International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359

Research Article | **February 2013**

Advanced Security Measures in a Wireless LAN

Kanak Pawade
Shri Shivaji College of Engg.& Technology,
Akola - 444005.
Maharashtra, India.

Abstract-

Wireless local area networks (wireless LANs, or WLANs) are metamorphosing the landscape of computer networking. The use of mobile computing devices, such as laptops and personal digital assistants, coupled with the demand for continual network connections without having to "plug in," are driving the adoption of enterprise WLANs. Network managers are using WLANs to facilitate network moves, add-ons and changes. In addition, the inherent flexibility of WLANs overcomes limitations created by older buildings, leased spaces, or temporary work areas. This paper not only furnishes the details about Wireless LANs but also bestows an abundant number of methods in which the security of these WLANs can be breached. It also contributes a myriad number of ways in which one can thwart the potential assault on the WLANs network..

KEYWORDS : IEEE802.11i, TKIP, VPN, WEP, Wi-Fi Protected Access, Wireless network MAC layer, WLAN security

I. INTRODUCTION

Wireless data communications have transformed not only the business world but also the whole human society by improving efficiency, flexibility, convenience and above all productivity besides providing the unique location, device and time-independent connectivity. Information security describes all measures taken to prevent unauthorized use of electronic data – whether this unauthorized use takes the form of disclosure, alteration, substitution, or destruction of the data concerned.

II. CHALLENGES IN WLAN

A. Seven wireless Networks security challenges – when a wireless network is established, designing

a secured network is a concern. Here are the seven key WLAN security challenges are;
1) Easy access – Strictly speaking this is not a security threat, but information available about a wireless Network is also the information needed to launch an attack on the network.
2) Rogue Access Points (AP) – Rogue AP's deployed by end users pose great security risks.
3) Unauthorized use of services – Most of the AP'srunning with default configurations have not activated with Wired Equivalent Privacy (WEP) .
4) Services and performance constraints – WLAN have limited transmission capacity. If an attacker were to launch a ping flood from a fast Ethernet segment it could easily overwhelm the capacity of an AP.
5) Mac spoofing and session hijacking – 802.11 networks do not authenticate frames like a traditional Ethernet , there is no protection against forgery of frame sources addresses. Attackers can use spoofed frames to redirect traffic and corrupt address resolution protocol (ARP) tables. At a much simple level attackers can observe the MAC addresses of station in use on the network and adopt those addresses for malicious transmission.
6) Traffic analysis and eaves dropping – 802.11 provide no protection against attacks that passively observe traffic. The main risk is that 802.11 do not provide a way to secure data in transit against eaves dropping.
7) Higher level attacks – Once an attacker gains access to a wireless network it can serve as a launch point for attacks on other systems.

B. Typical Wireless Security Attacks

Here comes some of the possible wireless security attacks, yet there are still more attack types.

WEP Cracking – WEP, the primary security algorithm currently under use, is vulnerable because, the encryption keys remain static [1]. The encryption key used by WEP [1], regardless of its length, never changes unless it is periodically and manually changed by the administrator on all devices. An attacker uses a relatively inexpensive wireless packet sniffer to collect packets. After gathering five to 10 million packets, the attacker runs readily available tools that can determine encryption keys of the cipher message in a few minutes, enabling the attacker to decrypt and read all data passing between the user and access point.

MAC Attack – Media Access Control **(**MAC) addresses can be cracked in the same way as WEP [1] encryption key .Once the encryption key is deciphered, all packets including the MAC ID is exposed. If no encryption is used, the MAC ID can be simply plucked from the air. Once a valid MAC address has been obtained, hackers can program their computer to spoof a valid user by programming a computer to broadcast the stolen ID.

Man-in-the-Middle Attacks – A hacker situated between the client and access point, intercepting all traffic, characterizes this type of attack. The hacker captures and decrypts the frames sent back and forth between a user's wireless NIC and AP during the association process. This provides essential information about the Wireless NIC and AP such as the IP addresses for both devices, the Wireless NICs association ID, and the network's SSID. With this information, someone can set up a rogue access point on a different wireless channel closer to a particular user, to force the user's wireless NIC to re-associate with the bogus access point. Both client and server believe they are connected directly each other, but instead are connected to a man in the middle. The attacker has access to all data passed between the two entities including login information.

Dictionary Attacks - This type of attack relies on conventional names and words being used as login names and passwords. The attacker gathers a challenge and response exchange from password-based protocols. Using open source tools based on a dictionary of hundreds of thousands of words, names and phrases, an offline computer tries essentially every name-password combination, and until the login information is decrypted. Once a name and password have been cracked, the attacker has access to the WLAN with all the rights and privileges of that user.

Session Hijacking – When an attacker is capable of not only listening to network traffic but also inserting their own information, a session is then susceptible to hijacking – redirecting it away from a legitimate end point. A hacker can set up an access point, and unsuspecting wireless LAN clients will try to connect to it by sending their authentication information.

Denial of Service (DOS) - DOS attacks are easily applied to wireless networks. An attacker can flood access points with illegitimate traffic, overwhelming that available bandwidth, slowing or stopping legitimate users from accessing the network.

C. WLAN Security - Processes.

Access Control is the process of ensuring that only trusted users can gain access to network resources and they can see only what they are authorized to see. It comprises two elements: authentication and authorization.

Authentication is the process the user confirms his/her identity to the system and authorization involves control over what the user can do on the system once he or she has been authenticated. Authentication systems range from simple name-password pairs, to more elaborate challenge-response systems, such as smart cards and biometrics. Role based Access control (RBAC) method is one such mechanism, where the access rights to the data and resources are granted based on job responsibilities. RBAC roles are created according to the job functions performed in an organization, permissions are granted

to those roles and finally users are assigned to the roles in accordance with their specific job responsibilities and qualifications. The confidentiality or privacy of communications is fundamental to a secure system and the usual way to ensure confidentiality is to employ encryption. WEP [6] algorithm has been the main stay for this encryption.

Integrity is the assurance that data has not been altered by anybody unauthorized to alter it. There are three ways in which access control is provided.

Service Set Identifier (SSID) - Network access control can be implemented using an SSID associated with an AP or group of access points. The SSID provides a mechanism to segment a wireless network into multiple networks serviced by one or more access points. Each AP is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID to access the AP, the SSID acts as simple password and thus provides a measure of security.

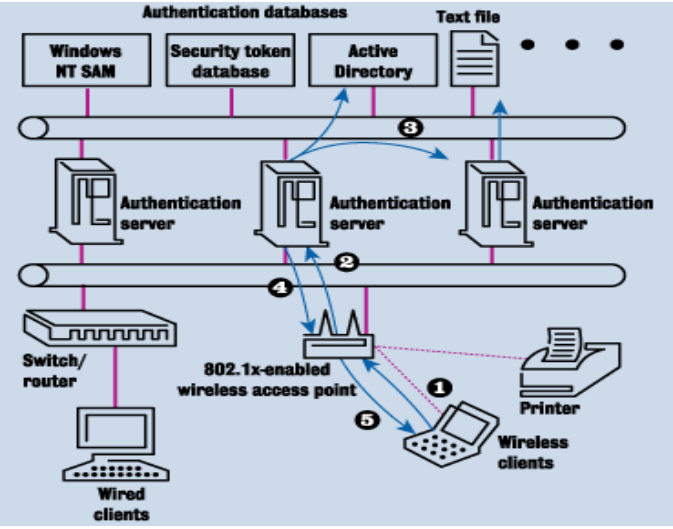
MAC Address Filtering - The second method is to use the unique Medium Access Control (MAC) identifier that is part of every Ethernet device. While an AP or group of access points can be identified by an SSID, a client computer can be identified by the unique MAC address of its 802.11 [2] network card. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the client computers to access it. If a client's MAC address is not included in the list, the client is not allowed to associate with the AP. This procedure is very effective for smaller operations where the MAC address list can be efficiently managed. Each AP must be manually programmed with a list of MAC addresses and the list must be kept up-to-date.

WEP-based Security - The third way is to use WEP security protocol to provide encrypted communication between the client and an AP. WEP employs the symmetric
key encryption algorithm, Ron's Code Pseudo Random Number Generator (RC4 PRNG). The shared secret is typically a 40-bit key or a 104-bit key shared between many stations. A key shared between the AP and its many stations is called a default key. A key shared between the AP and only one other station is called a key-mapping key. Both default keys and key-mapping keys are subsequently used to protect communications between associated stations.

The WEP protocol is primarily used to protect (MAC Protocol Data Units) MPDUs. It uses the default key or key-mapping key and the RC4[5] algorithm for encryption, and it uses CRC-32 to compute an Integrity Check Value (ICV) over the MPDU data. The resulting 32-bit ICV is appended to the MPDU prior to encryption. The RC4 [4] key is composed of a 24-bit Initialization Vector (IV) value concatenated with the default key or key-mapping key to form a per-packet key. The MPDU data and ICV are then encrypted under the per-packet key. The IV and a key identifier are pretended to the encrypted MPDU data field, forming the complete WEP protocol data unit. The receiver, which knows the shared key, is able to reproduce the key stream and to decrypt the message. If the ICV matches, the message is assumed to be authen

.

III. IEEE STANDARDS & WIRELESS NETWORKS-



802.1X- The protocols, algorithms, and techniques involved with improving the current 802.11 standard's security are complex and very interdependent. The 802.1X standard is a port based network access control that provides a framework for user authentication and dynamic encryption key distribution.

Fig2– How 802.1x wireless security process work

What Is Wi-Fi?

Wi-Fi stands for wireless fidelity. Personal computers (PCs) can be equipped with Wi-Fi adapters (which are available as internally-mounted cards, most typically a USB adaptor. Most laptops are standard now with a Wi-Fi interface that will handle all current Wi-Fi standards, including 802.11a/b/g/n. Wi-Fi adapters are fairly inexpensive. The adapters seek out signals broadcast by devices called access points (APs) that in turn are typically connected to the existing wired network. This gives Wi-Fi devices access to the same resources that devices connected to the wired network have. Although it is less common, Wi-Fi devices can also communicate directly (one-to-one) with each other. Wi-Fi devices, if capable, will adapt to the standard in use by APs within range and employ several different

technical standards grouped together and referred to as the IEEE 802.11 specification in order to communicate with an AP. a)

Table 1 – 802.11 Speed Comparison

IEEE Wireless Specification Designation	Release Date	Operating Frequency Range	Throughput Speeds (maximum)	Effective Throughput Speeds (typical)	Range (typical indoor distance in meters)
802.11a	1999	5.15-5.35/5.47-5.725/5.725-5.875 GHz	54 Mb/s	22 Mb/s	~25 meters
802.11b	1999	2.4-2.5 GHz	11 Mb/s	5 Mb/s	~35 meters
802.11g	2003	2.4-2.5 GHz	54 Mb/s	22 Mb/s	~25 meters
802.11n	2009	2.4 GHz or 5 GHz bands	600 Mb/s	100 Mb/s	~50 meters

There are three entities that are involved with this approach to authentication as in fig.3;

1) The supplicant - software resides on the wireless device
2) Authenticator – is the access point (AP)
3) The authenticator server – is most likely the RADIUS server

The first goal of 802.1X is to require a successful authentication of a user before a full network connection can be established. When the wireless device initiates connection with the AP, the AP creates a logical port that works in an unauthorized state until the user has been properly authenticated. The unauthorized state means that no traffic, other than authentication frames is allowed to pass. An analogy is having a chain on the front door, which will allow identifying a person who knocks before, allow him to enter into the house. The AP acts basically as middleman between the wireless device and the authentication server; it just passes the information between the two entities. The AP will only allow the wireless device to communicate with the authentication server until the entire authentication steps are completed successfully. After this the wireless device can then participate with the full network and its resources.

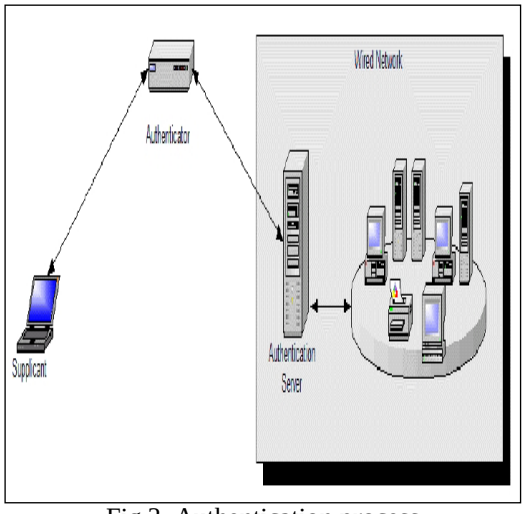


Fig.3. Authentication process

IV. WI-FI PROTECTED ACCESS (WPA)

WPA addresses the security vulnerabilities found in WEP-enabled 802.11 [4] WLANs. For example, WPA-compliant products will include dynamic key generation, as well as an improved RC4 data encryption scheme that uses Temporal Key Integrity Protocol (TKIP) and mandatory 802.1x authentication.

WPA is a software upgrade recommended by the IEEE 802.11i standard body to existing WEP-based Wi-Fi [4]certified hardware while maintaining forward compatibility with the future 802.11i standard. WPA provides WLAN users with data protection while helping to ensure that only authorized users gain access to the network. WPA has addressed all the

WEP vulnerabilities and can provide effective protection against both non-targeted and targeted attacks. Implementation of WPA will make it possible for enterprises to protect their campus wireless LANs with scalability without deploying VPN/firewall technology. WPA combines the functionality of 802.1X with TKIP that addresses the vulnerabilities of the static keys used in WEP. A TKIP implement rapid re-keying by generating a new encryption key every 10000 packets and uses a mixing function to cryptographically hash the initialization vectors of data packets with the shared key. TKIP is based on the same RC4 algorithm with 40-bit key used in WEP. The combination of 802.1X authentication, authentication protocols, dynamic keys and TKIP enhancements is a transitional step that enables enterprises to implement
WLANs increased data privacy and integrity protection. The TKIP process begins with a 128-bit temporal key shared among clients and access points. TKIP combines the temporal key with a client's MAC address, and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt data. TKIP provides an automated key mechanism, changing the temporal keys every 10, 000 packets. This offers a dynamic distribution method that significantly enhances the security of the network. TKIP employs a message integrity check (MIC), which adds stronger integrity checking than a simple CRC check to prevent attackers from changing messages after transmission.

Temporal Key Integrity Protocol (TKIP):

Having come across the deficiencies found in WEP, the IEEE 802.11TGi has come out with this short-term solution. TKIP installation will include a firmware upgrade and a driver upgrade. The requirements are defined as;

1) Deployed systems are to be software or firmware upgradeable
2) The current WEP hardware implementation to remain unchanged and
3) Minimize performance degradation imposed by the fixes.
4) TKIP is a set of algorithms that adapt the WEP protocol to address the known flaws while meeting these constraints. TKIP wraps WEP in three new elements
5) A message integrity code (MIC), called Michael, to defeat forgeries
6) A packet sequencing discipline, to defeat replay attacks
7) A per-packet key mixing function to prevent FMS (Fluher, Mantin and Shamir) attacks.

V. OTHER EFFECTIVE WIRELESS LAN SECURITY SOLUTIONS

A. Virtual Private Network *(VPN) over* WEP-enabled WLAN. A VPN enables users on a public or un-trusted network such as the Internet or a WEP-based Wireless LAN to establish a secure connection to a private network. The VPN protects the wireless LAN by creating a tunnel that shields data from unauthorized access. VPNs enable a high level of
trust through the use of proven industry-standard security mechanisms, including IPSec that employs strong algorithms such as Triple data encryption standard to encrypt data with other algorithms for authentication of data packets. IPSec also uses digital certificates to validate public keys. When used over a wireless LAN, the VPN gateway handles authentication, encapsulation and encryption. The combination of an IPSec-based VPN and 802.11 with WEP provides a practical and scalable solution for the protection of mission-critical data transmitted over a wireless LAN.

B. Key Distribution Method

In order to overcome the current practice of manually setting the group key in every station of a wireless LAN, here comes a simple key management scheme.

1) Every user U1, U2,….. Un to participate in a WLAN is assigned an individual key KUi to be used for distributing the group keys to them. These individual keys are stored in a central key management server (KMS) that has to be secured appropriately. As individual key of a user also needs to be available at the terminal of the user (for example, a laptop or any other mobile devices), it either has to be stored on the terminal, or to be computed on the fly.
2) The central KMS regularly generates a new group key K group and distributed it to i) all mobile stations by using specific broadcast messages, which are sent without encrypting them in the MAC layer, ii) all access points by setting the appropriate MIB-variable via the simple network management protocol (SNMP) and
3) The broadcasted key distribution frames contain a name identifying the key management domain (e.g. the name of the key management server), the sequence number p of the group key K group :p currently in use,
the sequence number q of the group key K group :q distributed in this key frame (these two numbers are used for fast setup and detection of a new group key), two numbers r and s defining the range of user-ids for which the group key is distributed in this key management frame, an integrity check value over the common part of the key management frame which is generated using the group key K group :q and for every user-i in the range [r, s], a tuple (I, E(K Ui, K group:q)).
When a user switches on his mobile phone, the key management process (KMP) is started. After receiving the first key distribution frame, KMP asks the user to type in his passphrase for the key management domain with the name specified in the receive frame. Using the passphrase the KMP computes the user's key KUi for this key management domain either by

decrypting the appropriate entry in the key-file, or by directly mapping the passphrase to the key, e.g. computing a cryptographic hash value of the passphrase. From local configuration information the KMP reads the identity i of the user in this key management domain, looks for the appropriate entry in the key distribution frame, and then decrypts the group key. After obtaining the group key K group :q, KMP computes the integrity check value and compares it to the value included in the key management frame. If both values match, the key management frame is assumed to be authentic. For computation of the integrity check value the authors have proposed to use the cryptographic hash function SHA-1 in the HMAC construction.

C. Firewall

Has the ability to restrict network traffic through a gateway according to a set of rules. Typically located at a gateway or access point, it controls the flow of traffic, preventing inside and outside users from accessing data and services as defined by the system administrator. Superior firewalls employ stateful packet inspection, rather than just packet filtering technology. WLANs can be isolated from the wired network with a firewall.

VI. WLAN SECURITY COMPONENTS-

IEEE 802.1X provides network login capabilities between PCs and the edge-networking infrastructure. It offers an architectural framework for implementing various authenticating schemes. 802.1X does not provide encryption as WEP, 3DES, AES or any other cipher. 802.1X focus on authentication and key management and it can be used in conjunction with a cipher. 802.1X is not a single authentication method and it utilizes EAP as its authentication framework and hence any 802.1X-enabled switches and access points can support a wide variety of authentication methods. It supports open standards for authentication, authorization, and accounting including RADIUS and LDAP, so it works with existing infrastructure for managing remote and mobile users. Using an authentication protocol such as EAP-TLS, LEAP, or EAP-TTLS, 802.1X provides port-based access control and mutual authentication between clients and access points via an authentication server.

RADIUS (Remote Authentication Dial-in User Service)

For authentication to work, the user's transmission must go through a wireless LAN access point to reach the back-end server performing the authentication. The wireless client contacts the access point, which in turn communicates with the RADIUS server on the enterprise LAN. The RADIUS server then verifies the client's credentials to determine whether the device is authorized to connect to the LAN. If the RADIUS server accepts the client device, the server sends data, including security keys, to the access point to enable a secure connection with the client.

VII. Using VPN technologies to protect data

VPN technologies such as IPsec with 3DES can protect data by ensuring that users authenticate to the network and credentials are made available to all access points in the environment that appropriate access control policies are enforced throughout the wireless network, and that encryption is efficiently implemented to protect enterprise data. In additional, cryptographic hashing function such as MD-5 or SHA-1 can also be used to ensure the integrity of the information transmitted over the wireless LAN.

VIII. Policing bandwidth for fair access and attack prevention

Wireless access points have low bandwidth capabilities and are shared by multiple users. This scenario allows intruders to simply blast traffic over the wireless link to prevent additional traffic with what are known as Denial-of-Service attacks. But even legitimate users can unintentionally hog bandwidth in the course of their everyday responsibilities. As part of the packet filtering solution, a good solution installs software that controls traffic by slowing large downloads in addition to a wide variety of other measures**.**

Experimental Work

Our work in the current generation of tether-less networks that transmit data over unlicensed radio frequencies has already demonstrated its effectiveness in a host of vertical markets, including health care, retail, manufacturing, logistics, warehousing and academia. Now as it find ways into more general business settings and, increasingly, into publicly accessible implementations, WLAN is definitely poised for a boom. Wireless technology changes the network paradigm of the wired user going to where the data Is, to the data going to the user. As such, wireless can support a variety of business critical applications that cannot be effectively met with conventional, wired connections. For day-today applications, wireless can provide convenient network access to improve worker productivity. Network designs will, of course, continue to be affected by the development of new technologies and user demands.

The next wave of wireless LANs is likely to be driven by mobility. 802.11 provide link-layer mobility. Users can move transparently within an IP subnet with no effect on their applications or connection. The mobile user can call the data up anywhere at any time. Due to the vulnerability of the wireless channel users may not feel comfortable of using or accessing their and applications and files by wireless Internet.

Network security is gaining attention as more number of enterprises are switching to WLANs having felt the need for stronger, faster, and efficient authentication, authorization, Integration and non- repudiation processes to keep the corporate information from excessively or impertinently inquisitive people. An effective and efficient security solution may enhance the utilization of pervasive and ubiquitous computing systems for information on demand and all kinds of applications.

CONCLUSION

It is preferable to have only one access point and make it run under a secure operating system like Linux. It is better to occasionally boot up and trap sections of traffic to look for any attack signatures. The user must connect via a VPN, the access point is secured so it cannot be reset, WEP is enabled, and access point is in a position that limits travel of the radio frequency outside of the premises. The traffic between the access point and the LAN passes through a firewall to help block any possible DOS attacks on the WLAN from entering the enterprise LAN.

ACKNOWLEDGMENT

Author gratefully acknowledge the contributions of Proff. Chopde. Professor of Shri Shivaji College Of Engg And Technology, Akola.

Proff. Arti Gutam. Proffesor of Shri Shivaji College Of Engg And Technology, Akola.

REFERENCES

1. David; Security of the WEP algorithm; March 4, 2005; http://www.isaac.cs.berkeley.edu/isaac/wepfaq.Html
2. BORISOV, N., GOLDBERG,I., AND WAGNER, D., Intercepting mobile communications: The insecurity of 802.11, MOBICOM 2001,2001.
3. Fluhrer S., Mantin I., Shamir I., Weaknesses in the key scheduling algorithm of RC4, SAC.2001, 2001.
4. Geier, Jim; 802.11 WEP: Concepts and Vulnerability; March 4, 2005; http://www.wifiplanet.com/tutorials/article.php/1368661
5. Mister and Tavares. Cryptanalysis of RC4-like ciphers. In SAC: Annual International Workshop on Selected Areas in Cryptography.LNCS, 1998. nudsen, Meier, Preneel, Rijmen, and Verdoolaege. Analysis methods for (alleged) RC4. In ASIACRYPT: Advances in Cryptology { ASIACRYPT: International Conference on the Theory and Application of Cryptology.LNCS, Springer-Verlag, 1998.
6. Prasithsangaree P., Krishnamurthi P., Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs, Global Telecommns. Conf., Globecom.03, Dec. 2003.
7. RIVEST, R., RSA Security response to weaknesses in key scheduling algorithm of RC4, http://www.rsasecurity.com/rsalabs/technotes/wep.html, 2001.
8. IEEE Std 802.11-1997. Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications, 18 Nov. 1997.