Wireless LAN Security Threats & Vulnerabilities:
A Literature Review

Md. Waliullah
Dept. of Computer Science & Engineering,
Daffodil International University,
Dhaka, Bangladesh

Diane Gan
School of Computing and Mathematical Science
University of Greenwich,
London, UK

Abstract—**Wireless LANs are everywhere these days from home to large enterprise corporate networks due to the ease of installation, employee convenience, avoiding wiring cost and constant mobility support. However, the greater availability of wireless LANs means increased danger from attacks and increased challenges to an organization, IT staff and IT security professionals. This paper discusses the various security issues and vulnerabilities related to the IEEE 802.11 Wireless LAN encryption standard and common threats/attacks pertaining to the home and enterprise Wireless LAN system and provide overall guidelines and recommendation to the home users and organizations.**

Keywords—WLAN; IEEE 802.11i; WIDS/WIPS; MITM; DoS; SSID; AP; WEP; WPA/WPA2

I. Introduction

Over the last twelve years, 802.11 Wireless LAN's have matured and really reshaped the network landscape. 802.11n is now rapidly replacing Ethernet as the method of network access. The rapid proliferations of mobile devices has led to a tremendous need for wireless local area networks (WLAN), deployed in various types of locations, including homes, educational institutions, airports, business offices, government buildings, military facilities, coffee shops, book stores and many other venues. Besides, the facilities of flexibility and mobility of wireless devices has been attracted by most organizations and consumers all over the world. Low cost of hardware and user friendly installation procedures allow anyone to set up their own wireless network without any specialist knowledge of computer networks.

However, the increased development of Wireless LAN has increased the potential threats to the home user, small businesses and the corporate world. Unlike a wired network, a WLAN uses radio frequency transmission as the medium for communication. This necessarily exposes layer 1 and layer 2 to whoever can listen into the RF ranges on the network. Wireless insecurity has been a critical issue since Wired Equivalent Privacy (WEP), an IEEE standard security algorithm for wireless networks, was compromised [1]. To address the significant security flaws in the WEP standard, the Wi-Fi alliance developed the 802.11i standard, called Wi-Fi Protected Access (WPA) and WPA2 [1]. However, many researchers have shown that the IEEE 802.11i standard cannot prevent eavesdropping, various denial of service attacks including de-authentication and disassociation attacks. Moreover, 802.11i's pre-shared key mode of WEP for flexibility and backward compatibility has made it easier for most hackers to perform a Dictionary and Brute force attack [2].

Recently, a scanning experiment based on London conducted by the security firm Sophos has revealed that more than one in four Wi-Fi networks in London are poorly secured or not secured at all [3]. Of 100,000 Wi-Fi networks detected on a 90 Km route, 8% of the Wi-Fi networks detected used no encryption at all. This figure excludes intentionally open networks such as coffee shops, hotels and Wi-Fi hotspots. Approximately, 9% of Wi-Fi networks detected were using default network names such as "default" or a supplier name enabling the hacker to break passwords more easily. More importantly, the experiment revealed that 19% of the Wi-Fi networks detected used obsolete WEP as the encryption standard which has already proved to be easily cracked within a second, using readily available hacking tools [3]. So, the security of a wireless LAN still remains the top concern in the home and corporate network.

This paper discusses the vulnerabilities and security issues pertaining to the IEEE 802.11 security standard and describes major well known attack/threats to the home and enterprise wireless LAN system. The remainder of the paper is organised as follows. A brief overview of WLANs are outlined in section II. Related work is presented in section III. The common vulnerabilities and security issues pertaining to the IEEE 802.11 security standard and WLAN are discussed in section IV. This is followed by an over view of the common threats/attacks on WLAN technology. Common guidelines and an overall recommendation is presented in section VI, and a conclusion is outlined in section VII.

II. Overview Of WLAN

An access point (AP) and a network interface card (NIC) are the two basic components of a WLAN. An AP typically connects the wireless clients or stations to each other by means of antenna and then connects to the wired backbone through a standard Ethernet cable. A NIC normally connects a wireless station to the AP in the Wireless LAN [4]. Any devices that have the ability to communicate with 802.11 networks are called a station i.e. laptops, printers, media servers, smartphones, e.g. IPhones, Windows mobile handsets, VoIP phones etc. All 802.11 stations operate in two ways, either in ad-hoc mode, where stations are connected to each other, or in infrastructure mode, where stations are communicating with each other via the access points to reach some other network [5].

Companies install as many access points as it takes to cover an entire building or even a campus. The whole network is configured with the same network name to act as one huge wireless network, which is called an extended service set identifier (ESSID) or a standard service set identifier (SSID). For example, if an IPhone wants to connect to a WLAN, it starts by scanning all channels; sends a probe request and listens for beacon frames that are sent by access points to advertise themselves. Then, it compares all those beacons and probe responses to the desired SSID and selects the best available access point.

Finally, the IPhone will send an authenticating packet and will associate the request to that access point by establishing a 4-way handshake mechanism. Once the IPhone is associated and authenticated it can send and receive data using that wireless network [5].

III. RELATED WORK

Sheldon, Weber, Yoo and Pan [1] described how the wireless LAN encryption standards such as WEP, WPA/WPA2 are vulnerable to attack. They presented some of the attacks on encryption standards such as Chop-chop attack, Brute force, Beck-Tews, Halvorsen-Haugen and the hole 196 attacks etc. Wang, Srinivasan, and Bhattacharjee [2] proposed a 3-way handshake model instead of the usual 4 way handshake method for the 802.11i protocol. They suggested how their alternative method can effectively prevent denial of service (DoS) attacks including de-authentication, disassociation and memory/CPU DoS attacks. Souppaya and Scarfone [6] discussed the need for security concerns and these should be applied from the configuration design stage to implementation and evaluation through to the maintenance stage of the WLAN. They provided some general guidelines and recommendations in order to reduce the vulnerabilities and prevent the most common threats.

Pan Feng [4] suggested that more than 70% of the WLAN security issues are due to human factors, such as data theft by acquaintances or colleagues. He addressed that remaining 30% of security threats are technology related. Reddy, Rijutha, Ramani, Ali, and Reddy [7] demonstrated how WEP can be cracked by freely available open source software tools such as Netstumbler, Ministubler, Airopeek, Kismat, Cain etc. They have mainly focused on securing WLANs by realizing miscellaneous threats and vulnerabilities associated with 802.11 WLAN standards and have used ethical hacking to try to make these more secure.

Li and Garuba [8] and Deng Shiyang [9] discuss various encryption standards relating to 802.11 WLAN, their vulnerabilities and security flaws. Stimpson et al [10] describes war driving techniques as a useful tool for assessing security and vulnerabilities of home wireless networks.

However, none of the above researchers has elaborately presented WLAN security vulnerabilities, threats and general guidelines/recommendations for securing them. Realizing the vulnerabilities, understanding the most common threats and providing general guidelines and recommendation in order to protect WLAN network and make them more secure for the home user and for enterprise networks is the aim of this paper.

IV. WLAN VULNERABILITIES

Wireless LANs have gained much more popularity than wired networks because of their flexibility, cost-effectiveness and ease of installation. However, the increasing deployment of WLANs presents the hacker or cracker with more opportunities. Unlike wired networks, WLANs transmit data through the air using radio frequency transmission or infrared. Current wireless technology in use enables an attacker to monitor a wireless network and in the worst case may affect the integrity of the data. There are a number of security issues that presents the IT security practitioner, system administrator securing the WLAN with difficulties [11].

As the name implies Wired Equivalent Privacy (WEP) was intended to provide users with the same level of privacy as that of a wired LAN. However, when this protocol was first developed by the IEEE 802.11b Task Force in 1999, it quickly proved to be less secure than its wired equivalent. WEP comes as 64 bit or 128 bit but the actual transmission keys are 40 bits and 104 bits long. In each case the other 24 bits is an Initialization Vector (IV). Before transmission, the packets are encrypted with a symmetric encryption algorithm (RC4) using a session key which is made up of the IV and the default transmit key. The IV is randomly generated for each session but the default transmit key is fixed. The IV is sent in the packet along with the data. Once the encrypted packet reaches the receiving end, it decrypts the packet using the same session key [12].

However, WEP has some serious security problems. It fails to meet the fundamental security goals of confidentiality, integrity and authentication. The main problem with WEP is that the 40 or 104 bit keys are static and common to all users in the WLAN. Since, WEP does not provide an effective key management technique, changing the keys on all devices is a time consuming and difficult task. Thus, if any devices are lost or stolen, the higher the chances of the key being compromised. This exposes the whole system to security breaches [12]. More importantly, the encryption algorithm RC4 used in WEP is flawed and encryption keys can be recovered through cryptanalysis [8]. Besides the default transmission key, the IV is short and can be easily sniffed by passive attack using freely available software tools. One of the other problems is that WEP is disabled by default and its use is optional, therefore, many users never turn on encryption. It is better to use of some form of encryption than no encryption at all [8][12] .

In order to eliminate all well-known attacks and address the significant security flaws in WEP, the Wi-Fi alliances developed IEEE 802.11i security standard in 2004 which is called Wi-Fi protected access (WPA) and subsequently WPA2. WPA uses the same encryption algorithm (RC4) used in WEP but improved by the use of a 48 bit temporary key integrity protocol (TKIP) sequence counter (TSC) instead of WEP's 24 bit key. Moreover, the 64 bit message integrity check (MIC) algorithm named Michael is used to ensure integrity [1]. Furthermore, to improve user authentication and access control, WPA uses the extensible authentication protocol (EAP) and the IEEE 802.1x standard port based access control. This method uses the Radius (Remote Authentication Dial-in User Service) server to authenticate each user on the network [8]. In the absence of a Radius server, it uses a pre-shared key (PSK), which is called WPA-PSK or WPA-Personal and is mostly used in small-offices and by home users [1].

Although, WPA is considered stronger than WEP, it does reuse the WEP algorithm. As a result it is vulnerable to offline dictionary and brute force attacks against the 4-way handshake protocol [10]. More importantly, it is much more vulnerable to DoS attacks which are carried out over the MAC layer by sending out de-authentication and disassociation messages to the client or AP resulting in the legitimate user being denied access to the service [8].

WPA2 employs the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) instead of TKIP and uses Advance Encryption Standard (AES) block cipher. AES replaces the WPA's RC4 stream cipher [1]. Although WPA2-AES is still regarded as extremely secure, it is vulnerable to DoS, offline dictionary and internal attacks and fails to provide the availability aspect of the CIA triad [2].

More importantly, the robust encryption standard only applies to data frames and not currently to the management frames. All 802.11 management and control frames are vulnerable to replay or forgery, including the messages that are used to probe, associate, authenticates, disassociate, and de-authenticate users from the WLAN. Besides, unlike the software upgrade required for migration from WEP to WPA, WPA2 requires the replacement of older hardware, extra processing power and has a much higher cost [12].

Both WPA and WPA2, are extremely vulnerable to dictionary and bruit-force attack, regardless of whether they are operating in Personal or Enterprise mode,. Most home networks use pre-shared key authentication, allowing quick and easy control over who can use the network. This PSK's are both simple and limited and they are the same as a group password. They can be shared with outsiders, or the device can be lost or stolen. As a result, it is hard to guess whether the WLAN being used by legitimate users or foes. Furthermore, the attacker can still listen to frames that are being sent and received without even trying to authenticate even in the case of 802.1x port based authentication. In addition 802.1x's lightweight EAP or LEAP, implement password authentication in a way that is vulnerable to a dictionary attack [5].

802.11 networks are inherently vulnerable to radio frequency interference problems. Most of the wireless LAN standards operate on the 2.4 GHz channel frequency band, while many other devices such as Bluetooth, cordless phones and microwave signals also operate on the same frequency band. This can lead to signal interference and cause a legitimate user to be disconnected [4].

Our inability to effectively contain radio signals makes the WLAN vulnerable to a different set of attacks from wired LANs. Although businesses can position their access points and use antennas to focus their signals in a specific direction, it is hard to completely prevent wireless transmission from reaching an undesirable location like nearby lobbies, semi-public areas and parking lots. This makes it easier for intruders to sniff sensitive data [5].

MAC address filtering can be configured in an access point in order to allow only an authorized client in the network. However, the various available open source hacking tools i.e. Kismet, SMAC etc. can be used to passively sniff a large amount of network traffic, including the MAC addresses of authorized computers. These can then be changed to act as legitimate clients on the network. Moreover, in a large network the continually updated list of MAC address at the access point sometimes creates a security hole, if the list is not correctly updated [13].

SSID is an identification that allows the clients to communicate with an appropriate access point. The available access points on the market come with a default SSID name and password. This creates potential security vulnerabilities, if these are not changed by the administrator or user. For example some of the common default passwords are: "tsunami" (Cisco), "101" (3Com), "Compaq" (Compaq) etc. Furthermore, most hotspots and guest networks operate in an open system mode allowing any stations to connect to that network without requiring any form of authentication [14].

V. GENERAL ATTACKS/THREATS TO WLAN TECHNOLOGY

An attack is an action that is carried out by an intruder in order to compromise information in an organization. Unlike wired networks, a WLAN uses radio frequency or infrared transmission technology for communication; thus, making them susceptible to attack. These attacks are aimed at breaking the confidentiality and integrity of information and network availability. Attacks are classified into the following two categories:

- Passive attacks.
- Active attacks

Passive attacks are those types of attack in which the attacker tries to obtain the information that is being transmitted or received by the network. These types of attacks are usually very difficult to detect as there is no modification of the contents by the attacker [15]. There are two types of passive attack and these are traffic analysis and eaves dropping.

On the other hand, active attacks where the attacker not only gains access to the information on the network but also changes the information/contents or may even generate fraudulent information on the network. This type of malicious act, results in great loss for any organization [15]. Following are a list of active attacks in WLAN technology:

- Unauthorized Access
- Rogue Access Point
- Man in the Middle Attack (MITM)
- Denial-of-Service
- Reply Attack
- Session High jacking

According to the CIA triad, information security should meet three main principles, which are confidentiality, integrity and availability. All three concepts are needed to some extent to achieve true security. Otherwise, the network will be vulnerable to attack. Furthermore, two other principals involved i.e. access control and authentication.

- Confidentiality is the prevention of intentional/unintentional disclosure of data.
- Integrity is control over the intentional/unintentional modification of data.
- Availability is the control over provision of system resources on demand to authorized users/systems/processes.
- Access control is the control of access to the resources by a legitimate user.
- Authentication is the process by which a system verifies the identity of a user who wants to access it [16].

Based on the CIA triad, access control and the authentication definitions described, various types of attack/threats in a WLAN are discussed below. These attack categories can also fall in the above active or passive types.

A. *Confidentiality Attacks*

In this type of attack, intruders attempt to intercept highly confidential or sensitive information that has been sent over the wireless association either encrypted or in clear text by the 802.11 or higher layer protocols. Examples of passive attacks are Eavesdropping, Man-in-the-Middle attack, Traffic Analysis etc. Active attack categories are WEP Key Cracking, Evil Twin AP and AP Phishing etc. [16].

1) Traffic Analysis: Also known as footprinting, is the first step which is carried out by most hackers before attempting further attacks. This is a technique whereby the attacker determines the communication load, the number of packets being transmitted and received, the size of the packets and the source and destination of the packet being transmitted and received. Thus, the overall network activity has been acquired by the traffic analysis attack [17]. To accomplish this attack, the attacker uses a wireless card that can be set to promiscuous mode and special types of antenna to determine the signal range e.g. yagi antenna, along with the global positioning mode (GPS). Furthermore, there are a number of freely available software that can be used e.g. Netstumbler, Kismet etc.

The intruders obtain three forms of information through traffic analysis. First, they identify if there is any network activity on the network. Secondly, he or she identifies the number of access points and their locations in the surrounding area. If the broadcast SSID has not been turned off in the AP, then it broadcasts the SSID within the wireless network in order to allow wireless nodes to get access to the network. Even if it is turned off, a passive sniffer like Kismet can obtain all the information about the network including the name, location and the channel being used by any AP. Finally, the third piece of information the attacker can learn through traffic analysis is the type of protocol that is being used in the transmission, along with the size, type and number of packets being transmitted. For example, analysis of the three-way handshake information of TCP [17].

2) Eavesdropping: An Eavesdrop attack, enables an attacker to gain access to the network traffic and read the message contents that are being transmitted across the network. The attacker passively monitors the wireless session and the payload. If the message is encrypted, the attacker can crack the encrypted message later. The attacker can gather information about the packets, specially their source, destination, size, number and time of transmission. More importantly, there are many directional antennas available in the market which can detect 802.11 transmissions under the right conditions, from miles away. This is an attack that cannot be easily prevented using adequate physical security measures. Besides, this attack can be done far away from the premises of any organizations [17][18].

3) Man-in-the-Middle Attack: A man-in-the-middle attack can be used to read the private data from a session or to modify them, thus, breaking the confidentiality and integrity of the data. This attack also breaks indirect data confidentiality. However, an organisation could employ security measures such as a VPN or IPsec, which only protect against direct data confidentiality attacks. This is a real time attack which occurs during the target machine's session. There are multiple ways to implement this attack. For example, in step one, the attacker breaks the target's client session and requires them to re-associate with the access point. In step two, the target client attempts to re-associate with the access point but can only re-associate with the attacker's machine, which is mimicking the access point. In the meantime, the attacker associates and authenticates with the access point on behalf of the target client. If an encrypted tunnel is in place, the attacker establishes two encrypted tunnels, one between it and the target client and another to the access point. In short, in this type of attack, the attacker appears to be an AP to the target client and a legitimate user of the AP [17].

4) Evil Twin AP: An Evil Twin attack poses as great a danger to wireless users on public and private WLANs alike. In this type of attack, an attacker sets up a phony access point in the network that pretends to be a legitimate AP by advertising that WLAN's name i.e. extended SSID. Karma is an attack tool that is used to perform this attack by monitoring station probes, watching commonly used SSIDs and using them as its own. Even APs that do not send SSIDs in the beacon can also be accessed using NetStumbler, Kismet or another WLAN analyzer tool while posing as a legitimate user [16].

B. *Access Control Attacks*

This attack attempts to penetrate a network by bypassing the filters and firewall to gain unauthorized access. war driving, rogue access points, MAC address spoofing and unauthorized access are the most common types of attack in this category.

1) War Driving: While war driving, the attacker drives around in a car with a specially configured laptop that has software such as Netstumbler or Kismet installed which identifies the network characteristics. More importantly, an external antenna and a GPS can be used to clearly identify the location of a wireless network [19]. The attacker discovers wireless LANs i.e. all the APs, the physical location of each AP, the SSID and the security mechanisms etc. by listening to the beacon or by sending a probe request. This attack provides the launch point for further attacks [19].

2) Rogue Access Point: In this type of attack, an intruder installs an unsecured AP usually in public areas like airports, shared office areas or outside of an organization's building in order to intercept traffic from valid wireless clients, to whom it appears as a legitimate authenticator. As a result, this attack creates a backdoor into a trusted network. The attacker could fool the legitimate client by changing its SSID to the same as that used by the target organization. Furthermore, the attacker uses an unused wireless channel to set up this fake access point. It is easy to trick unsuspecting users into connecting to the fake access point. Thus, the credential information of a user could easily be stolen [20][21].

3) MAC addresses spoofing: In this type of attack, the attacker gains access to privileged data and various resources such as printers, servers etc. by assuming the identity of a valid user in the network. To do so, the attacker reconfigures their MAC address and poses as an authorized AP or station. This could be easily done, because 802.11 networks do not authenticate the source MAC address frames. Therefore, the attacker can spoof MAC addresses and hijack a session. Furthermore, 802.11 does not require an AP to prove it is a genuine AP [14].

4) Unauthorized Access: Here the attacker is not aiming at a particular user, but at gaining access to the whole network. The attacker can gain access to the services or privileges that he/she is not authorized to access. Moreover, some WLAN architecture not only allows access to the wireless network but also grants the attacker access to the wired component of the network. This can be done by using war driving, rogue access points or MAC spoofing attack. This attack gives the attacker the ability to do a more malicious attack such as a MITM [17].

C. Integrity Attacks

An Integrity attack alters the data while in transmission. In this attack, the intruder tries altering, deleting or adding management frames or data i.e. forged control packets to the network, which can mislead the recipient or facilitate another type of attack [22]. DoS attacks are the most common example of this type of attack which is described in section D. Other types include session hijacking, replay attacks, 802.11 frame injection, 802.11 data replay, and 802.11 data deletion etc.

1) Session Hijacking: In Session Hijacking, an attacker takes an authorized and authenticated session away from the legitimate user of the network. The legitimate user thinks that the session loss may be a normal malfunction of the WLAN. Thus, he/she has no idea that the session has been taken over by the attacker. This attack occurs in real-time and the attacker uses the session for whatever purpose he/she wants and can maintain the session for an extended period of time [17].

In order to successfully execute a Session Hijacking attack, the attacker performs two tasks. Firstly, the attacker masquerades as the valid target to the WLAN. This requires a successful eavesdropping on the target communication to gather the necessary information. Secondly, the attacker deluges the air with a sequence of spoofed disassociate packets to keep the legitimate target out of the session [17].

2) Replay Attack: This type of attack is not a real time attack and uses the legitimate authentication sessions to access the WLAN. The attacker first captures the authentication of a session or sessions. Later on, the attacker replays authenticated sessions to gain access to the network without altering or interfering with the original session or sessions [17].

3) 802.11 Frame Injection Attack: In a frame injection attack intruders capture or send forged 802.11 frames. They also inject their own Ethernet frames into the middle of the transmission. For example, an attacker could inject a frame while a user is trying to logon into a banking website. The website looks legitimate but it is not, as the attacker has injected Ethernet frames. Thus, all the login information will be recorded by the intruders [16].

4) 802.11 Data /802.11X EAP / 802.11 RADIUS replay attack: This attack involves the capture of 802.11/ 802.11X EAP/ 802.11 RADIUS data frame or authentication information and save it for later use. This information can be used for 80.1X EAP or for 802.1 X RADIUS authentication. Once the attacker captures and saves the authentication information, they can monitor traffic for another authentication in order to inject saved frames instead of the legitimate authentication frames to gain access to the system [22].

5) 802.11 Data deletion: This type of attack involves the attacker deleting the data being transmitted. An attacker could jam the wireless signal from reaching its intended target and provide acknowledgements (ACKs) back to the sources. As a result, data would never reach the legitimate target and the senders have no idea as they appear to receive ACKs [22].

D. Availablity Attacks

This attack prevents or prohibits the legitimate clients by denying access to the requested information available on the network. DoS attack is the most common type of availability attack which focuses on attacking a specific part of the network so the network becomes unreachable. There are several types of DoS attack which are described below:

1) Denial-of-Service Attack: In this type of attack, an attacker tries to prevent or prohibit the normal use of the network communication by flooding a legitimate client with *bogus packets, invalid messages, duplicate IP or MAC address.*

2) Radio frequency (RF) Jamming: An 802.11 network operates in the unlicensed 2.4 GHz and 5 GHz frequency band. In this type of attack, the attacker jams the WLAN frequency with a strong radio signal which renders access points useless [17]. As a result, legitimate users cannot access the WLAN.

3) 802.11 Beacon Flood: An intruder overloads the network by flooding it with thousands of illegitimate beacons so that the wireless AP is busy serving all the flooding packets and cannot serve any legitimate packets. Thus, making it very difficult for legitimate clients to find the real AP [16].

4) 802.11 Associate/Authentication Flood: In this type DoS attack, an attacker sends thousands of authentication/association packets from MAC addresses in order to fill up the target AP's association table. This makes it harder for a legitimate user to gain access in the network [16].

5) 802.11 De-authentication & Disassociation: The attacker pretends to be a client or AP and sends unauthorized management frames by flooding thousands of de-authentication messages or disassociation messages to the legitimate target. This forces them to exit the authentication state or to exit the association state [21].

6) Queensland DoS / Virtual carrier-sense attack: In this type of attack, an intruder exploits the clear channel assessment (CCA) by periodically claiming a large duration field in a forged transmission frame to make a channel appeared busy. This prevents other clients from gaining access to the channel [16].

7) Fake SSID: The attacker floods the air with thousands of beacon frames with fake SSIDs and all the access points become busy processing the fake SSIDs [21].

8) EAPOL flood: In this type of attack, the attacker deluges the air with EAPOL beacon frames with 802.11x authentication requests to make the 802.1x RADIUS server busy. Thus, legitimate client authentication requests are denied [21].

9) AP theft - This an attack where the attacker physically removes the access point from the public space making the network unavailable for the user [16].

E. Authentication Attack

In an authentication attack, an intruder steals legitimate user's identities and credentials in order to gain access to the public or private WLAN and services. Dictionary attacks and brute force attacks are the most common techniques in this category. Once they have got the required information, the attacker impersonates or masquerades as an authorized user. Thereby gaining all the authorized privileges in the WLAN [5].

1) Dictionary & Brute force attack: A brute force attack involves trying all possible key's in order to decrypt the message. On the other hand dictionary attacks only try the possibilities which are most likely to succeed, usually derived from a dictionary file. If the appropriate time is given, a brute force attack can crack any key. Whereas, Dictionary attacks will be unsuccessful if the password is not in the dictionary [23].

Most access points use a single key or password that is shared with all connecting devices on the wireless LANs. A brute force attack can be applied on sniffing packets captured by the attacker in order to obtain the key.

Authentication attacks that are directly or indirectly involved with brute force and dictionary attack techniques after capturing the required information are discussed below [16]:

1) Shared Key Guessing: The attacker attempts 802.11 shared key authentication with the cracked WEP keys or with the provided vendor default key.

2) PSK Cracking: In this type of attack, the cracker first captures the WPA-PSK key handshake frame, using open source tools such as Aircrack-ng, Kismet etc. Later, they run a dictionary or a brute force attack to recover the WPA-PSK key.

3) Application Login Theft: The cracker captures user credentials e.g. e-mail address and passwords etc. from clear text application protocols.

4) VPN Login Cracking: The attacker runs brute force attacks on the VPN authentication protocol in order to gain the user credentials e.g. PPTP (point to point tunnelling protocol) password or IPsec Preshared Secret Key etc.

5) Domain Login Cracking: The cracker runs a brute force or dictionary attack on NetBIOS password hashes. Thus accessing the user credentials e.g. windows login and password.

6) 802.1X Identity Theft: The attacker captures 802.1X identity response packets. Later they run the brute-force attack to recover user identities.

7) 802.1X LEAP Cracking: The intruder captures 802.1X lightweight EAP beacon frames and then runs a dictionary attack in order to recover user credentials.

8) 802.1X Password: The attacker repeatedly attempts 802.1X authentication to guess the user's password by using a captured user's identity [16].

Beyond the above attack categories there are many more attacks pertaining to 801.11 technologies and describing all those is out of the scope of this paper. For example, a WLAN is vulnerable to upper layer threats. Fishing messages, mass mailing worms and Trojan downloaders can be carried over either wired or wireless networks. Attackers can poison ARP and DNS caches on wireless devices. Furthermore, there are other kinds of attack that try to exploit the wireless encryption standard. Examples are the Chopchop attack, the Original Beck-Tews attack, Halvorsen-Haugen attacks, the hole 196 attack and the Ohigashi-Morii attack etc. [1].

VI. Securing a Wireless Lan

The above vulnerabilities and threats come to the conclusion that it is very important to make sure that the wireless network is secure whether for a home user or an enterprise network. However, still there is no true security solution that has been implemented and is presently available. But, the following steps could serve as a guideline to prevent most known vulnerabilities and some common threats:

The security of a WLAN should be considered throughout the WLAN development lifecycle, from the initial design and deployment stage through implementation, maintenance and monitoring. The Administrator should ensure that the organization's WLAN client devices and AP's have followed standard security configurations and are always compliant with the organization's security policies. Furthermore, the organization should implement continuous attack and vulnerability monitoring and perform periodic technical security assessment to measure overall security of the WLAN [6].

The use of strong encryption standards protect WLANs from the worst threats. The best practice would be to enable Wi-Fi protected access WPA/WPA2 rather than WEP. Furthermore, it is recommended to uses the WPA2, AES-CCMP protocol rather than to use WPA, as WPA-TKIP uses the WEP encryption algorithm for backward compatibility [10]. However, when using WPA2-PSK, it is important to ensure that the users are using strong, longer and hard to guess passwords for authentication. Moreover, larger organisations should consider using certificate-based authentication mechanism or RADIUS, allowing the users to access their own managed credentials in order to protect their network from sharing [24].

All manufacturers' default SSIDs, usernames and passwords are very well known to hackers. Therefore, changing the default SSID is a crucial step for securing home and enterprise network. More importantly, in the case of choosing the name, a user should try and use a unique name that doesn't give much information away about the owner, such as house number, street name or business name. This could enable the hacker to identify the exact location of the network [8].

By disabling SSID, this effectively hides the access point. This means that the user has to manually configure the network name and password in order to access the WLAN. This provides a very light defence, as by using readily available sniffing software tools anyone can discover the hidden network name. However, further security for routers can be managed where WEP is the only option available [10].

For connections to an open network such as a Wi-Fi hotspot and those commonly provided by hotels, Starbucks, McDonalds and so on, a virtual private network (VPN) can be a good security solution to deliver consistent protection over any internet connection and provide end-to-end security on wireless devices. Furthermore, large organisations can benefit by using a VPN to secure data that is sent over to a home or business partner WLAN without having to rely on a business partner to secure their part. Employees can use a VPN-enabled device which uses a secure tunnelling protocol such as IPSec or SSL to connect to company networks. Besides, a VPN can be useful to secure traffic that is sent by devices such as Smartphones which frequently roam between wireless and wired network [5].

Captive portal is a kind of authentication method used for guest access to a network. It is widely used in public internet networks such as hotels, conference centres, cafes and so on. Using this method, users automatically get redirected to the login page. Once the user's credentials are verified, the user would then successfully be able to access the network. This challenge response authentication is encrypted using SSL to prevent a hacker from sniffing user's credentials. However, some portals offer only authentication without any encryption of password or user data. It is very important to make sure that the portal offers an adequate security service [25].

Virtual Local Area Networks (VLAN) are another technology that can be used in corporate wireless network to enforce a security policy. VLANs work by tagging LAN frames assigned to different workgroups. Those tags actually decide where incoming frames can and cannot go within the corporate network. For example, if a business provides guest and consultant access, all traffic coming from that wireless LAN will be tagged so that traffic is limited to the public internet thus, keeping them away from corporate data and services [5].

Network Access Control (NAC) is another authentication technology that can be used in conjunction with the 802.1x and VLANs to enforce an extra layer of security. Instead of filtering traffic based on IP addresses and port numbers, NAC controls user access to network resources based on the sender's authenticated user identity, the state of the user's device and the configured policy. With NAC, network devices like Ethernet switches, APs, routers and firewalls all can still control access but they are enforcing decisions made by the NAC. For example, NAC decisions can be enforced by permitting or denying the use of a particular SSID or using 802.1x to direct wireless clients to particular subnets or VLANs [5].

A wireless intrusion detection and prevention system can be an essential tool for identifying intrusions and notifying the system administrator of attacks. There is no option to stop passive sniffing on the network with the traditional firewall. As a result, WIDS/WIPS can be deployed to act as a watchdog in order to detect and prevent new threats and any malicious activity. A VPN used with WIDS/WIPS can provide a good security measure by actively monitoring the network to identify anomalies. This adds another layer of assurance for data confidentiality [5].

VI. Conclusion

Securing the wireless network is an ongoing process. Realistically, still there is no single true security measure in place. When a new technology is first introduced, hackers study the protocol, look for vulnerabilities and then cobble together some program and scripts to try to exploit those vulnerabilities. Overtime those tools become more focused, more automated and readily available and published on the open source network. Hence, they can be easily downloaded and run by anyone. So, we never eliminate all threats and vulnerabilities and even if we do, we will probably end up wasting money by defeating some low probability and low impact attack. On the other hand, if we start eliminating the biggest security loopholes, attackers may turn to easier targets.

Thus, true WLAN security is always going to be a game of balancing acceptable risk and the countermeasure to mitigate those risks. Understanding business risk, taking action to deter most important and most frequent attacks and following industry good practices gives us better security solutions.

REFERENCES

[1] F. Sheldon, J. Weber, S. Yoo, W. Pan, "The Insecurity of Wireless Networks." IEEE Computer Society, vol. 10, no. 4, July/August, 2012, pp. 54-61.

[2] L. Wang, B. Srinivasan, N. Bhattacharjee, "Security Analysis and Improvements on WLANs", Journal of Networks, vol. 6, no. 3, March 2011, pp. 470-481

[3] W. Ashford, "More than a quarter of London's Wi-Fi networks are poorly secured", 2012 http://www.computerweekly.com/news/2240162747/More-than-a-quarter-of-Londons-Wi-Fi-networks-are-poorly-secured, [Accessed on: 14/11/12].

[4] P. Feng, "Wireless LAN Security Issues and Solutions", IEEE Symposium on Robotics and Applications, Kuala Lumpur, Malaysia, 3-5 June, 2012, pp. 921-924.

[5] L. Phifer, "Wireless Lunchtime Learning Security School", 2009, http://searchsecurity.techtarget.com/guides/Wireless-Security-School, [Accessed on: 14/11/12]

[6] M. Souppaya, K. Scarfone, "U.S Department of Commerce - Guidelines for Securing Wireless Local Area Networks (WLANs)", Gaithersburg, MD 20899-8930: National Institute of Standards and Technology, 2012, SP 800-153.

[7] S. Reddy, K. Rijutha, K. Ramani, S. Ali, C. Reddy, "Wireless Hacking – A WiFi Hack By Cracking WEP", IEEE 2nd International Conference on Education Technology and Computer, Shanghai, China, 22-24 June, 2010, p. 189-193.

[8] J. Li, M. Garuba, "Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities", Fifth International Conference on Information Technology: New Generations, Las Vegas, Nevada, 7-9 April, 2008, pp. 557-562.

[9] D. Shiyang,"Compare of New Security Strategy With Several Others in WLAN", IEEE 2nd International Conference on Computer Engineering and Technology, Chengdu, China, 16-18 April, 2010. pp. 24-28.

[10] T. Stimpson, L. Liu, J., Zhang, R. Hill, W. Liu, Y. Zhan, "Assessment of Security and Vulnerability of Home Wireless Networks", IEEE 9th International Conference on Fuzzy Systems and Knowledge Discovery, Chongqing, China, 29-31 May, 2012, pp. 2133-2137.

[11] H. Bulbul, I. Batmaz, M. Ozel, "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (Wi-Fi Protected Access) and RSN (Robust Security Network) Security Protocols.", Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia, Adelaide, Australia, Jan 21-23, 2008. Belgium: Institute for computer Sciences, Social-informatics and telecommunications Engineering (ICST).

[12] P. Kahai, S. Kahai, "Deployment Issues And Security Concerns With Wireless Local Area Networks: The Deployment Experience At A University" Journal of Applied Business Research, 2004, vol. 20, no. 4, pp. 11-24.

[13] M. Mathews, R. Hunt, "Evolution of wireless LAN security architecture to IEEE 802.11i (WPA2)", University of Canterbury, New Zealand

[14] SANS Institute Infosec Reading Room, "Wireless LAN: Security Issues and Solution" 2003, US: SANS Institute, 1.4b.

[15] B. Forouzan, Data Communications & Networking. 4th edition. New York: McGraw-Hill, 2008

[16] Search Security, (2011) Information security tutorials [Online], Available at: http://searchsecurity.techtarget.com/tutorial/Information-security-tutorials, [Accessed on: 14/11/12]

[17] D. Welch, S. Lathrop, "Wireless Security Threat Taxonomy", Proceeding of the Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, U.S Military Academy, West Point, NY, 18-20 June, 2003, pp. 76-83

[18] N. Sunday, "Wireless Local Area Network (WLAN): Security Risk Assessment and Countermeasures", Thesis (MSc), Blekinge Institute of Technology, 2008.

[19] C. Hurley, F. Thornton, M. Puchol, R. Roger, "WarDriving Drive, Detect, Defend A Guide to Wireless Security", 2004, US: Syngress

[20] Y. Zahur, T. Yang, "Wireless LAN Security and Laboratory Designs" Journal of Computing Sciences in Colleges, vol. 19, no. 3, January 2004, pp. 44-60.

[21] Z. Tao, A. Ruighaver, "Wireless Intrusion Detection: Not as easy as traditional network intrusion detection", Tencon 2005 IEEE Region 10 Conference, Melbourne, Australia, 21-24 Nov, 2005, pp. 1-5

[22] M. Roche, "Wireless Hacking Tools", 2007, Available at: http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html, [Accessed on: 14/11/12]

[23] YouTube, "Dictionary vs. Bruteforce Attacks – Explained", 2008, Available at: http://www.youtube.com/watch?v=2hveQ8QZ9MQ, [Accessed on: 14/11/12].

[24] J. Lyne, "Hot Tipes for Securing Your Wi-Fi Network", 2012, http://www.sophos.com/en-us/medialibrary/Gated%20Assets/white%20papers/sophostipsforsecuringwifinetwork.pdf, [Accessed on: 14/11/12].

[25] K. Hole, E. Dyrnes, P. Thorsheim, P., "Securing Wi-Fi Networks", IEEE Computer Society, 2005, vol. 38, no. 7, pp. 28-34.