 2004 "Wireless LAN security and laboratory designs." [Accessed November 21, 2016]
[44] Zhang, Y., Zheng, J. & Ma, M. 2008."Handbook of research on wireless security", Information Science Reference. [Accessed January 10, 2017]