Wireless LANs – Convenience or Security

Dhaval Doshi
Department of Computer Science & Engineering
The University of Texas at Arlington.
doshi@cse.uta.edu

ABSTRACT

Wireless LANs have revolutionized the way in whic h people communicate and share information. The market for wireless applications and hardware is growing at a phenomenal rate. With wireless networks proliferating rapidly, security of these networks becomes a major concern. Networks using the IEEE 802.11b standard have been proven inherently insecure. Hence, there exists the need for a fool -proof mechanism to secure WLANs from hacking, sniffing and other forms of unauthorized access. The goal of this paper is to analyze the various security policies presen tly in force and provide a platform for the development of a more robust and secure architecture .

1. INTRODUCTION

Wireless LANs (WLAN) are being deployed at a remarkable pace. Considered to be an expensive technology until recent past, one can find them not only in the corporate world but also at airports, hotels, shopping malls and libraries to name a few. Marketing trends estimate that by the end of 2006, 21 million homes will have implemented a Local Area Network (LAN), and of those 21 million homes 65% will use wireless solutions. [1] The mention of wireless LAN not only involves the mobile users connected to the network by means of their wireless network cards but also includes the wired community as they are connected to the network at some point of time for the purpose of application or resource sharing. Hence the security of both these forms must co-exist in order to achieve the desired security level. Wireless networking brings a whole new meaning to networking security risk analysis and mitigation.

Low cost, platform independence and convenience coupled with ease of operation have made these networks appealing to the masses. The IEEE standard 802.11 is considered to be the backbone of most wireless networks in use today. It's major attraction being the ability to provide a public wireless gateway to the Internet. Its versatility has also made it

an ideal target for hackers. As with most new technologies that gain market acceptance, the deployment phase is usually followed by the discovery of security flaws and subsequent tweaking. The standard defines protocols for two forms of the network: Adhoc networks and Infrastructure networks. An adhoc network is a simple network where communications are established between multiple stations in a given coverage area without the use of an access point or base station. The infrastructure mode uses an access point that controls the allocation of transmit time for all stations/clients and allows clients to roam from cell to cell. The access point is used to handle the traffic from the mobile system to the backbone of the network.

In recent years several technologies have been derived from the 802.11 namely 802.11a, 802.11b and 802.11g. The Table below shows a comparison of these:

802.11b	**802.11a**		**802.11g**
Maximum Data Rate	11 Mbps	54 Mbps	54 Mbps
Maximum TCP Throughput	5.9 Mbps	24.4 Mbps	24.4 Mbps
Indoor Range	~300 feet	~300 feet	~300 feet
Non-Overlapping Channels (US)	3	12	3
Access Point Density (Aggregate BW)	Lower	Higher	Lower
Noise / Interference	Higher	Lower	Higher
Power Consumption	Higher	Lower	Lower
Interoperability Testing/Certification	2000	2002	2003

Table 1: Comparing 802.11 Standards [6]

All computer systems face security threats that can compromise system performance and the data stored or transmitted between the systems. Unauthorized network access risks and eavesdropping risks can become an issue because anyone with a wireless data interface can gain access to the network. Unlike a wired network where a user must have physical access to a network outlet in order to gain access, access to the wireless cell is available anywhere within the operating radius of the wireless base station.

A problem client is another issue related to WLANs. A problem client is a user connected to the network whose activities hamper the normal operation of the wireless cell. Consider the case wherein a client on the network sends or receives large chunks of data thereby preventing other users from carrying out their work. This could occur intentionally by a user or unintentionally, by a virus-infected computer. It becomes difficult to identify the location of the user or for that matter disable his activities in a wireless environment.

The majority of the commercial providers provide security and authentication, using the "captive portal." As soon as a new user connects to the WLAN, a router behind the access point, using MAC filtering captures all packets from the users machine and sends them to a particular server; regardless of the destination. The user cannot have access to the Internet, until he or she opens the web browser. The first http request from the browser reaches the designated server and the user sees a web page prompting him/her for a username and password. After the user provides the required authentication information, the MAC filter is disabled and all the traffic from the users' computer is allowed to flow normally. This mechanism has some serious deficiencies. First, if the captive portal does not use SSL to get the authentication information, passwords or credit card numbers can be stolen. Second, after the authentication is completed the MAC address of the authenticated user can be stolen and be spoofed to gain unauthorized entry (MAC addresses are software updateable). This paves the way for the launch of a possible hacking attack.

2. AUTHENTICATION METHODS

2.1 Authentication

Authentication is used to regulate access and control who can use the wireless network. Currently, there is a range of techniques that can be used and each has its advantages and disadvantages. The stronger the authentication, the higher the overhead in terms of hardware, software, and effort to roll out and maintain the security solution. The most common authentication methods for wireless LANs include:

- No Authentication
- Mac Address Filtering
- Shared WEP Key
- Pre-Shared Key
- 802.1X
- VPN Authentication

Some of these authentication methods can be combined together to create stronger security solutions. MAC Address Filtering is a separate authentication layer that can be applied to any of the other authentication methods. For users desiring stronger authentication, 802.1X with a secure EAP type may be the best choice. This can be combined with MAC Address Filtering in really high security deployments.

2.2 Data Encryption Methods

After selecting the desired Authentication method, a suitable encryption scheme needs to be selected to protect data packets traveling over the open airwaves. Some of these encryptions schemes can only be used with specific authentication methods.

Each of the authentication methods can be combined with a data encryption method to secure the wireless LAN. The most common data encryption schemes available for wireless include:

- No Encryption
- Static WEP
- Dynamic WEP
- Wi-Fi Protected Access
- VPN Encryption

For enterprise-class wireless security, the minimum security standard that should be considered is Dynamic WEP. Dynamic WEP uses 802.1X to provide strong authentication and dynamically generates a unique WEP key for every user on the wireless LAN. Every time the user signs onto the wireless LAN, a new unique WEP key is created and assigned to the user's wireless client.

Static WEP's vulnerabilities are well publicized and there are many tools freely available to break into wireless LANs using this encryption method. Hence static WEP should only be considered for wireless LANs that require low security – such as guest networks.

Authentication Method	Encryption Method	EAP Needed?	RADIUS Needed?	Description and Comments
None	None	No	No	Layer 2 network with no security. Can be used for free access hot spots, guest networks, or as 3rd party VPN security solution.
Shared Key	Static WEP	No	No	Selected for ease of implementation over data security and authentication complexity. Ideal for guest networks and low security networks.
802.1X	WEP	Yes	Yes	Strong user authentication. Unique encryption keys generated randomly for each user per session. More overheads and greater security.
Pre-Shared Key	WPA	No	No	Strong data encryption provided through WPA using TKIP. Authentication is simplified through the use of pre-shared keys. Generally used in smaller wireless deployments.

802.1X	WPA	Yes	Yes	Strong data encryption provided through WPA using TKIP. Good for enterprise wireless LANs that require strong authentication and strong data encryption.
MAC Address Filtering	Optional	Optional	Optional	Can be applied to any of the security combinations mentioned above. Adds an additional layer of security but also adds maintenance complexity as lists of client MAC addresses. Hackers can bypass filtering with the knowledge of MAC Spoofing. Generally used with lower security schemes to provide a little extra security.

Table 2: Common Security Schemes [6]

Without stringent security procedures and policies in place, installing a WLAN can be equivalent to placing Ethernet access ports outside the office letting anyone and everyone plug into one's network. Hence a synthesis of the desired security paradigms has to be deployed in order to provide a secure atmosphere.

One of the goals of the current WLAN standard was to provide security and privacy that was "wired equivalent," and to meet this goal the designers implemented several security mechanisms to provide for confidentiality, authentication, and access control.

Access Control

There are two major forms of access control: access control lists, and a "closed network" mechanism. An ACL is essentially a lookup table based on the identity that indicates what resources the specific identity is permitted to use. Thus, the MAC ACL lists the MAC addresses with permission to use the network. If the MAC address does not appear in the list, then the station is not permitted to use the network. Since the MAC address can be changed at will, an attacker need only sniff the wireless network to identify those MAC addresses that are permitted access. The attacker changes their card to the same address once an authorized MAC address is identified—now the attacker's traffic will be permitted by the ACL of the access point. The second form of widely used access control is the "closed network" approach. In this case, the user must present a secret to the access point to gain access—generally a reasonable method of access control—provided the secret remains so. Unfortunately in the closed network approach, this is not the case. The string used as the shared secret is actually the network name, and this name is broadcast

in the clear in several management frames during the course of normal WLAN operation. As a result, once again the attacker need only “sniff” the network to gain enough information to use the network resources.

Authentication

The current WLAN standard includes two forms of authentication: open system and shared key. The open system authentication is a null authentication process where the station, or client, always successfully authenticates everyone associated with an access point. The second authentication method utilizes a shared key with a challenge and a response. The station requests authentication using a shared key and the access point responds with a 128-byte randomly generated challenge. This value is sent back to the requesting station. Upon receiving the challenge, the station encrypts it using the shared key and the RC4 encryption algorithm, returning it to the access point. The access point decrypts, using RC4 and the shared key, and then checks to see if the decrypted value matches the random value sent in the second message. If it does, the station is authenticated; otherwise, authentication fails. The problem is that an attacker eavesdropping on this process can collect both the plaintext (the random challenge) and the corresponding ciphertext (the encrypted response).

In spite of these problems careful following of certain steps does ensure network safety. Care must be taken to ensure the WLAN does not offer a way to bypass enterprise firewalls. If WLANs are treated the same as wired LANs, then stations are inside the firewall. In this way, WLAN stations are treated like any other Internet host. Adversaries may use the free bandwidth to launch attacks on other enterprises. This can be thwarted by employing a firewall with more than two ports. One port connects to the enterprise network, a second port connects to the Internet, and additional ports connect to WLANs. In this way, the firewall policy will determine which WLAN stations can access the Internet as well as the enterprise network.

The cryptographic security in the IEEE 802.11 standard is flawed. The standard is addressing these concerns, and while waiting for the standards committee to complete their work.

3. WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP), as the name implies, was meant to provide the same level of security as a wired network. It is an encryption provision applied for protecting wireless communication from unauthorized access using encryption. There are free tools available that exploit those vulnerabilities, enabling even novice hackers to be able to break the WEP key. One can not only monitor the network traffic but also gain entry into the area of operation without any strong authentication mechanism.

The vulnerabilities of WEP are discussed here. The sender generates a 24-bit Initialization Vector (IV) and appends this to the shared key (either 40-bit or 104-bit) to come up with a unique key for each packet. It then calculates the Cyclic Redundancy Checksum (CRC) of the data to be transmitted and appends it to the data. The 64-bit or 128-bit "unique" key is then sent through a RC4 Pseudo Random Number Generator (PRNG). The generated key stream (64-bit or 128-bit) is then XORed with the plaintext data and CRC to create the cipher text. After setting a bit in the header to indicate that it is WEP encrypted and inserting the IV into an appropriate field of the header, the frame with the cipher text is sent to the receiver. The weakness of WEP arises from the usage of IV and the RC4 stream cipher. The IV is 24 bits long and after 224 keys, the IV starts repeating. Now, since a stream cipher (RC4 in this case) can never be reused, it implies that the shared key needs to be changed to prevent hackers from determining the key. Since it is not practical that the shared key will be replaced as soon as 224 packets have been transmitted (which could be in every couple of hours), so we end up having duplicate keys and hence are susceptible to attacks [9].

WEP has several serious inherent problems. It does not meet its fundamental goals of wired-equivalent confidentiality. The use of WEP is optional, and as a result, many real installations never even turn on encryption. By default, WEP uses a single shared key common to all users of a WLAN, and this common key is often stored in software-accessible storage on each device. If any device is lost, stolen, or compromised, the only recourse is to change the shared secret in all of the remaining devices. Since WEP does

not include a key management protocol, distributing the new secret to all users is an unwieldy process. As a result, key compromises are often ignored.

The most serious problem with WEP is that its encryption keys can be recovered through cryptanalysis. WEP uses a common stream cipher, RC4, in a nonstandard way: Experiments in the field indicate that, with proper equipment, it is practical to eavesdrop on WEP-protected networks from distances of a mile or more from the target. Once the WEP key is discovered, all security is lost. The security risks are:

- An attacker can decrypt intercepted packets and read encrypted traffic.
- An attacker can forge new encrypted packets that will be accepted by the access point, and join the wireless network, or attack other hosts, defeating the WEP integrity and authentication goals.
- Integrity protection for source and destination addresses is not provided.

TKIP: IEEE 802.11i Short-Term Solution

To address the WEP vulnerabilities on this hardware, TGi has defined the Temporal Key Integrity Protocol, or TKIP. TKIP is intended to serve as an interim solution. The requirement to run on deployed hardware imposes several constraints:

- Allow deployed systems to be software or firmware upgradeable;
- Allow the current WEP hardware implementation to remain unchanged; and
- Minimize performance degradation imposed by the fixes.

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:

- A message integrity code (MIC), called Michael, to defeat forgeries;
- A packet sequencing discipline, to defeat replay attacks; and
- A per-packet key mixing function, to prevent FMS attacks.

CCMP: IEEE 802.11i Long-Term Solution

- CCMP stands for the Counter-Mode-CBC-MACProtocol. Like TKIP, the long-term solution addresses all known WEP deficiencies, but without the shackles of already-deployed hardware.

The CCMP Protocol

As with TKIP, CCMP employs a 48-bit IV, ensuring the lifetime of the AES key is longer than any possible association. In this way, key management can be confined to the

beginning of an association and ignored for its lifetime. CCMP uses the same AES key to provide confidentiality and integrity protection for all of the packets in an association. Since CCMP provides both services, it is straightforward to provide confidentiality and integrity protection over the same data structure. CCMP must, however, protect nearly the entire packet header to defend against fragmentation attacks. Thus CCMP helps in reduced key management overhead and minimizes the time spent computing AES key schedules. It supports pipelining to increase the throughput.

The problems associated with WEP have been reviewed and new protocols proposed. To summarize, WEP meets none of its security goals because of misuse of cryptographic primitives. The new protocols, TKIP and CCMP, address all known WEP problems. As they are deployed, it is expected the new protocols will finally cause the struggle between hacker and defender to shift to layers above the wireless MAC.

4. ACCESS POINTS

The authentication between the client and access point is only one way – the access point authenticates the client but the IEEE 802.11 standard doesn't provide for authenticating an access point. This is a serious limitation and has been made use of by hackers. If you can set up an access point outside an office building so that the signal from it is strong enough within the building, then legitimate clients can mistakenly connect to your access point in the parking lot, instead of the authenticated access points. This will enable the parking lot hacker to have access to all the data that the client computers are transmitting, some of which could be corporate secrets. The majority of installations use the default setting, i.e no WEP key enabled. This makes the task a lot easier for "backdoor" entry into the network bypassing all firewalls and other security provisions deployed.

5. LOCATION AWARENESS

This problem of finding a *rogue machine* on a wireless network is a special case of the general wireless localization problem. A wide variety of techniques have been designed to accomplish this, both using custom hardware devices, such as sonar or infrared sensors, and using the limited signal-strength measurements that can be performed by existing WLAN cards. Such a location sensing system has the potential to trump the

inherent stealth advantage that intruders on wireless networks currently enjoy. However, a rogue machine may desire *not* to be found. The localizing agents do not know what WLAN hardware the rogue machine is using, and they do not know the power level at which the rogue machine is broadcasting. To track such a target, a location sensing system must be complacent to identify the differences among mobile device configurations and also overcome any interference by the intruder.

Location-aware computing deals with two principal tasks: determining and tracking the position of a mobile device, and providing useful user functionality based on localization primitive. WLAN location sensing can determine the position of any laptop, PDA, or other device with WLAN hardware. Systems use the signal strength readings from WLAN cards as a sensor and implement the Markov localization algorithm commonly used in various robotics applications. Following this technique, conditional probability distributions are built correlating sensor readings to position space by sampling these sensor readings at known positions in the building. This off-line phase is referred to as *training* or *learning*. During the on-line phase, measurements are integrated and a probability distribution is built over position space. A maximum likelihood estimate is then used to determine the accurate position.

6. HOTSPOTS

In recent times, wireless Internet service providers (WISPs) have established Wi-Fi hotspots in increasing numbers at public venues, providing local coverage to traveling users and empowering them with the ability to access email, Web, and other Internet applications on the move. It is observed that while the mobile computing landscape has changed both in terms of number and type of hotspot venues, there are several technological and deployment challenges remaining before hotspots can become a ubiquitous infrastructure. These challenges include authentication, security, coverage, management, location services, billing, and interoperability.

Can a mobile user open his laptop anywhere he roams and find hotspot coverage? How easy is it to configure the connection parameters? Is there a common way for him to authenticate herself to each hotspot service provider? What is the payment model for the connection? What does he do when he goes out of range of a hotspot while roaming? All

these questions remain partially answered. Although next-generation cellular data services will undoubtedly play a role in providing long-range, wide-area coverage, these networks require expensive licenses and have a high installation cost.

Authentication

Hotspots provide access to unknown users, who might not have visited the network before. This necessitates the use of a formal authentication mechanism that enables users to identify themselves to the network. Authentication helps the network to establish the users' identity. Today, since each hotspot is likely administered by a different provider, users will have to repeatedly authenticate themselves at each hotspot location. And since each hotspot is configured differently for access, either through a Web-based user interface or through proprietary client software requiring installation and configuration, hotspot users need to get used to the various provider specific modes of authentication. The goal of providing fast and seamless service, while simultaneously ensuring user accountability, involves a trade-off between ease of use and robustness.

• Third-Party Authenticators: How can global databases be used to establish user identity? How can multiple authentication domains be integrated into the infrastructure? One approach is to use trusted third-party authentication databases that allow hotspot providers to offer users with end-to-end security [2].

Wireless hop Security

A second, related challenge to the authentication problem is wireless hop security. Users who do not trust the hotspot infrastructure can use higher layer security mechanisms such as SSH, SSL, or VPNs to connect to a private network. For these users, the availability of wireless hop security would not be a major concern. First, the average user is not very familiar with these higher-layer security mechanisms. Second, since user authentication is done before procuring a secure tunnel or a VPN connection, sensitive information such as username, password, keys, etc., need to be exchanged securely with the authenticating entity. Current approaches achieve network security through per-user authentication, authorization of authenticated users through access keys, and access control of all user traffic through per-packet verification [2].

Security Challenges

Despite the aforementioned research certain challenges exist before the hotspot operators.

• Mutual Trust: How can wireless-hop security be provided in a way to ensure mutual trust between the user and the hotspot provider?

• Simplicity-Robustness Tradeoffs: Can hotspot networks employ WEP-based security by choosing from a set of *guestaccess* . How can WEP keys be distributed transparently and scalably under such circumstances?

• Dynamic Key Management.

• Hardware Approaches: Do smartcards provide the appropriate tradeoff between security and convenience?

• Denial-of-Service Attacks.

7. VIRTUAL PRIVATE NETWORK (VPN)

Virtual Private Networks (VPNs) offer a solid solution to many security issues, where an authenticated key provides confidentiality and integrity for IP datagrams. WLAN stations are treated similarly to dialup stations. First the user is authenticated, and the key is established. Then, the key is used to encrypt and integrity protect the IP datagrams. Deployment of VPNs is not always easy. While the software is getting better with each release, authentication depends on at least one of three factors: something you know (such as a password); something you have (such as a security token); something you are (such as your fingerprint). Using more than one factor is desirable, and using all three is the most secure. However, each factor comes with some administrative burden.

A VPN is a very attractive method for remote access since the VPN user will be presented with a desktop interface almost identical to the one they are accustom when they are in the office. A VPN:

- Requires special client software
- Requires special configuration settings
- Provides a point-to-point secured tunnel
- Requires a username/password
- Requires specific network addressing

However, in a hot spot wireless environment, a VPN connection can be a security risk. A VPN is a network-to-network connection. The main problem with using a VPN in a public wireless hot spot connection is that everyone accessing the hot spot is sharing the

same network segment. It is very easy for a hacker, using readily available tools, to scan all of the connected PCs to determine who has and hasn't applied the latest security patches.

Network security is made up of equal parts of preventative technologies, security policies, employee education and human nature anticipation. It is the latter element that dictates this VPN prohibition. One of the most proven network security strategies is to insulate a corporate network by providing access to resources at the application layer using a variety of protocols rather than at the network layer. In order to give complete Web access to corporate systems, however, there is an increased necessity for stronger authentication.

Network layer security will remain important to the wireless user in an untrusted wireless network, but is most effective when used in combination with link layer security. Standalone network layer security solutions, such as VPNs, are not sufficient for securing wireless networks. Link layer security used in conjunction with improved network layer encryption is likely to meet the security needs of most organizations.

8. INTEROPERATION WITH WAN DATA SERVICES

Today's network wireless user has several different options of network access, through both wired and wireless means. The wide-area cellular access technologies complement Wi-Fi connectivity for a typical mobile user such as GPRS over GSM, CDMA data services, etc., and potential challenges in integrating Wi-Fi services seamlessly with these technologies.

Interoperation between cellular and hotspot networks is beneficial to both wireless carriers and hotspot operators. Since cellular networks have better coverage, they can support the connectivity needs of users that are out of range of hotspots. On the other hand, when cellular users enter a building, they can avail of high-bandwidth Wi-Fi connectivity indoors, and reduce the load on the cellular network. There are different ways in which interoperability can be provided to the user. An obvious way to achieve it is to include hardware support for both cellular data services (e.g., GPRS, CDMA, etc.) and Wi-Fi on mobile devices to migrate the connection across access technologies. In addition to the hardware, these devices need the software ability, through sensing, to

switch to the most resource-efficient mode of access, where the resource could be network bandwidth, power, device form factor, price, etc. A second way to achieve interoperability is to migrate connections across devices and across access technologies. A second infrastructure related challenge to achieving interoperability is the establishment of roaming relationships and agreements between network operators of these various access networks. There are industry efforts underway to achieve this goal. From a research standpoint, however, some issues need to be explored:

• Handoff Mechanism: When a user on a cellular network enters into a Wi-Fi coverage area, how can connectivity be seamlessly handed off from the cellular network to theWi-Fi network? Can user location be used to determine when the handoff might occur? By combining this cellular location with a Wi-Fi coverage zone map, the network would have the capability to trigger a cellular-to-Wi-Fi services hand-off based on location when a user enters into a Wi-Fi zone.

• System Support for Handoff: Is handoff initiated at the user device or by the network? What support does it need from the network for handoff to occur smoothly and quickly? Can handoff latency be reduced so as to not affect the performance of real-time applications? What support does a network-initiated handoff need at the user device?

• Billing: Which access network receives the revenue for the user's access? How can potential conflicts be resolved? If both networks get a share of the revenue and billing information is transferred between them, how can this be done securely?

9. WHAT THE FUTURE HOLDS - 802.11I TASK GROUP

The 802.11i task group is responsible for enhancing the security and authentication mechanism for 802.11. The group is working on 802.1x, an IEEE standard that provides an authentication framework for 802 based LANs. 802.1x is not tied to any networking protocol but acts as a basis for defining a means of authenticating the clients. 802.1x provides user based authentication and centralized key management and distribution. The user authentication is provided by Extensible Authentication Protocol (EAP).

There are three entities involved in a 802.1x network architecture. The first is a client seeking permission to the wireless network and is also known as the supplicant. The second is the access point (also known as the authenticator in 802.1x standard). The last

is the centralized authentication server (mostly RADIUS server). The supplicant seeks to use some service offered through a port on the authenticator. The permission request is forwarded to the authentication server and based on its response, the authenticator either grants or denies access to the port/service. 802.1x still suffers from the fact that it provides only one-way authentication. The client is authenticated to the access point but the client doesn't authenticate the access point. This loophole (lack of mutual authentication) can be used to perform man-in-the-middle attacks if the higher layer protocol also performs a one way authentication.

To provide a secure means of transporting authentication data, the task group is looking at two IETF drafts – Tunneled Transport Layer Security (TTLS) and Protected Extensible Authentication Protocol (PEAP). Both of them provide a secure transport medium by using a tunnel between the client and the authentication server. The standard will allow to set up an end-to-end tunnel without the need of having certificates.

Wi-Fi Protected Access (WPA) – Interim WEP Replacement

WPA is designed specifically for wireless networks, and provides users with data protection while allowing only authorized users to have access to the network. WPA not only addresses the security vulnerabilities of WEP, but also provides effective protection from both non-targeted attacks (Denial of Service attacks) and targeted attacks (Peer-to-Peer attacks). WPA is standards based and works with most other traditional security devices, which reduces dependence on vendor-specific components. It provides effective link layer security, making wireless security sufficiently strong. WPA also:

- Fixes all known WEP privacy vulnerabilities
- Dramatically improves Wi-Fi security
- Is required for Wi-Fi certification in Q3, 2003
- Has no known attack that can crack WPA
- Requires an authentication server
- Uses RADIUS protocols for authentication and key distribution
- Centralizes user credential management
- Works in home, small business, and enterprise environments

10. CONCLUSION

Wireless security can be achieved by implementing proper policies and procedures coupled with the right authentication and control mechanisms. The wireless LAN challenges need to be addressed with proper precaution. Network designs will continue to be affected by the development of new technologies and user demands.

As a countermeasure to the technology's limitations and risks, man needs to be involved to make wireless networks more secure through appropriate enforcement of policies and procedures. Hence, the combination of technology and human factor can undoubtedly alleviate the security posture of the wireless networks.

The next wave of wireless LANs is likely to be driven by mobility. 802.11 provides link-layer mobility. Users can move transparently within an IP subnet with no effect on their applications or connection – a true seamless integration of technologies.

11. REFERENCES

[1] Turner, Raymond. "Wireless Security and Monitoring for the Home Network" August 21, 2003.

[2] Anand Balachandran, Geoffrey M.Voelker, Paramvir Bahl. "Wireless Hotspots: Current Challenges and Future Directions" September 19, 2003.

[3] Austin Godber, Partha Dasgupta. "Secure Wireless Gateway" September 28, 2002.

[4] Ping Tao, Algis Rudys, Andrew M.Ladd, Dan S.Wallach. "Wireless LAN Location-Sensing for Security Applications" September 19, 2003.

[5] Nancy Cam-Winget, Russ Housley, David Wagner, Jesse Walker. "Security Flaws in 802.11 Data Link Protocols" May 2003.

[6] Lisa Phifer, Philip Kwan. "White Paper: Ironshield Best Practices Deploying Wireless LANs" September 2003.

[7] Joseph Williams. "Providing for Wireless LAN Security, Part 2".

[8] Interlink Networks. "Link Layer and Network Layer Security for Wireless Networks".

[9] Rakesh Arora. "State of Affairs of Wireless Networks" Jan 30, 2003.