International Journal of Scientific Research Engineering & Technology (IJSRET)
Volume 1 Issue5 pp 171-178 August 2012 www.ijsret.org ISSN 2278 – 0882

Data Security on WLAN

[1]Naveen Kumar, [2]B.S.Roohani
[1, 2]Computer Science & Engineering
Babu Banarasi Das Institute of Engineering Technology & Research Centre, Bulandshahr, U.P
naveen9001@gmail.com
bsroohani2007@gmail.com

ABSTRACT
A Wireless local area network (WLAN) has been widely used in many sectors. As the name wireless means a network without wire in which radio signals are used to transmit data. This technology is very popular due to several reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it or intend to use it should be aware of these threats. In this paper we will look at different types of attacks such as Denial of Service, Spoofing, and Eavesdropping. The IEEE standard used for the encryption for wireless networking is 802.11b/WiFi.
This paper will then explain how Wired Equivalent Privacy (WEP) works, which is the IEEE standard used for encryption of data. Discussion of WEP continues by examining its weaknesses, which result in it being much less secured than what was originally intended. This situation leads to further research regarding practical solutions in implementing a more secured WLAN. Finally, this paper ends with the conclusion of highlighted issues and solutions.

KEYWORDS*: Wireless – network, WLAN, Mobile – access, W EP, Access Point, ICV*

I. INTRODUCTION
The introductory section gives brief information on the WLAN components and its architecture in order to examine the WLAN security threats. A Wireless local area networks (WLANs) based on the Wi-Fi (wireless fidelity) standards are one of today's fastest growing technologies in businesses, schools, and homes, for good reasons. They provide mobile access to the Internet and to enterprise networks so users can remain connected away from their desks. These networks can be up and running quickly when there is no available wired Ethernet infrastructure. They can be made to work with a minimum of effort without relying on specialized corporate installers. A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, 802.11 were implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. The currently most spread and deployed standard, IEEE 802.11b, was introduced late 1999. It still operates in the same frequency range, but with a maximum speed of 11 Mbps. WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing.

All wireless computer systems face security threats that can compromise its systems and services. Unlike the wired network, the intruder does not need physical access in order to pose the following security threats:

Eavesdropping: This involves attacks against the confidentiality of the data that is being transmitted across the network. In the wireless network, eavesdropping is the most significant threat because the attacker can intercept the transmission over the air from a distance away from the premise of the company.

Tampering: The attacker can modify the content of the intercepted packets from the wireless network and this result in a loss of data integrity.

Unauthorized access and spoofing: The attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This kind of attack is known as spoofing. To overcome this attack, proper authentication and access control mechanisms need to be put up in the wireless network.

Denial of Service: In this attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. The attacker could also flood a receiving wireless station thereby forcing to use up its valuable battery power.

Other security threats: The other threats come from the weakness in the network administration and vulnerabilities of the wireless LAN standards, e.g. the vulnerabilities of the Wired Equivalent Privacy

(WEP), which is supported in the IEEE 802.11 wireless LAN standard.

II. COMPONENTS OF WLAN

One important advantage of WLAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the needs to pull cable through walls and ceilings. The physical architecture of WLAN is quite simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NICs)/client adapters.

Access Points: Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable and communicates with wireless devices by means of an antenna. An AP operates within a specific frequency spectrum and uses 802.11 standard specified modulation techniques. It also informs the wireless clients of its availability and authenticates to associates wireless clients to the wireless network.

Network Interface Cards (NICs)/client adapters: Wireless client adapters connect PC or workstation to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with APs available in PCMCIA (Personal Computer Memory Card International Association) card and PCI (Peripheral Component Interconnect) card. These cards are used to connect desktop and mobile computing devices wirelessly to all network resources. The NIC scans the available frequency spectrum for connectivity and associates it to an access point or another wireless client. It is coupled to the PC/Workstation operating system using a software driver. The NIC enables new employees to be connected instantly to the network and enable Internet access in conference rooms also.

III. ARCHITECTURE OF WLAN

The above mentioned components of WLAN can be connected in certain configurations. There are three main types of WLAN architecture: Independent, Infrastructure and Microcells and Roaming.

Independent infrastructure of WLAN: The simplest WLAN configuration is an independent or peer-to-peer WLAN. It is a group of computers, each equipped with one wireless LAN NIC/client adapter. In this type of configuration, no access point is necessary and each computer in the LAN is configured at the same radio channel to enable peer-to-peer networking. Independent networks can be set up whenever two or more wireless adapters are within range of each other.

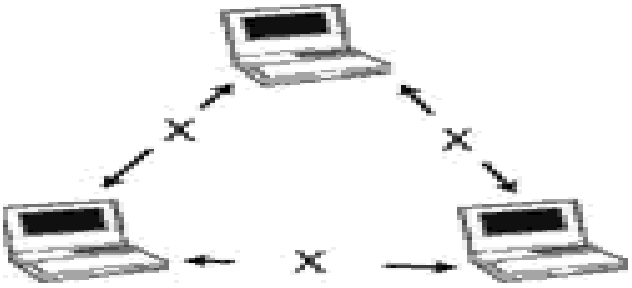

Figure 1: Architecture of Independent WLAN.

Infrastructure WLAN: Infrastructure WLAN consists of wireless stations and access points. Access Points combined with a distribution system (such as Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility. The access points not only provide communications with the wired network but also mediate wireless network traffic in the immediate neighborhood. This network configuration satisfies the need of large-scale networks arbitrary coverage size and complexities.

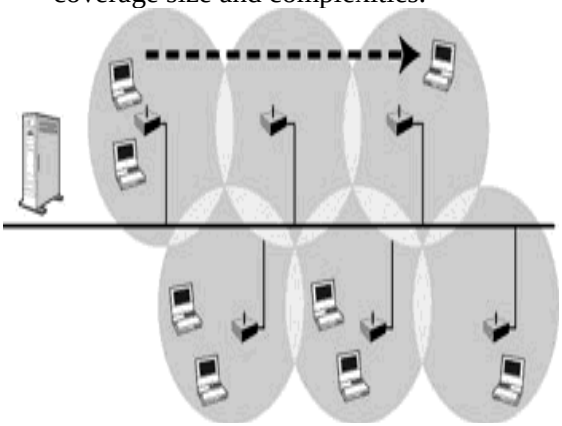

Figure 2: Architecture of Infrastructure WLAN.

Microcells and Roaming: The area of coverage for an access point is called a "microcell'. The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access. One of the main benefits of WLAN is user mobility. Therefore, it is very important to ensure that users can move seamlessly between access points without having to login again and restart their applications. Seamless roaming is only possible if the access points have a way of exchanging information as a user connection is handed off from one access point to another. In a setting with overlapping microcells, wireless nodes and access points frequently check the strength and quality of transmission. The WLAN system hands off roaming users to the access point with the strongest and highest quality signal in accommodating roaming from one microcell to another.

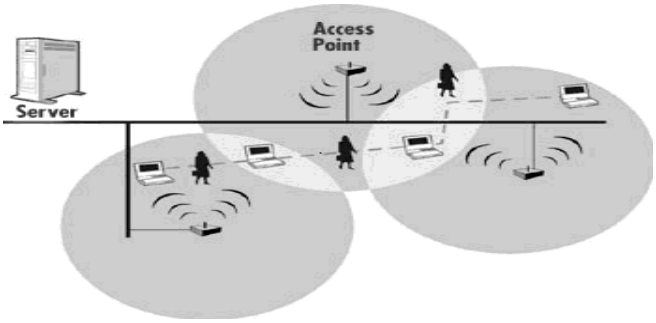

Figure 3: Architecture of Microcells and Roaming

IV. SECURITY THREATS OF WLAN

As the WLAN uses radio waves for carrying the data it create a risk where the network can be hacked. This section explains three examples of important threats: Denial of Service, Spoofing and Eavesdropping.

Denial of Service: In this kind of attack the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attacks. By using a powerful enough transceiver, radio interference can easily be generated that would unable WLAN to communicate using radio path.

Spoofing and Session Hijacking: *H*ere the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. Moreover, 802.11 do not require an Access Point to prove it is actually an AP. This facilitates attackers who may masquerade as AP's. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN.

Eavesdropping: This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance away from the premise of the company.

V. WIRED EQUIVALENT PRIVACY

Wired Equivalent Privacy (WEP) is a standard encryption for wireless networking. It is a user authentication and data encryption system from IEEE 802.11 used to overcome the security threats. Basically, WEP provides security to WLAN by encrypting the information transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the information. The following section explains the technical functionality of WEP as the main security protocol for WLAN.

Working of WEP: When installing WLAN, it is important to understand the ability of WEP to improve security. This section describes how WEP functions accomplish the level of privacy as in a wired LAN. WEP uses a pre-established shared secret key called the base key, the RC4 encryption algorithm and the CRC-32 (Cyclic Redundancy Code) checksum algorithm as its basic building blocks. It supports up to four different base keys, identified by Key IDs 0 thorough 3. Each of these base keys is a group key called a default key, means that the base keys are shared among all the members of a particular wireless network. Some implementations also support a set of nameless per-link keys called key-mapping keys. However, this is less common in first generation products, because it implies the existence of a key management facility, which WEP does not define. The WEP specification does not permit the use of both key-mapping keys and default keys simultaneously, and most deployments share a single default key across all of the 802.11 devices.

WEP tries to achieve its security goal in a very simple way. It operates on MAC Protocol Data Units (MPDUs), the 802.11 packet fragments. To protect the data in an MPDU, WEP first computes an integrity check value (ICV) over to the MPDU data. This is the CRC-32 of the data. WEP appends the ICV to the end of the data, growing this field by four bytes. The ICV allows the receiver to detect if data has been corrupted in flight or the packet is an outright forgery. Next, WEP selects a base key and an initialization vector (IV), which is a 24-bit value. WEP constructs a per-packet RC4 key by concatenating the IV value and the selected shared base key. WEP then uses the per-packet key to RC4, and encrypt both the data and the ICV. The IV and Key ID identifying the selected key are encoded as a four-byte string and pre-appended to the encrypted data.

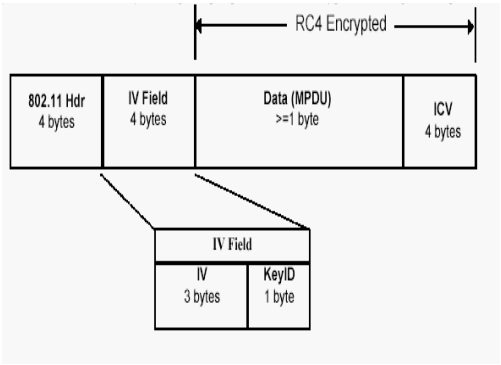

Figure 4: WEP-encoded MPDU

The IEEE 802.11 standard defines the WEP base key size as consisting of 40 bits, so the per-packet key consists of 64 bits once it is combined with the IV. Many in the 802.11 community once believed that small key size was a security problem, so some vendors modified their products to support a 104-bit base key as well. This difference in key length does not make any different in the overall security. An attacker can compromise its privacy goals with comparable effort regardless of the key size used. This is due to the vulnerability of the WEP construction which will be discussed in the next section.

Weaknesses of WEP: WEP has undergone much scrutiny and criticism that it may be compromised. What makes WEP vulnerable? The major WEP flaws can be summarized into three categories:

No forgery protection: There is no forgery protection provided by WEP. Even without knowing the encryption key, an adversary can change 802.11 packets in arbitrary, undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user. Even worse, an adversary can also learn more about the encryption key with forgery attacks than with strictly passive attacks.

No protection against replays: WEP does not offer any protection again replays. An adversary can create forgeries without changing any data in an existing packet, simply by recording WEP packets and then retransmitting later. Replay, a special type of forgery attack, can be used to derive information about the encryption key and the data it protects.

Reusing initialization vectors (IV): By reusing initialization vectors, WEP enables an attacker to decrypt the encrypted data without the need to learn the encryption key or even resorting to high-tech techniques. While often dismissed as too slow, a patient attacker can compromise the encryption of an entire network after only a few hours of data collection. A report done by a team at the University of California's computer science department presented the insecurity of WEP which expose WLAN to several types of security breaches. The ISAAC (Internet Security, Applications, Authentication and Cryptography) team which released the report quantifies two types of weaknesses in WEP.

The first weakness emphasizes on limitations of the Initialization Vector (IV). The value of the IV often depends on how vendor chose to implement it because the original 802.11 protocol did not specify how this value is derived. The second weakness concerns on RC4's Integrity Check Value (ICV), a CRC-32 checksum that is used to verify whether the contents of a frame have been modified in transit. At the time of encryption, this value is added to the end of the frame. As the recipient decrypts the packet, the checksum is used to validate the data. Because the ICV is not encrypted, however, it is theoretically possible to change the data payload as long as you can derive the appropriate bits to change in the ICV as well. This means data can be tampered and falsified.

VI. SOLUTIONS FOR SECURING WLAN

Despite the risks and vulnerabilities associated with wireless networking, there are certain circumstances that demand their usage. Even with the WEP flaws, it is still possible for users to secure their WLAN to an acceptable level. This could be done by implementing the following actions to minimize attacks into the main networks.

Changing Default SSID: Service Set Identifier (SSID) is a unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to a particular WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. In fact, it is the only security mechanism that the access point requires to enable association in the absence of activating optional security features. Not changing the default SSID is one of the most common security mistakes made by WLAN administrators. This is equivalent to leaving a default password in place.

Utilize VPN: A VPN is a comprehensive solution in a way that it authenticates users coming from an untrusted space and encrypts their communication so that someone listening cannot intercept it. Wireless AP is placed behind the corporate firewall within a typical wireless implementation. This type of implementation

opens up a big hole within the trusted network space. A secure method of implementing a wireless AP is to place it behind a VPN server. This type of implementation provides high security for the wireless network implementation without adding significant overhead to the users. If there is more than one wireless AP in the organization, it is recommended to run them all into a common switch, then connecting the VPN server to the same switch. Then, the desktop users will not need to have multiple VPN dial-up connections configured on their desktops. They will always be authenticating to the same VPN server no matter which wireless AP they have associated with.

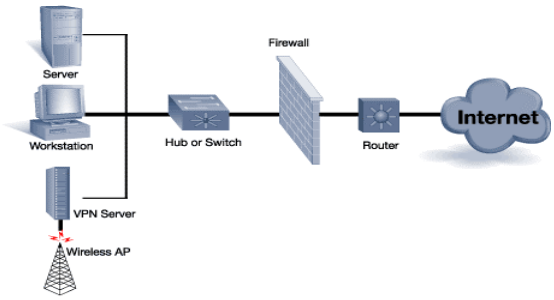

Figure 5: Securing a wireless AP

Utilize Static IP: By default, most wireless LANs utilize DHCP (Dynamic Host Configuration Protocol) to more efficiently assign IP addresses automatically to user devices. A problem is that DHCP does not differentiate a legitimate user from a hacker. With a proper SSID, anyone implementing DHCP will obtain an IP address automatically and become a genuine node on the network. By disabling DHCP and assigning static IP addresses to all wireless users, you can minimize the possibility of the hacker obtaining a valid IP address. This limits their ability to access network services. On the other hand, someone can use an 802.11 packet analyzer to sniff the exchange of frames over the network and learn what IP addresses are in use. This helps the intruder in guessing what IP address to use that falls within the range of ones in use. Thus, the use of static IP addresses is not fool proof, but at least it is a deterrent. Also keep in mind that the use of static IP addresses in larger networks is very cumbersome, which may prompt network managers to use DHCP to avoid support issues.

Access Point Placement: WLAN access points should be placed outside the firewall to protect intruders from accessing corporate network resources. Firewall can be configured to enable access only by legitimate users based on MAC and IP addresses. However, this is by no means a final or perfect solution because MAC and IP addresses can be spoofed even though this makes it difficult for a hacker to mimic.

Minimize radio wave propagation in non-user areas: Try orienting antennas to avoid covering areas outside the physically controlled boundaries of the facility. By steering clear of public areas, such as parking lots, lobbies, and adjacent offices, the ability for an intruder to participate on the wireless LAN can be significantly reduced. This will also minimize the impact of someone disabling the wireless LAN with jamming techniques.

VII. NEW STANDARDS FOR IMPROVING WLAN SECURITY

Apart from all of the actions in minimizing attacks to WLAN mentioned in the previous section, we will also look at some new standards that intend to improve the security of WLAN. There are two important standards that will be discussed in this paper: 802.1x and 802.11i.

802.1x: One of the standards is 802.1x which was originally designed for wired Ethernet networks. This standard is also part of the 802.11i standard that will be discussed later. The following discussion of 802.1x is divided into three parts, starting with the concept of Point-to-Point Protocol (PPP), followed by Extensible Authentication Protocol (EAP), and continues with the understanding of 802.1x itself.

PPP: The Point-to-Point Protocol (PPP) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, error detection, and option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation. By any measure, PPP is a good protocol. However, as PPP usage grew, people quickly found its limitation in terms of security. Most corporate networks want to do more than simple usernames and passwords for secure access [13]. This leads to the designation of a new authentication protocol, called Extensible Authentication Protocol (EAP).

Extensible Authentication Protocol: The Extensible Authentication Protocol (EAP) is a general authentication protocol defined in IETF (Internet Engineering Task Force) standards. It was originally developed for use with PPP. It is an authentication

protocol that provides a generalized framework for several authentication mechanisms. These include Kerberos, public key, smart cards and one-time passwords. With a standardized EAP, interoperability and compatibility across authentication methods become simpler. For example, when user dials a remote access server (RAS) and use EAP as part of the PPP connection, the RAS does not need to know any of the details about the authentication system. Only the user and the authentication server have to be coordinated. By supporting EAP authentication, RAS server does not actively participate in the authentication dialog. Instead, RAS just re-packages EAP packets to hand off to a RADIUS server to make the actual authentication decision.

How does EAP relate to 802.1x?

802.1x: IEEE 802.1x relates to EAP in a way that it is a standard for carrying EAP over a wired LAN or WLAN. There are four important entities that explain this standard.

Authenticator

Authenticator is the entity that requires the entity on the other end of the link to be authenticated. An example is wireless access points.

Supplicant

Supplicant is the entity being authenticated by the Authenticator and desiring access to the services of the Authenticator.

Port Access Entity (PAE)

It is the protocol entity associated with a port. It may support the functionality of Authenticator, Supplicant or both.

Authentication Server

Authentication server is an entity that provides authentication service to the Authenticator. It maybe co-located with Authenticator, but it is most likely an external server. It is typically a RADIUS (Remote Access Dial In User Service) server.

The supplicant and authentication server are the major parts of 802.1x.

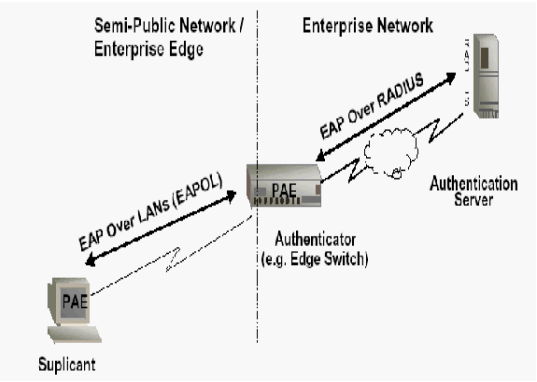

Figure 6: General topology of 802.1x components.

EAP messages are encapsulated in Ethernet LAN packets (EAPOL) to allow communications between the supplicant and the authenticator. The following are the most common modes of operation in EAPOL.

i) The authenticator sends an "EAP-Request/Identity" packet to the supplicant as soon as it detects that the link is active.

ii) The supplicant sends an "EAP-Response/Identity" packet to the authenticator, which is then passed to the authentication (RADIUS) server.

iii) Next, the authentication server sends back a challenge to the authenticator, with a token password system. The authenticator unpacks this from IP and repackages it into EAPOL and sends it to the supplicant. Different authentication methods will vary this message and the total number of messages. EAP supports client-only authentication and strong mutual authentication. Only strong mutual authentication is considered appropriate for the wireless case.

iv)The supplicant responds to the challenge via the authenticator and passes the response onto the authentication server. If the supplicant provides proper identity, the authentication server responds with a success message, which is then passed to the supplicant. The authenticator now allows access to the LAN, which possibly was restricted based on attributes that came back from the authentication server.

802.11i: In addition to 802.1x standard created by IEEE, one up-and-coming 802.11x specification, which is 802.11i, provides replacement technology for WEP security. 802.11i is still in the development and approval processes. In this paper, the key technical elements that have been defined by the specification will be discussed. While these elements might change, the information provided will provide insight into some of the changes that 802.11i promises to deliver to enhance the security features provided in a WLAN system.

The 802.11i specification consists of three main pieces organized into two layers. On the upper layer is the 802.1x, which has been discussed in the previous section. As used in 802.11i, 802.1x provides a framework for robust user authentication and encryption key distribution. On the lower layer are improved encryption algorithms. The encryption algorithms are in the form of the TKIP (Temporal Key Integrity Protocol) and the CCMP (counter mode with CBC-MAC protocol). It is important to understand

how all of these three pieces work to form the security mechanisms of 802.11i standard. Since the concept of 802.1x has been discussed in the previous section, the following section of this paper will only look at TKIP and CCMP. Both of these encryption protocols provide enhanced data integrity over WEP, with TKIP being targeted at legacy equipment, while CCMP is being targeted at future WLAN equipments. However, a true 802.11i system uses either the TKIP or CCMP protocol for all equipments.

TKIP: The temporal key integrity protocol (TKIP) which initially referred to as WEP2, was designed to address all the known attacks and deficiencies in the WEP algorithm. According to 802.11 Planet [6], the TKIP security process begins with a 128-bit temporal-key, which is shared among clients and access points. TKIP combines the temporal key with the client machine's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. Similar to WEP, TKIP also uses RC4 to perform the encryption. However, TKIP changes temporal keys every 10,000 packets. This difference provides a dynamic distribution method that significantly enhances the security of the network. TKIP is seen as a method that can quickly overcome the weaknesses in WEP security, especially the reuse of encryption keys. The following are four new algorithms and their function that TKIP adds to WEP.

i) A cryptographic *message integrity code*, or MIC, called Michael to defeat forgeries.
ii) A new IV *sequencing discipline*, to remove replay attacks from the attacker's arsenal.
iii) A per-packet *key mixing function*, to de-correlate the public IVs from weak keys.
iv) A *re-keying* mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

CCMP: As explained previously, TKIP was designed to address deficiencies in WEP; however, TKIP is not viewed as a long-term solution for WLAN security. In addition to TKIP encryption, the 802.11i draft defines a new encryption method based on the advanced encryption standard (AES). The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. It is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [3]. More robust than TKIP, the AES algorithm would replace WEP and RC4. AES based encryption can be used in many different modes or algorithms. The mode that has been chosen for 802.11 is the counter mode with CBCMAC protocol (CCMP). The counter mode delivers data privacy while the CBC-MAC delivers data integrity and authentication. Unlike TKIP, CCMP is mandatory for anyone implementing 802.11i.

VIII. TOOLS FOR PROTECTING WLAN

There are some products that can minimize the security threats of WLAN such as:

Air Defense: It is a commercial wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a WLAN from intruders and attacks, and assists in the management of a WLAN. Air Defense also has the capability to discover vulnerabilities and threats in a WLAN such as rogue APs and ad hoc networks. Apart from securing a WLAN from all the threats, it also provides a robust WLAN management functionality that allows users to understand their network, monitor network performance and enforce network policies.

Isomair Wireless Sentry: This product from Isomair Ltd. automatically monitors the air space of the enterprise continuously using unique and sophisticated analysis technology to identify insecure access points, security threats and wireless network problems. This is a dedicated appliance employing an Intelligent Conveyor Engine (ICE) to passively monitor wireless networks for threats and inform the security managers when these occur. It is a completely automated system, centrally managed, and will integrate seamlessly with existing security infrastructure. No additional man-time is required to operate the system.

Wireless Security Auditor (WSA): It is an IBM research prototype of an 802.11 wireless LAN security auditor, running on Linux on an iPAQ PDA (Personal Digital Assistant). WSA helps network administrators to close any vulnerabilities by automatically audits a wireless network for proper security configuration. While there are other 802.11 network analyzers such as Ethereal, Sniffer and Wlandump, WSA aims at protocol experts who want to capture wireless packets for detailed analysis. Moreover, it is intended for the more general audience of network installers and administrators, who want a way to easily and quickly verify the security configuration of their networks, without having to understand any of the details of the 802.11 protocols.

IX. CONCLUSION

The general idea of WLAN was basically to provide a wireless network infrastructure comparable to the wired Ethernet networks in use. It has since evolved

and is still currently evolving very rapidly towards offering fast connection capabilities within larger areas. However, this extension of physical boundaries provides expanded access to both authorized and unauthorized users that make it inherently less secure than wired networks. WLAN vulnerabilities are mainly caused by WEP as its security protocol. However, these problems can be solved with the new standards, such as 802.11i, which is planned to be released later this year. For the time being, WLAN users can protect their networks by practicing the suggested actions that are mentioned in this paper based on the cost and the level of security that they wish. However, there will be no complete fix for the existing vulnerabilities. All in all, the very best way to secure WLAN is to have the security knowledge, proper implementation, and continued maintenance.

REFERENCES

1. Cisco website www.cisco.com
2. Dlink website www.dlink-india.com
3. 3com website www.3com.com
4.http:\www.proxim.com\learn\library\whitepapers\ wp2001-06-what.html
5.http://www.clearlake.ibm.com/wireless/lan_design.html
6.http://iwsun4.infoworld.com/articles/tc/xml/01/03/26/010326tcwireless.xml
7. www.wlana.com
8. http://www.cit.cornell.edu/oit/wireless.html.