International Journal of Neural Networks
ISSN: 2249-2763 & E-ISSN: 2249-2771, Volume 2, Issue 1, 2012, pp.-10-13.
Available online at http://www.bioinfopublication.org/jouarchive.php?opt=&jouid=BPJ0000238

SECURITY AND VULNERABILITY ANALYSIS OF WIRELESS NETWORKS

BHATIA V.[1]*, GUPTA D.[2] AND SINHA H.P.[3]
[1]Baddi University of Emerging Sciences and Technology, Solan-173 205, Himachal Pradesh, India.
[2]Electronic Science Department, University College, Kurukshetra University, Kurukshetra-136 119, Haryana, India.
[3]M.M.University, Mullana-133 207, Haryana, India.
*Corresponding Author: Email- vinay4research@yahoo.com

Received: October 25, 2012; Accepted: November 06, 2012

Abstract- Recent years have witnessed an inclination towards wireless technology. This technology has well penetrated in computers and phones. The result is a wide range of networks emerging up collectively known as wireless networks. Due to various advantages these networks offer there has been an exponential increase in both deployment and use of these networks. However these networks are not limited by any physical boundaries which make the information on these networks prone to various forms of attacks. Thus with increase in need of wireless networks the security aspect of these ought to be analyzed. In this paper we present the analysis of various attacks on a popular form of these networks; the wireless LAN. In addition various security algorithms used to counter these attacks are explored in detail.

Keywords- Initialization Vector, TKIP, wireless LAN, wireless security, WEP.

Citation: Bhatia V. et al. (2012) Security and Vulnerability Analysis of Wireless Networks. International Journal of Neural Networks, ISSN: 2249-2763 & E-ISSN: 2249-2771, Volume 2, Issue 1, pp.-10-13.

Introduction

Today is the world of networks. Networks have penetrated all social and economical aspects of life. However recent years have witnessed a sudden inclination towards wireless networks [1]. The advantage of a wireless network is mobility and the freedom from the restriction of wires or a fixed connection. The benefits of having a wireless network further include easier setup, hassle less connections, ease of installation as no drilling and cabling is required. Moreover it saves time and botheration when physical places are shifted very often. Such networks allow easy expansion of networks also. These networks allow use of laptops anywhere within a region from home to office and thus provide the facilities as surfing internet, printing, file transfer and many more applications with an added advantage of mobility.

A wired network uses a number of wires for providing links between various network devices converting even a small network complex. [Fig-1] shows a typical wired LAN with few number of devices connect together to share common resources. On the other hand wireless networks don't use cables for connections. Instead, they use radio waves, like cordless phones. This allows increase in number of devices hereby called nodes to be connected without increasing the complexity. Instead these networks provide mobility and suppleness. [Fig-2] depicts a typical wireless LAN with number of nodes connected together. These networks are not limited by physical boundaries therefore they are vulnerable to various attacks. In this paper the authors intend to analyze some of popular attacks on a special standard IEEE 802.11 wireless local area network (WLAN). WLAN is the most common form of a wireless network usually found in campuses, hot spots, public building and hotels to provide internet facility to clients which they are in mobile mode. With increase in use and deployment of such networks, the need to protect them from various networks has come to picture. Keeping this in mind various security algorithms which may be used to protect a wireless network are also analyzed.

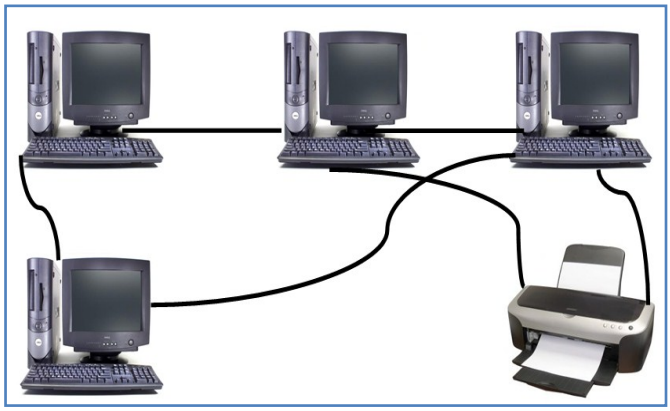

Fig. 1- Typical Wired LAN

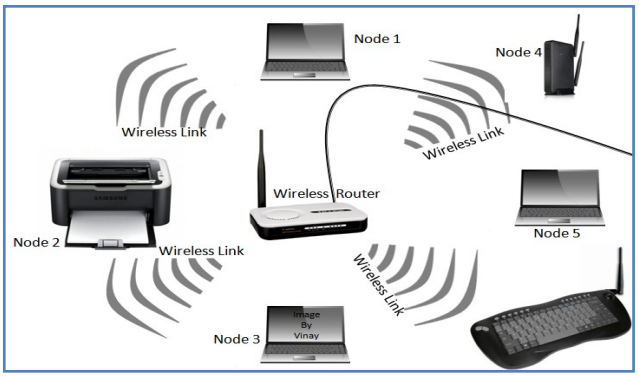

Fig. 2- Typical Wireless LAN

Attacks on Wlans

During the past few years, wireless LAN security threats have increased promptly which has affected users, vendors as well as manufacturers. The level of attacks has become more and more complex as attack applications available have become sophisticated and highly automated. The type of attack, the effect of the attack and the level of attack may vary from network to network. In this paper we intend to discuss various popular networks which affect a wireless LAN.

Dictionary Attack

A dictionary attack exploits the basic tendency of users to use weak passwords. In this attack, the wireless LAN is subjected to defeat by determining its secret key by repeatedly trying different passwords from a standard set, which in cryptography is known as the dictionary; hence the name Dictionary Attack [2-3]. Let us consider this challenge–response transaction between a sender S and receiver R which is commonly used in authentication protocols. In this transaction, both nodes can generate a random string. This string is transmitted to the other node so that it can encrypt the string with the key it has. The encrypted response is returned to the sender node and this is sufficient to guarantee that the peer does in fact posses the appropriate key. Let us consider a typical situation in which a sender S generates a random data packet (Dp) and sends it to receiver R after encrypting it using the secret key. This forms a challenge for the receiver R. R decrypts, calculates Dp +1 and returns it back to S after encryption.

However if secret key is a weakly chosen password, and it belongs to a set of words in the dictionary D, then the challenge – response transaction can be attacked. The intruder guesses a key $\in$ D and tries to decrypt both messages Dp and Dp + 1 with the guessed key. Using this key the intruder obtains two values, P and Q respectively. If P = Q + 1, then the attacker has deduced the correct secret key.

Brute Force Attack

In cryptography, a brute-force attack is a comprehensive key search that can, in theory, be used against any encrypted data. It involves systematically checking all possible keys until the correct key is found. In the worst case, complete search space may be exhausted during navigation [4]. The key length used in the encryption determines the realistic feasibility of performing a brute-force attack. Brute-force attacks can be made less effectual by camouflaging intended sense of the data to be encoded, something that makes it more difficult for an attacker to recognize even when intruder has cracked the code.

DDOS Attack

A denial of service occurs when an attacker has engaged most of the resources a host or network has available, rendering it unavailable to legitimate users. More specifically, this sort of attack targets the availability of the network i.e. by blocking network access, causing excessive delays, consuming valuable network resources, etc. The attack known as distributed denial of service causes denial of services in a wireless LAN [5]. A Distributed Denial-of-Service (DDoS) attack is characterized by one in which a large number of compromised systems attack a single target, thereby causing denial of service for users of the targeted system. The avalanche of data packets essentially forces the target to shut down, thereby denying service to the system to legitimate users.

In a typical DDoS attack, a hacker begins by exploiting vulnerability in one computer system and making it the DDoS master. From this master system the intruder identifies and communicates with other systems of the network whose security can be compromised. Since the intruder can instruct all controlled machines with a single command this attack becomes dangerous for any wireless network.

Wormhole Attack

In a wormhole attack, the malicious nodes perturb various routing protocols by creating tunnels [6] which affect to decision of choosing the route. Data packets are snooped using these tunnels which may be transmitted in remote location. This creates an illusion of fake routes in the network which appear more efficient. This disturbs the complete routing protocol and may cause undesirable effects in various part of the network. This results in rendering the network weak in terms of security and confidentiality.

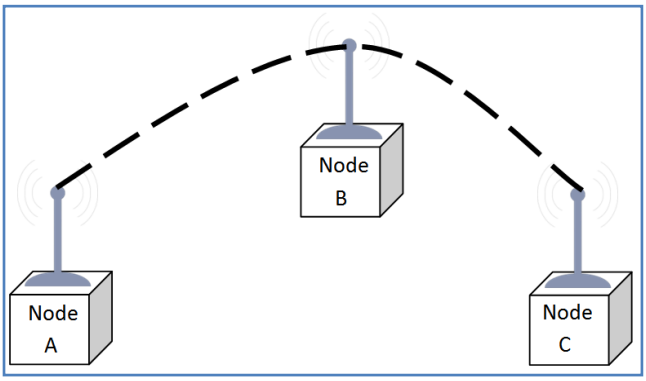

Fig. 3- Implementation of wormhole (Normal routing)

Since the wormhole attack is characterized by tunneling to capture data packets and replaying the same in some other part of the network, it become more dangerous for a wireless network [7]. This is because in a wireless network there is no physical boundary limitation due to which, the attacker can create wormholes for data which are not intended for him too.

Let us consider a part of wireless LAN in which node A has a data packet intended for node C through node B as shown in [Fig-3]. A wormhole attack creates transreceiver in this route so as to modify the routing path. This situation is shown in [Fig-4]. As seen from

the figure data packet is not available to the node B although the original routing protocol is designed to provide it. Thus similar situations create a different routing protocol which was not designed. This makes the network vulnerable to threats.

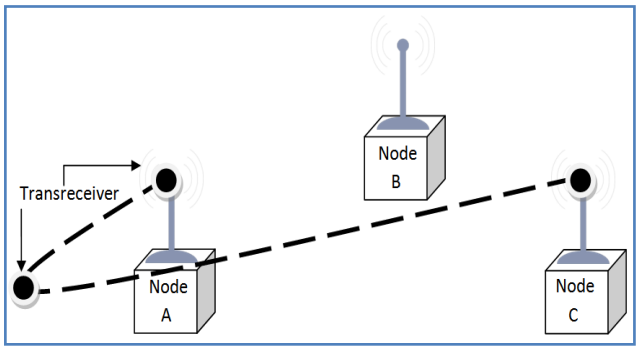

Fig. 4- Implementation of wormhole (Attack in action)

There are different ways in which a tunnel is set up during a wormhole attack. It could be by packet encapsulation of creating and out of band channel. The tunnel creates the false impression that the two end points are in close vicinity to each other, by making tunneled packets arrive either sooner with lesser number of hops compared to the packets sent over normal routes. This may completely change the routing algorithm. Once the wormhole attackers have control of a link, they can do a number of things to actively disrupt the network. The wormhole attack can affect network routing, data aggregation and clustering protocols, and location-based wireless security systems.

Man-in-the-Middle Attack - Evil Twin

The Evil Twin and the man-in-the-middle attack are closely related type of attacks in which passwords are forged by creating fake users which appear to be genuine. A man-in-the-middle attack refers to type of attack in which an attacker intercepts the information between two users by impersonation of legitimate users. The Evil Twin is a malicious server, which may be used to extract sensitive information such as bank details. Evil twin is a term for a malicious Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up by a hacker to snoop on wireless communications among Internet surfers. This type of attack may be used by an attacker to steal the passwords of unsuspecting users by either probing the communication link or by phishing, which involves setting up a fraudulent web site. This type of attack is usually followed by some another type of attacks already discussed to create a more hazardous effects. This type of attack can be avoided using security algorithms discussed in the next section.

Table 1- Vulnerability Analysis for Wireless LAN

S. No.	Various attacks on a wireless LAN Type of attack	Implementation Process
1	Dictionary attack	Attacker tries different passwords from a set of words in a dictionary
2	Brute force attack	Systematically checks all possible keys until the correct one is found
3	DDOS attack	Attacker engages most of the resources, leaving a few for genuine users
4	Wormhole attack	Creates a tunnel to spoil the routing protocols
5	Man-in-the-middle	Intercepts the information between two users

[Table-1] summarizes various attack forms and compares their modulus operandi. As inferred from the table all attack types vary in operation which makes use of a single security algorithm challenging. Subsequent section dwells on various security algorithms used practically to analyze their effect on different attack types discussed.

Security Algorithms

Since a wireless LAN is vulnerable to number of attacks, some of which have been described in previous section, it is important to secure a WLAN from them. This section describes various algorithms which may be employed to provide security in a wireless LAN.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is an encryption algorithm used to protect 802.11 networks developed by the 802.11b task force in 1997. It consists of RC4 encryption algorithm and has provisions for a 40 bit and a 104 bit key. The RC4 algorithm is a two step process consisting of the Key Scheduling Algorithm (KSA) and the Pseudo Random Number Generator (PRGA). WEP was intended to provide security similar to a wired network in a wireless LAN. WEP integrate two types of security, a secret key and encryption. The secret key comprises of 64 bits with a 24 bit IV (Initialization vector) to provide security. Another feature particular to WEP is integrity check. An integrity check ensures that packets are not changed during the transmission. This is accomplished using CRC-32 algorithm. The used in WEP is scrambled using a cryptographic function; RC4. RC4 is not particular to WEP but has been used in this algorithm. Although WEP was designed to secure a wireless network from different types of attacks but serious flaws were demonstrated in it ever since its launch [8-9]. Therefore this algorithm is still used as a security measure. WEP can keep away number of attacks using simple approach. WEP concatenates the data and IC with the keystream using the exclusive-or (XOR) function. Without an IV, the plaintext would always produce the same ciphertext. An eavesdropper would be able to see patterns and predict plaintext. With the IV, the ciphertext changes as the IV changes, so it would be more difficult for an eavesdropper to see patterns and predict plaintext. The WEP key is available in two strengths, 64-bit and 128-bit. The WEP keys are also referred to as 40-bit and 104-bit as the initialization vector is 24-bit. WEP uses the RC4 algorithm for encryption and the same key used to encrypt and decrypt the data. The purpose of the RC4 algorithm is to keep hackers from altering the data during the transmission. The RC4 algorithm then generates the keystream from the secret key and IV. By regenerating the RC4 keystream from the IV and the known key, the recipient can decrypt the data by running XOR.

Due to various problems, the IEEE has recommended both manufacturers and users to move away from WEP and adopt WPA which provides a stronger and currently resilient encryption.

Wi-fi Protected Access

Since various flaws of WEP were discovered the Wi-Fi Alliance discovered Wi-Fi Protected Access (WPA). WPA was discovered as an intermediate solution to various security threats which remained unanswered by WEP. Purpose was to provide the Wireless users to provide an immediate solution until a secure and stable

version was created. Although the underlying feature of WPA is also same as that of WEP, it differs in its strength to resist various attacks [9]. This is due to use of stronger encryption technology used. Typically it uses in Temporal Key Integrity Protocol (TKIP) which provides pre-packet key mixing and a message integrity check. TKIP utilizes a longer encryption key than WEP which employed a forty-bit key which is relatively weak even when properly implemented. The 128-bit WEP addressed this short-key problem but it was never part of an IEEE standard. Each 802.11 vendor implemented 128-bit WEP on its own, and these unique implementations caused problems for heterogeneous environments in which interoperability was an issue. By using longer keys and implementation standards, TKIP addresses WEP's short-key problem.

Although WPA is known to be stronger then WEP as it is effective against many attacks which WEP cannot withstand, but still fails to serve as the ultimate security protocol as it is vulnerable to Denial-of-Service attacks.

WPA shuts down the network if two packets using the wrong key are sent in any second. Practically when the access point receives these two packets it assumes the hacker is trying to gain access to the network. Therefore it shuts off all connections for 1 minute to avoid the possible compromise of resources on the network. Although this was done to provide strength against some wireless attacks, it is used by the attacker to his advantage to bring down the WPA protected wireless LAN. In this situation, a continuous string of unauthorized data could keep the network from operating indefinitely. In this way the security feature is exploited by the attacker to break in to network.

WPA has two variants: AES and TKIP. AES (Advanced Encryption Standards) is a stronger encryption scheme than RC4, the encryption scheme in WEP. TKIP makes use of the RC4 algorithm for encryption and hence is backward compatible with the WEP hardware. WPA2 made further changes to WPA by making AES encryption mandatory and using CCMP in place of MIC for integrity check. WPA comes in two modes, enterprise mode and consumer mode. Enterprise mode uses Remote Authentication Dial In User Service (RADIUS) for authentication. The RADIUS server checks that the information is correct using the authentication scheme Extensible Authentication Protocol (EAP) to process the information. RADIUS is the de facto standard for authentication and other protocols are rarely used. A RADIUS server can be used for different internet connections other than dial-up.

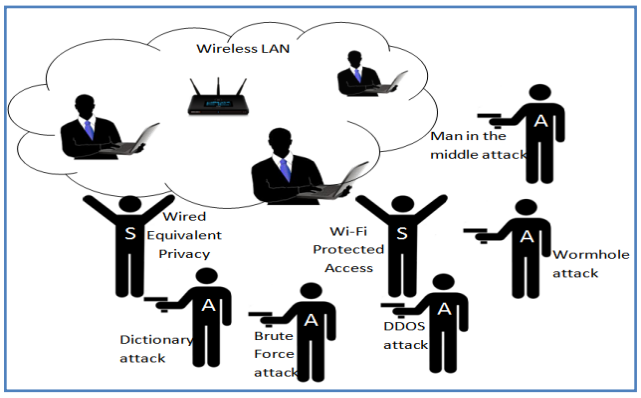

Fig. 5- Vulnerability and security of WLAN

The consumer mode (or personal mode) of WPA uses a combination of pre-shared keys (PSK), TKIP and MIC. The consumer version is typically used in homes or small offices, which require each user to enter a common password. If consumer mode users select the typical 6-8 character passwords that corporate networks require for login purposes, the resulting system will still be insecure. WPA-PSK (Wi-Fi Protected Access with Pre-Shared Key) is the better choice for SOHO users, because of its simple setup and deployment across a multi-vendor environment. Although WPA-PSK was originally intended for home users, it has been adopted by small offices due to the cost and difficulty in setting up a RADIUS server.

[Fig-5] depicts various forms of attacks a wireless LAN can be subjected to and security options available to counter them.

Conclusions

In this paper we have addressed to vulnerability and security issues in common wireless network; the wireless LAN used in SOHO networks. Various common wireless attacks have been analyzed with their protocols and working methods. Typically dictionary attack, brute force attack, denial of services attack, wormhole attack and the man-in-the-middle attack have been analyzed as part of vulnerability analysis. Another parameter of key concern analyzed is the security protocol available and its strength against various attacks. It is thus concluded that although no security protocol used practically is complete in the sense that it can withstand all wireless attacks but WPA due to increased key length and better encryption method is better than WEP as it is resistant to some attacks which the WEP is not.

References

[1] Rodoplu V. and Meng T.H. (2003) *IEEE Global Telecommunications Conference*, *GLOBECOM,* 5, 2819-2823.

[2] Delaune S. and Jacquemard F. (2004) *IEEE 17th Computer Security Foundations Conference*, 2-15.

[3] Vykopal J., Plesnik T. and Minarik P. (2009) *IEEE International Conference on Future Networks*, 23-27.

[4] Couture N. and Kent K.B. (2004) *Second Annual IEEE Conference on Communication Networks and Services Research*, 333 -336.

[5] Haddadi F. and Sarram M.A. (2010) *IEEE Second International Conference on Computer and Network Technology (ICCNT)*, 84- 87.

[6] Mahdi T., Naderi Majid, Barekatain and Bagher M. (2010) *IEEE 18th Iranian Conference on Electrical Engineering (ICEE)*, 331-335.

[7] Ren Y., Choo Chuah M., Yang J. and Chen Y. (2010) *IEEE Wireless Communications*, 36- 42.

[8] Williams J. (2001) *IEEE Journal IT Professional*, 3(6), 96, 91-95.

[9] Liu Y., Jin Z. and Wang Y. (2010) *IEEE 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM)*, 3(6), 96, 91-95.