Global Information Assurance Certification Paper

GIAC Security Essentials
Version 1.4b
William P. Bryceland

The Quest for Secure Wireless Networks

Introduction

This document begins with an overview of the WLAN IEEE standards and the Proposed Standards not yet implemented, and then details understanding the 802.11 framework. After that we'll take a look at some basic vulnerabilities and known risks as well as understanding WEP and the problems with WEP. With these basic concepts of wireless technology we can next begin to understand some of the industry and vendor solutions and how they will be incorporated into standards that will change the face of Wireless Security. While we are waiting for the standards to be complete and put into place private vendors are implementing their own solutions to keep the Wireless market alive and secure. The only problem with the vendors' solutions are that they may or may not be compatible with other vendor solutions and equipment.

Organizations today are deploying wireless technology at a rate faster than most IT departments can keep up with. This rapid deployment is due in part to the low cost of the devices and ease of deployment. In the past two years more than 12 million wireless LAN cards and AP's were sold.

You've heard about the problems with Wireless LANs (WLAN's), you've read about how the main security protocol (WEP) has been broken, and you've been told the best thing is to never allow WLAN's on your network. However the statistics of how fast the technology is growing and becoming mainstream IT departments cannot avoid them. Given these realities we in the field must figure out how to secure them. Because most WLAN devices ship with all security features disabled, this wide deployment attracted the attention of the hacker community. Several Web sites have now started documenting all the freely available wireless connections nationwide. Although most hackers are using these connections as a means to get free Internet access or to hide their identity, a smaller group sees this situation as an opportunity to break into networks that otherwise might have been difficult to attack from the Internet because unlike a wired network, wireless networks send data over the air and usually extend beyond the physical boundary of an organization. When strong directional antennas are used, a WLAN can reach well outside the buildings that it is designed for. Traditional physical security controls are ineffective because the packets can be viewed by anyone within radio frequency range.

IEEE WLAN Standards and Proposed Standards

802.11b

Current Wi-Fi (Wireless Fidelity) standard, A Physical Layer (PHY) standard (IEEE Std. 802.11b-1999) that specifies operating in the 2.4 GHz band using Direct Sequence Spread Spectrum (DSSS) 802.11b is rated at 11 Mbps. It specifies three available radio channels, maximum link rate of 11 Mbps per channel. 802.11b was enhanced to include 5.5 Mbps and 11 Mbps data rates in addition to the 1 Mbps and 2 Mbps data rates of the initial standard. To provide the higher data rates, 802.11b uses CCK (Complementary Code Keying) a modulation technique that makes efficient use of the radio spectrum.
Most wireless LAN installations today comply with 802.11b, which is also the basis for Wi-Fi certification from the Wireless Ethernet Compatibility Alliance (WECA). [3], [4]

DSSS is a transmission technology used a data signal at the sending station is combined with a higher data rate bit sequence, or chipping code, that divides the user data according to a spreading ratio. The chipping code is a redundant bit pattern for each bit that is transmitted, which increases the signal's resistance to interference. If one or more bits in the pattern are damaged during transmission, the original data can be recovered due to the redundancy of the transmission.

802.11a

A Physical Layer (PHY) standard (IEEE Std. 802.11a-1999) (Wi-Fi5) that specifies operating in the 5 GHz UNII band using Orthogonal Frequency Division Multiplexing (OFDM). 802.11a supports data rates ranging from 6 to 54 Mbps. It specifies eight available radio channels (available radio spectrum in some countries would permit the use of 12 channels), maximum link rate of 54-Mbps per channel. The data throughput will be greater for 11a than for 11b. A greater number of usable radio channels (eight as opposed to three) give better protection against possible interference from neighboring access points.

Because of operation in the 5 GHz bands, 802.11a offers much less potential for radio frequency (RF) interference than other PHYs (e.g., 802.11b and 802.11g) that utilize 2.4 GHz frequencies. With high data rates and relatively little interference, 802.11a does a great job of supporting multimedia applications and densely populated user environments. This makes 802.11a an excellent long-term solution for satisfying current and future requirements.
OFDM works by splitting the radio signal into multiple smaller sub-signals that are then transmitted simultaneously at different frequencies to the receiver. OFDM reduces the amount of crosstalk in signal transmissions.
There is also a follow-up to this early 802.11a technology. This technology will include the capability to support 802.11i as well as being upgradeable to 802.11h. In addition to this, 802.11a+ will be Wi-Fi5 compliant simply by having enough variety of solutions to test against. This technology will address all of the concerns of the enterprise-class organization - security, interoperability, reliability, and management. [3], [4], [5]

802.11c: Bridge operation procedures

Provides required information to ensure proper bridge operations. This project is completed, and related procedures are part of the IEEE 802.11c standard. Product developers utilize this standard when developing access points. There's really not much in this standard relevant to wireless LAN installers. [3], [4]

802.11d: Global harmonization

When 802.11 first became available, only a handful of regulatory domains (e.g., U.S., Europe, and Japan) had rules in place for the operation of 802.11 wireless LANs. In order to support a widespread adoption of 802.11, the 802.11d task group has an ongoing charter to define PHY requirements that satisfy regulatory within additional countries. This is especially important for operation in the 5 GHz bands because the use of these frequencies differ widely from one country to another. As with 802.11c, the 802.11d standard mostly applies to companies developing 802.11 products. [3], [4]

802.11e: MAC Enhancements for QoS

Without strong quality of service (QoS), the existing version of the 802.11 standard doesn't optimize the transmission of voice and video. There's currently no effective mechanism to prioritize traffic within 802.11. As a result, the 802.11e task group is currently refining the 802.11 MAC (Medium Access Layer) to improve QoS for better support of audio and video (such as MPEG-2) applications. The 802.11e group should finalize the standard by the end of 2002, with products probably available by mid-2003.

Because 802.11e falls within the MAC Layer, it will be common to all 802.11 PHYs and be backward compatible with existing 802.11 wireless LANs. As a result, the lack of 802.11e being in place today doesn't impact your decision on which PHY to use. In addition, you should be able to upgrade your existing 802.11 access points to comply with 802.11e through relatively simple firmware upgrades once they are available. [3], [4]

802.11f: Inter access point protocol

The existing 802.11 standard doesn't specify the communications between access points in order to support users roaming from one access point to another. The 802.11 WG purposely didn't define this element in order to provide flexibility in working with different distribution systems (i.e., wired backbones that interconnect access points).

The problem, however, is that access points from different vendors may not interoperate when supporting roaming. 802.11f is currently working on specifying an inter access point protocol that provides the necessary information that access points need to exchange to support the 802.11 distribution system functions (e.g., roaming). The 802.11f group expects to complete the standard by the end of 2002, with products supporting the standard by mid-2003. In the absence of 802.11f, you should utilize the same vendor for access points to ensure interoperability for roaming users. In some cases a mix of access point

vendors will still work, especially if the access points are Wi-Fi certified. The inclusion of 802.11f in access point design will eventually open up your options and add some interoperability assurance when selecting access point vendors. [3], [4]

802.11g

A Physical Layer (PHY) standard for wireless LANs in the 2.4GHz and 5GHz radio band. It specifies three available radio channels. The maximum link rate is 54-Mbps per channel - compared with 11 Mbps for 11b. 802.11g uses orthogonal frequency-division multiplexing (OFDM) modulation but, for backward compatibility with 11b, it also supports complementary code keying (CCK) modulation and, as an option for faster link rates, allows packet binary convolutional coding (PBCC) modulation. The myriad of modulation techniques could create complexity and confusion. Conflicting interests between key vendors have divided support within IEEE task group for the OFDM and PBCC modulation schemes. The task group included both types of modulation in the draft standard. With the addition of support for 11b's CCK modulation, the end result is three modulation types. This is perhaps too little, too late and too complex compared with 11a. However, there are advantages for vendors looking to supply dual-mode 2.4GHz and 5GHz products, in that using OFDM for both modes will reduce silicon cost. If 802.11h fails to obtain pan-European approval by the second half of 2003, then 11g will become the high-speed WLAN of choice in Europe. Completed standard expected in the second half of 2002. Products will be available in the first half of 2003. [3], [4], [6]

802.11h

This standard is supplementary to the MAC layer to comply with European regulations for 5GHz WLANs. European radio regulations for the 5GHz band require products to have transmission power control (TPC) and dynamic frequency selection (DFS). TPC limits the transmitted power to the minimum needed to reach the furthest user. DFS selects the radio channel at the access point to minimize interference with other systems, particularly radar. Completion of 11h will provide better acceptability within Europe for IEEE-compliant 5GHz WLAN products. A fast-dwindling group will continue to support the alternative HyperLAN standard defined by ETSI. Although European countries such as the Netherlands and the United Kingdom are likely to allow the use of 5GHz LANs with TPC and DFS well before 11h is completed, pan-European approval of 11h is not expected until the second half of 2003, possibly longer. [3], [4]

802.11i

This standard is also supplementary to the MAC layer to improve security. It will apply to 802.11 physical standards a, b and g. It provides an alternative to Wired Equivalent Privacy (WEP) with new encryption methods and authentication procedures. IEEE 802.1x forms a key part of 802.11i. Security is a major weakness of WLANs. Vendors have not improved matters by shipping products without setting default security features. In addition, the WEP algorithm weaknesses have been exposed. The 11i specification is part of a set of security features that should address and overcome these issues by the end of 2002. Solutions will start with firmware upgrades using the Temporal Key Integrity Protocol (TKIP), followed by new silicon with AES (an iterated block cipher) and TKIP backwards compatibility. New silicon with an AES cipher is expected by the second half of 2003. [3], [4]

802.1x: Framework for Authentication

Combined with an authentication protocol, such as EAP-TLS, LEAP, or EAP-TTLS, IEEE 802.1X provides port-based access control and mutual authentication between clients and access points via an authentication server. The use of digital certificates makes this process very effective. 802.1X also provides a method for distributing encryption keys dynamically to wireless LAN devices, which solves the key reuse problem found in the current version of 802.11. Microsoft supports 802.1X in Windows XP, and many vendors offer 802.1X in wireless LAN devices. 802.11i is including 802.1X in the future 802.11 standard. [11],[12]

Understanding the 802.11 Framework

The entire process for setting up a wireless connection between a station and an access point can be broken down into three phases; probe phase, authentication phase, and association Phase. Also is the station is in motion it might be necessary to perform a reassociation from time to time. [9]

Probe Phase – A station may locate an access point by active scanning. The station first sends a probe request packet out on all channels. The access points that hear this message will send a probe response packet back to the station. The response packet contains identification information, which the station uses to determine what access to address in the sequel. A second method by which a station can initialize a connection is via passive scanning. The station listens for signals that are periodically transmitted by each access point, and makes its choice based on that information. [9]

Authentication Phase – When a suitable point has been selected, the authentication phase begins. In the IEEE 802.11 standard, two kinds of authentication are defined: *Open System* and *Shared Key* Authentication. In Open System Authentication, the station sends an authentication request to the access point. The access point processes this request and determines whether or not to allow the station to proceed. Based on the type of response (success or failure) from the access point, the station will either continue or discontinue the process. Shared Key Authentication makes use of the WEP privacy mechanism.

It is assumed that the two entities share a WEP key. The station sends an authentication request to the access point. The access point generates and sends a 128 bit challenge text to the station. The station is required to encrypt this challenge and return the encrypted message to the access point. Finally, the access point tries to decrypt this packet; if it succeeds, the station may proceed with the association phase. [9]

Association Phase – If the authentication phase is completed successfully, the station proceeds to send an association request packet to the access point. The access point analyses the information in this packet, and adds the station to its association table. A station may be associated with no more than one access point at one time, but the access point of course can be associated with several stations. [9]

Reassociation – Each station is associated to a particular access point. Roaming refers to the situation where a station moves away from its old access point and towards a new access point. The station uses its scanning function to locate the new access point. At the same time, the old access point is notified by the system that it is no longer associated with the station.

The authentication mechanisms defined in the standard are not satisfactory. The Open System Authentication is in fact a null authentication. The messages are sent in the clear, so anyone could impersonate either the station or the access point. In Shared Key Authentication, the station authenticates by proving its knowledge of the WEP key. But there is no mechanism for the access point to prove its identity to the station, which opens up for malicious access points to try to participate in the communication. Authentication is only one way. Also note that only the station is authenticated not the user of the station. As you can now tell protection against an attacker with access to a wireless LAN device is not satisfactory. [9]

Wireless Vulnerabilities and Known Risks

Known Risks

Although attacks against 802.11 wireless technologies will more than likely increase in number and sophistication over time, the most current 802.11 risks fall into seven basic categories. These vulnerability classes should also be broken down into 3 different classes; Confidentiality, Integrity and availability.

Confidentiality is defined as only predefined users have read write execute and modify privileges on data. [8]

Integrity is defined as only authorized users can modify data.

Availability is defined as the data is accessible during normal business operations.

Insertion attacks

Interception and unauthorized monitoring of wireless traffic

Jamming

Client-to-Client attacks

Brute force attacks against access point passwords

Encryption attacks
Misconfiguration

Note that these classifications can apply to any wireless technology. Understanding how they work and using this information to prevent their success is a good stepping stone for any wireless solution. [8]

Insertion Attacks (Confidentiality Compromised)

Insertion attacks are based on deploying unauthorized devices or creating new wireless networks without going through security process and review.

Unauthorized Clients – An attacker tries to connect a wireless client, typically a laptop or to an access point without authorization. Access points can be configured to require a password for client access. If there is no password, an intruder can connect to the internal network simply by enabling a wireless client to communicate with the access point. Note, that some access points use the same password for all client access, requiring all users to adopt a new password every time the password needs to be changed.

Unauthorized or Renegade Access Points – An organization may not be aware that internal employees have deployed wireless capabilities on their network. This lack of awareness could lead to the previously described attack, with unauthorized clients gaining access to corporate resources through a rogue access point. Organizations need to implement policy to ensure secure configuration of access points, plus an ongoing process in which the network is scanned for the presence of unauthorized devices. [8]

Interception and Monitoring of Wireless Traffic (Confidentiality and Integrity Compromised)

As in wired networks, it is possible to intercept and monitor network traffic across a wireless LAN. The attacker needs to be within range of an access point (approximately 300 feet for 802.11b) for this attack to work, whereas a wired attacker can be anywhere where there is a functioning network connection. The advantage for a wireless interception is that a wired attack requires the placement of a monitoring agent on a compromised system. All a wireless intruder needs is access to the network data stream. There are two important considerations to keep in mind with the range of 802.11b access points.

- First, directional antennae can dramatically extend either the transmission or reception ranges of 802.11b devices. Therefore, the 300 foot maximum range attributed to 802.11b only applies to normal, as-designed installations. Enhanced equipment also enhances the risk.
- Second, access points transmit their signals in a circular pattern, which means that the 802.11b signal almost always extends beyond the physical boundaries of the work area it is intended to cover. This signal can be intercepted outside buildings, or even through floors in multistory buildings.
- Wireless Packet Analysis – A skilled attacker captures wireless traffic using techniques similar to those employed on wired networks. Many of these tools capture the first part of the connection session, where the data would typically include the username and password. An intruder can then masquerade as a

legitimate user by using this captured information to hijack the user session and issue unauthorized commands.
- Broadcast Monitoring – If an access point is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcasted out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless access point, an attacker can monitor
sensitive data going over wireless not even intended for any wireless clients.
- Access Point Clone (Evil Twin) Traffic Interception – An attacker fools legitimate wireless clients into connecting to the attacker's own network by placing an unauthorized access point with a stronger signal in close proximity to wireless clients. Users attempt to log into the substitute servers and unknowingly give away passwords and similar sensitive data. [8]

Jamming (Availability Compromised)

Denial of service attacks are also easily applied to wireless networks, where legitimate traffic cannot reach clients or the access point because illegitimate traffic overwhelms the frequencies. An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, corrupting the signal until the wireless network ceases to function. In addition, cordless phones, baby monitors and other devices that operate on the 2.4 GHz band can disrupt a wireless network using this frequency. These denials of service can originate from outside the work area serviced by the access point, or can inadvertently arrive from other 802.11b devices installed in other work areas that degrade the overall signal. [8]

Client-to-Client Attacks Confidentiality (Compromised)

Two wireless clients can talk directly to each other, bypassing the access point. Users therefore need to defend clients not just against an external threat but also against each other.
- File Sharing and Other TCP/IP Service Attacks – Wireless clients running TCP/IP services such as a Web server or file sharing are open to the same exploits and misconfigurations as any user on a wired network.
- DOS (Denial of Service) – A wireless device floods other wireless client with bogus packets, creating a denial of service attack. In addition, duplicate IP or MAC addresses, both intentional and accidental, can cause disruption on the network. [8]

Brute Force Attacks Against Access Point Passwords (Confidentiality Compromised)

Most access points use a single key or password that is shared with all connecting wireless clients. Brute force dictionary attacks attempt to compromise this key by methodically testing every possible password. The intruder gains access to the access point once the password is guessed. In addition, passwords can be compromised through less aggressive means. A compromised client can expose the access point. Not changing the keys on a

frequent basis or when employees leave the organization also opens the access point to attack. Managing a large number of access points and clients only complicates this issue, encouraging lax security practices. [8]

Attacks against Encryption (Confidentiality Compromised)
802.11b standard uses an encryption system called WEP (Wired Equivalent Privacy). WEP has known weaknesses and there are many tools that are readily available for exploiting them. [8]

Misconfiguration (Confidentiality, Availability and Integrity Compromised)
Many access points ship in an unsecured configuration in order to emphasize ease of use and rapid deployment. Unless administrators understand wireless security risks and properly configure each unit prior to deployment, these access points will remain at a high risk for attack or misuse. The following are the most widely misconfigured options;[8]
- Server Set ID (SSID) – SSID is a configurable identification that allows clients to communicate with an appropriate access point. With proper configuration, only clients with the correct SSID can communicate with access points. In effect, SSID acts as a single shared password between access points and clients. Access points come with default SSIDs. If not changed, these units are easily compromised. Here are three common default passwords:
"tsunami"
Cisco Aironet 340 series 11MBPS DSSS Wireless Lan Access Point
Cisco Aironet 340 series 11MBPS DSSS PCI Card with 128-bit encryption
"101"
3Com AirConnect 11MBPS Wireless Lan Access Point
3Com AirConnect 11MBPS Wireless PCI Card
"RoamAbout Default Network Name"
Avaya Orinoco AS-2000 Access Server (Lucent/Cabletron)
Avaya Orinoco PC Gold Card (Lucent/Cabletron)

SSIDs go over the air as clear text if WEP is disabled, allowing the SSID to be captured by monitoring the network's traffic. In addition, the Lucent access points can operate in Secure Access mode. This option requires the SSID of both client and access point to match. By default this security option is turned off. In non-secure access mode, clients can connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any".
- Wired Equivalent Privacy (WEP) – WEP can be typically configured as follows:
No encryption
40 bit encryption
64 bit encryption
128 bit encryption

All access points mentioned above have WEP turned off. Although 128 bit encryption is more effective than 40 bit encryption, both key strengths are subject to WEP's known flaws.

- SNMP Community Passwords – Many wireless access points run SNMP (Simple Network Management Protocol) agents. If the community word is not properly configured, an intruder can read and potentially write sensitive data on the access point. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well. By default, all three access points are read accessible by using the community word,
"public". 3Com access points allow write access by using the community word, "comcomcom". Cisco and Lucent/Cabletron require the write community word to be configured by the user or administrator before the agent is enabled.
- Configuration Interfaces – Each access point model has its own interface for viewing and modifying its configuration. Here are the current interface options for these three access points:
Cisco – SNMP, serial, Web, telnet
3Com – SNMP, serial, Web, telnet
Lucent / Cabletron – SNMP, serial (no web/telnet)
3Com access points lack access control to the Web interface for controlling configuration. An attacker who locates a 3Com access point Web interface can easily get the SSID from the "system properties" menu display. 3Com access points do require a password on the Web interface for write privileges. This password is the same as the community word for write privileges.
- Client Side Security Risk – Clients connected to an access point store sensitive information for authenticating and communicating to the access point. This information can be compromised if the client is not properly configured. Cisco client software stores the SSID in the Windows registry, and the WEP key in the firmware, where it is more difficult to access. Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP is stored in the Windows registry, but it is encrypted using an undocumented algorithm. 3Com client software stores the SSID in the Windows registry. The WEP key is stored in the Windows registry with no encryption. [8]

Understanding WEP and the problems with WEP;

First Wired Equivalent Privacy (WEP) should be regarded as completely broke. It is possible for a hacker to retrieve the secret key in a matter of seconds by simply sniffing encrypted packets over the air. WEP is like giving everyone in the company the same password and never changing it. With this said it is still better than nothing.

Just as 802.11 describes wireless communications, WEP (Wired Equivalent Privacy) currently describes "wireless security". Today, WEP comes in 64-bit and more secure 128-bit, as well as proprietary versions that are designed to stop unauthorized access. But is 128-bit WEP the ultimate in wireless security that will withstand everything that hackers can throw at it? And what about the immediate future for wireless security ?
- The biggest WEP issue today is the inherent weaknesses that remain even as the technology evolves. There are three major flaws in WEP. To start, the technology relies on a short initialization vector (IV), which when used with the

shared key is eventually reused. By monitoring a network for an hour or less, hackers can theoretically crack a key that the network is using.
- A second major flaw is WEP's use of a static shared key. Should hackers crack the key, it is clearly exposed and easily exploited. Stronger security demands a dynamic key that, when exposed, is quickly replaced by a new one.
- Last, WEP relies on RC4 encryption. While RC4 was state-of-art when WEP was adopted, it has been surpassed by stronger encryption schemes. The move to 128-bit WEP by itself does not solve the weaknesses in WEP, it just makes it harder to crack the key.

By using a much larger key, 128-bit encryption provides greater cryptographic protection. Although more difficult to hack, 128-bit WEP falls victim to many of the same problems of lower bit WEP encryption. The 128-bit WEP extension is really not that much more secure than its brethren. 128-bit WEP is not the final answer, although it can serve as an interim solution.

Industry and Vendor Interm Solutions

There are two key technologies that are designed to improve wireless security:

Temporal Key Integrity Protocol (TKIP)
Advanced Encryption Standard (AES) protocol.

TKIP's dynamic keying scheme is designed to remedy WEP's static key problem by changing the temporal key every 10,000 packets. While the IV used under TKIP is larger, TKIP still relies on RC4 encryption. A big benefit here is that most of the 802.11 installed base can upgrade to TKIP though firmware patches. TKIP was initially called WEP2, but its name was changed so it wouldn't be associated with "WEP" security.

AES offers far stronger encryption than RC4. The main drawback is that AES requires more processing horsepower, and may only be used with new WLAN products. AES is essentially a more secure encryption technology, versus RC4 (which both WEP and TKIP use.[7]

TKIP: Interim Encryption Solution

The temporal key integrity protocol (TKIP), initially referred to as WEP2, is an interim solution that fixes the key reuse problem of WEP, that is, periodically using the same key to encrypt data. The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the 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 the data.

TKIP uses RC4 to perform the encryption, which is the same as WEP. A major difference from WEP, however, is that TKIP changes temporal keys every 10,000 packets. This provides a dynamic distribution method that significantly enhances the security of the network.

An advantage of using TKIP is that companies having existing WEP-based access points and radio NICs can upgrade to TKIP through relatively simple firmware patches. In addition, WEP-only equipment will still interoperate with TKIP-enabled devices using WEP. TKIP can be deployed quickly.
Why stick with RC4? RC4 is a stream cipher commonly used by SSL, where TCP connections prevent packet loss. However, WEP operates at the link level in networks where loss is common. Ultimately, the IEEE is expected to use the Advanced Encryption Standard (AES), a more appropriate cipher for wireless. Unfortunately, AES requires considerably more horsepower than most existing 802.11b cards provide. Keeping RC4 for now means that TKIP can be deployed in firmware updates instead of new chipsets, protecting consumer investment in 802.11b gear. Today's WEP keys can be reversed in as little as 15 minutes. To solve this, you need to do two things. You need to build [encryption] code that is as tight as possible and you need to change keys frequently enough to defeat key reversal. Lack of key management is why most 802.11b products now rely on manually configured keys. Several vendors ship proprietary solutions for dynamic key management. NextComm's approach is "key hopping;" short-lived keys derived by hashing a shared value with session seeds. Key hopping is available today for those people who want to use it now. In fact, the IEEE has long been laboring to find a robust, secure key management solution for wireless LANs. Keys, sequence spaces, and replay windows must all be resynchronized frequently without degrading performance or preventing roaming between access points. As it turns out, this challenge must be answered not only in long-term 802.11i standards, but also in the near-term fix for legacy systems. To avoid key reuse, temporal keys must be changed frequently. How frequently depends upon the packet rate. IEEE 802.1x will be used to manage temporal keys. Despite pressure to quickly deliver, the IEEE must also make sure that the legacy fix is secure.[7]

A three-part fix

TKIP is now composed of three elements and doesn't address just one part of the problem. To overcome pitfalls that crippled WEP, key-hashing must be combined with a real message integrity check to prevent forgery and replay, and dynamic key management (rekeying) to keep the ball rolling. In the current proposal, wireless endpoints begin with a 128-bit shared secret, referred to a temporal key (TK). The transmitter's MAC address is mixed with TK to produce a Phase 1 key. The Phase 1 key is then mixed with an initialization vector (IV) to derive per-packet keys. Each key is used with RC4 to encrypt one and only one data packet. This defeats the attacks based on the weaknesses in the key scheduling algorithm of RC4. [7]

TKIP is a temporary solution, and stronger encryption is still needed.

AES: Long Term Encryption Technique

In addition to the TKIP solution, the 802.11i standard will likely include the Advanced Encryption Standard (AES) protocol. AES offers much stronger

encryption. In fact, the U.S. Commerce Department's National Institutes of Standards and Technology (NIST) organization chose AES to replace the aging Data Encryption Standard (DES). AES is now a Federal Information Processing Standard (FIPS Publication 197) that defines a cryptographic algorithm for use by U.S. Government organizations to protect sensitive, unclassified information. The Secretary of Commerce approved the adoption of AES as an official Government standard in May 2002.
An issue, however, is that AES requires a coprocessor (additional hardware) to operate. This means that companies need to replace existing access points and client NICs to implement AES. [7]

A More In-depth look at the details of 802.1x;

The use of IEEE 802.1X offers an effective framework for authenticating and controlling user traffic to a protected network, as well as dynamically varying encryption keys. 802.1X ties a protocol called EAP (Extensible Authentication Protocol) to both the wired and wireless LAN media and supports multiple authentication methods, such as token cards, Kerberos, one-time passwords, certificates, and public key authentication. Initial 802.1X communications begins with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic. The following are specific interactions that take place among the various 802.1X elements:
- The client sends an EAP-start message. This begins a series of message exchanges to authenticate the client
- The access point replies with an EAP-request identity message.
- The client sends an EAP-response packet containing the identity to the authentication server.
- The authentication server uses a specific authentication algorithm to verify the client's identity. This could be through the use of digital certificates or other EAP authentication type
- The authentication server will either send an accept or reject message to the access point.
- The access point sends an EAP-success packet (or reject packet) to the client.
- If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic. [11],[12]

The basic 802.1X protocol provides effective authentication regardless of whether you implement 802.11 WEP keys or no encryption at all. Most of major wireless LAN vendors, however, are offering proprietary versions of dynamic key management using 802.1X as a delivery mechanism. If configured to implement

dynamic key exchange, the 802.1X authentication server can return session keys to the access point along with the accept message. The access point uses the session keys to build, sign and encrypt an EAP key message that is sent to the client immediately after sending the success message. The client can then use contents of the key message to define applicable encryption keys. In typical 802.1X implementations, the client can automatically change encryption keys as often as necessary to minimize the possibility of eavesdroppers having enough time to crack the key in current use.

It's important to note that 802.1X doesn't provide the actual authentication mechanisms. When utilizing 802.1X, you need to choose an EAP type, such as Transport Layer Security (EAP-TLS) or EAP Tunneled Transport Layer Security (EAP-TTLS), which defines how the authentication takes place. At this point the software supporting the specific EAP type resides on the authentication server and within the operating system or application software on the client devices. The access point acts as a "pass through" for 802.1X messages, which means that you can specify any EAP type without needing to upgrade an 802.1X-compliant access point. As a result, you can update the EAP authentication type as newer types become available and your requirements for security change.

The use of 802.1X is well on its way to becoming an industry standard. Windows XP implements 802.1X natively, and some vendors support 802.1X in their 802.11 access points. The 802.11i committee is specifying the use of 802.1X to eventually become part of the 802.11 standard. [11],[12]

Extensible Authentication Protocol (EAP) - The Extensible Authentication Protocol is a general authentication protocol defined in IETF standards. In a wireless LAN context, the access point sends one or more requests to the station, and the station sends a response in reply to each request. The access point ends the authentication phase with a success or failure message. The IEEE 802.1X standard provides a framework that makes it possible to send EAP packets between IEEE 802.11 entities. Here, a back-end server (RADIUS) is connected to the access point. The server is communicating with the station during the authentication. The access point is not doing any calculations during the authentication phase, it just forwards packets back and forth between the station and the server. In a roaming environment, the station may connect to several access points during a session. All the access points are assumed to be connected to the same back-end authentication server.

Protected EAP (PEAP) - RSA, Microsoft, and Cisco have developed a new EAP mechanism called Protected EAP. PEAP fixes a known vulnerability in the new 802.1x When a station wishes to associate with a wireless LAN access point. It is assumed that a back-end server is sitting behind the access point. The TLS handshake protocol is used to authenticate the back-end server. First the station notifies the access point that a new connection should be initiated, and sends a list of preferred cryptographic algorithms. The back-end server responds with a new Session ID, a list of selected cryptographic algorithms and a public key certificate. The station then generates a secret, encrypts it using the public key

obtained from the server, and sends the result. Finally, the server in its last message proves its ability to retrieve the secret. [9]

At this stage, both station and server may generate any amount of new key material to be used for subsequent bulk encryption. TLS provides a secure link over which authentication of the user can be established, by simply tunneling another authentication mechanism. The user provides a username and a one-time passcode provided by a hardware token. The authentication information is transferred to the back-end server over the secure TLS link. The back-end server itself may need to contact some other server to get this information validated. The messages sent by the station during user authentication are not transmitted in clear. This is very important in a wireless environment where passive eavesdropping is a serious threat. [9]
It will require a certificate for the authentication server but not for the clients, and t will use an encrypted channel for password transmission to mitigate dictionary attacks.

LEAP – Cisco provides Lightweight Extensible Authentication Protocol (LEAP) authentication based on the IEEE 802.1x security standard. LEAP uses Remote Authentication Dial-In User Service (RADIUS) to provide a means for controlling both devices and users allowed access to the wireless network. LEAP provides for dynamic per-user, per-session WEP keys. Although the WEP key is still the 128-bit RC4 algorithm proven to be ineffective in itself. LEAP adds features that maintain a secure environment. Using LEAP, a new WEP key is generated for each user, every time the user authenticates to use the wireless network. [10]

EAP TLS – Transport Layer Security is an open standard supported by nearly all the Wireless vendors. It requires the use of PKI which makes it extremely secure. Provides mutual authentication, integrity protected cipher suite negotiation, and mutual determination of encryption and signing key material between the wireless client and the authentication server (RADIUS). Authentication occurs automatically with no intervention by the user. Also it does not require any dependencies on the user account password.[7]

EAP TTLS – Tunneled Transport Layer Security is Funk software's version of EAP that uses Funk's Odyssey or Steel Belted RADIUS server. With TTLS PKI certificates are required only on the authentication server but not on the clients. This is considered almost as secure as EAP TLS while making deployment simpler. It also requires the use of PKI.[7]

EAP MD5 – This is the least secure version of EAP because it uses user names and passwords for authentication and is vulnerable to dictionary attacks. Also it does not support dynamic WEP keys which is a critical liability.

RADIUS - Remote Authentication Dial-In User Service (RADIUS) provides a means for controlling both devices and users allowed access to the wireless

network. Radius provides authentication and authorization of wireless clients.[10]

IPSec VPN's - IPSec is a secure encryption algorithm available in VPNs. VPNs allow users and telecommuters to connect to their corporate intranets or extranets. By requiring all wireless network traffic to be IPSec encrypted to the VPN over the WEP-encrypted 802.11 Layer 2 protocol, any data passed to and from wireless clients can be considered secure. All traffic is still susceptible to eavesdropping, but will be completely undecipherable. IPSec is a framework of open standards for ensuring secure private communications over IP networks. IPSec VPNs use the services defined within IPSec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPSec also has a practical application to secure WLANs by overlaying IPSec on top of clear text 802.11 wireless traffic. [10]

When deploying IPSec in a WLAN environment, an IPSec client is placed on every PC connected to the wireless network and the user is required to establish an IPSec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and DHCP/DNS server. IPSec provides for confidentiality of IP traffic, as well as authentication and antireplay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), which encrypts the data three times with up to three different keys. [10]

Though IPSec is used primarily for data confidentiality, extensions to the standard allow for user authentication and authorization to occur as part of the IPSec process.

L2TP - Layer 2 Tunnel Protocol is an emerging Internet Engineering Task Force (IETF) standard that combines the best features of two existing tunneling protocols: Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension to the Point-to-Point Protocol (PPP), which is an important component for VPNs.

PKI – Public Key Infrastructure is used to issue certificates to the IAS server and the wireless client for EAP TLS authentication. PKI manages digital certificates and creates an environment for authenticated, private and legally binding electronic communications and transactions.

Conclusion

Numerous options are available to secure a wireless network. A secure wireless network is possible using available technologies and techniques. A highly secure design will include, at a minimum, an authentication server such as a RADIUS, a high level encryption algorithm such as IPSec over a VPN, access points that are capable of restricting access to the wireless network based on

some type of mutual authentication, and an existing user database for authentication while providing for dynamic keying.

Though this document contains a large amount of detail on most aspects of wireless security it is not intended to cover every technology out there that is used for Wireless. Nor does it claim to cover every vulnerability and fix as these items change on a daily basis. In addition, it does not provide specific best practices on general WLAN deployment and design issues. This paper is instead intended to show a broad view of what technologies are available for wireless networks. Hopefully this paper will give you some choices on what technologies may be best for your organization's wireless network.

References

1.) The best way to secure wireless access
By Lee Schlesinger
February 7, 2002
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2845902,00.html

2.) Wireless Lan Security
March 29, 2002
http://techupdate.zdnet.com/techupdate/filters/specialreport/0,14622,6022247,00.html

3.) The ABCs of 802.11 standards
By Ian Keene
March 21, 2002
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2857227,00.html

4.) 802.11 Alphabet Soup
By Jim Geier
August 20, 2002
http://www.80211-planet.com/tutorials/article.php/1439551

5.) Enterasys on Standard's Confusion
By Kelly Kanellakis
http://www.80211-planet.com/tutorials/article.php/981611

6.) IEEE 802.11g
New Draft Standard Clarifies future of Wireless Lan
By William Carney, Marketing Manager
Wireless Networking Business Unit, Texas Instruments
(Note: White Paper has to be down loaded)

https://www-a.ti.com/apps/bband/xt_register.asp?mscssid=B85R1XME71F08KBLWMEBUSA1566J8NPF

7.) 802.11 Security Beyond WEP
By Jim Geier
http://www.80211-planet.com/tutorials/article.php/1377171

8.) Wireless Lan Security (PDF)
By Internet Security Systems

9.) Wireless LAN upper Layer authentication and key negotiation (PDF)
By Hakan Anderson, RSA Laboratories
January 17, 2002

10.) An Architecture for Securing Wireless Networks
By Gregory R.Scholz, Northrop Grumman Information Technology
http://www.cisco.com/en/US/about/ac123/ac147/ac175/about_cisco_ipj_archive09186a00800fa297.html

SAFE:
11.) Wireless LAN Security in Depth
By Sean Convery and Darrin Miller
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.pdf

12.) 802.1X Offers Authentication and Key Management
By Jim Geier
http://www.80211-planet.com/tutorials/article.php/1041171