A Comparison of Data-Link and Network Layer Security for IEEE 802.11 Networks

Group #8
Harold L. McCarter, Ryan Calme, Hongwu Zang, Wayne Jones
INFS 612
Professor Yih-Feng Hwang
July 17, 2006

Abstract

This paper presents a discussion of various types of security solutions for IEEE 802.11 networks at the Data-Link and Network Layer. This comparison is then applied to example network configuration in an attempt to determine the best security solutions for those instances.

I. Introduction

Wireless local area networks (WLANs) now play a larger role in corporate and home network environments. These networks are being used for a variety of purposes in corporate environments such as inventory management, mobile access, voice over internet protocol (VoIP), and long range bridging to remote locations. In the home environment they are being increasing used as a method to network multiple systems and deliver multi-media rich content within the home.

These systems are typically not as secure as wired networks because of the nature of radio frequency (RF) propagation. Because of this various methods were developed to address these security concerns.

These security methods are typically applied at that data-link and/or network layers, but because of this many users are forced to decide whether to implement security at layer 2, layer 3 or both in some circumstances. This can be a daunting tasked and is usually based on the needs of the organization with respect to network security and manageability.

II. Research Problem

Layer 2 security typically involves medium dependent procedures associated with the IEEE 802.11 standard. These include encryption mechanisms such as Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP) which is part of the Wireless Protected Access (WPA) standard, and Counter Mode/CBC-MAC Protocol (CCMP) which is based on the Advanced Encryption Algorithm (AES) as part of WPA2 and IEEE 802.11i.

In addition to encryption, there are various forms of authentication available to the IEEE 802.11 standard to help ensure user identities within wireless networks. Today these are typically limited to various forms of the Extensible Authentication Protocol (EAP) such as EAP-Transport Layer Security (EAP-TLS), EAP-Tunneled TLS (EAP-TTLS), Protected EAP (PEAP), and Cisco's Lightweight EAP (LEAP).

Layer 3 security involves the use of software applications to encrypt data between two points in order to ensure data integrity. This is typically done using a Virtual Private Network (VPN) implementing a form of encryption such as Internet Protocol Security (IPSec), Point to Point Tunneling (PTPP), or Layer 2 Tunneling Protocol (L2TP).

We propose to examine these various areas and identify several possible options for wireless security in various types of network configurations. For example, the security implemented by a corporate network must meet more stringent standards than those present to secure a home network.

III. Data-Link Security Solutions

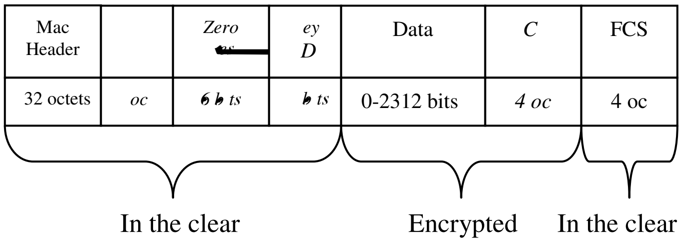
Data-Link security solutions for wireless networks involve various types of encryption and authentication. Authentication is used to ensure that only authorized users have access to the wireless network while encryption scrambles communications between authorized devices so that no data can be intercepted. Layer 2 security solutions are typically associated with the networking protocol in use; however, as we shall see there are proprietary encryption techniques offered by third party vendors.

The three main categories of data-link security that will be discussed are static Wired Equivalent Privacy (WEP), 802.1x / Extensible Authentication Protocol (EAP) variations, and third party proprietary encryption methods. These are the most common types of security solutions employed on most of today's wireless networks, and are often combined with network layer security solutions such as VPNs, which will be discussed in the next chapter.

A. t t c EP

WEP was the first security mechanism to be utilized on IEEE 802.11 networks. It originally solved the problem of authentication and encryption simultaneously through the used of shared keys that were either 64 or 128 bits in length. The protocol was supposed to provide the same level of protection as a wired environment, but fell short in several areas.

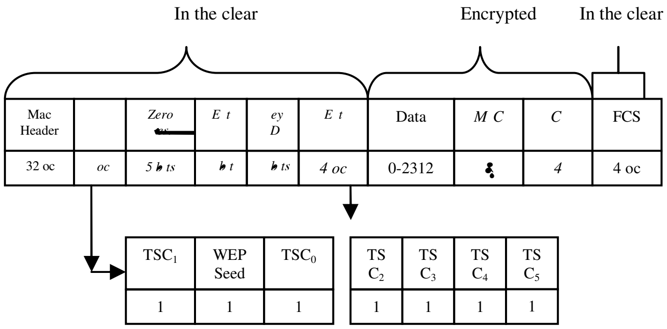
The authentication piece was solved by ensuring that only users with the same pre-shared key (PSK) could access the network. This prevented access to users without this PSK and also provided a method for data encryption. The WEP protocol utilizes the propriety RC4 algorithm developed by RSA Security to provide encryption for the data communications. The same PSK is passed through the RC4 algorithm to generate the WEP encryption keys. As you can see in Figure 1, important header information is sent in the clear, including the Initialization Vector (IV) for the algorithm, which is the greatest weakness associated with WEP.



Mac Header		*Zero*	*ey D*	Data	*C*	FCS
32 octets	*oc*	*6 b ts*	*b ts*	0-2312 bits	*4 oc*	4 oc

Figure 1

WEP falls short in the security world because the IV does not rotate sufficiently and is passed in the clear. This allows malicious users the ability to guess the IV's and ultimately the PSK after analyzing sufficient network traffic with powerful computer programs. Because WEP's primary weakness resides in the encryption portion of the protocol a new algorithm was used to generate the WEP keys. TKIP was introduced to add additional components to a standard WEP frame, while still utilizing the RC4 algorithm and preventing the need to upgrade hardware to implement it. This new encryption algorithm was central to WPA. TKIP is not bullet proof, but provided a tremendous upgrade in the ability to secure wireless networks



Mac Header		*Zero*	*E t*	*ey D*	*E t*	Data	*M C*	*C*	FCS
32 oc	*oc*	*5 b ts*	*b t*	*b ts*	*4 oc*	0-2312	[illegible]	*4*	4 oc

TSC_1	WEP Seed	TSC_0
1	1	1

TSC_2	TSC_3	TSC_4	TSC_5
1	1	1	1

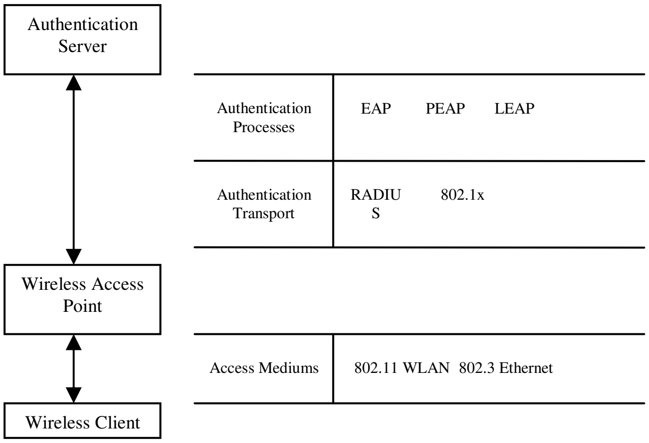
Figure 2

B. [illegible] . EAP r t ons

In addition to the encryption improvement that TKIP brought, the WPA standard also allowed the use of 802.1x and EAP for mutual authentication and the use of dynamic keys in the encryption process. This improvement increased the security capabilities of wireless networks and would ultimately become the standard for enterprise distributions.

802.1x is a port based protocol that provides an authentication framework for 802 compliant networks. EAP and its various types, provide a method to exchange user information between an authentication server and a client. These protocols also allow for the exchange of dynamic session keys to be used with the encryption mechanism in place: WEP, TKIP, or CCMP which will be discussed later. 802.1x also supports the use of the Remote Access Dial-In User Service (RADIUS) for authentication exchange messages.

Figure 3 depicts how 802.1x, EAP, and RADIUS work together to exchange user information and authenticate a client on a wireless network.



Authentication Processes	EAP PEAP LEAP
Authentication Transport	RADIU S 802.1x
Access Mediums	802.11 WLAN 802.3 Ethernet

Figure 3

EAP has several variations that operate with different levels of security. For example, EAP-MD5 uses the Challenge-Handshake Authentication Protocol (CHAP) to exchange passwords, but because the keys are passed in the clear it is insecure. Other EAP methods such as LEAP, PEAP, EAP-TLS, and EAP-TTLS were developed with additional security mechanisms to protect the exchange of crucial passwords and session keys.

In the newly released IEEE 802.11i standard the use of 802.1x/EAP in combination with TKIP or CCMP encryption is required. The Wi-Fi Alliance has incorporate IEEE 802.11i into its new WPA2 standard which allows backwards compatibility with WPA in some scenarios. IEEE 802.11i provides the most robust solutions for IEEE 802.11 networks without external proprietary techniques or additional Layer 3 security solutions.

C. Proprietary Encryption Techniques

The final security method discussed is a third party encryption technique developed by various companies to provide enhanced security to wireless networks. These solutions typically involve the use of Enterprise Encryption Gateways (EEGs) which are placed between the physical connection of the wireless and wired networks within an organization and handle the encryption and authentication of wireless clients. An example of this type of solution is Fortress Technology's Air Fortress product line.

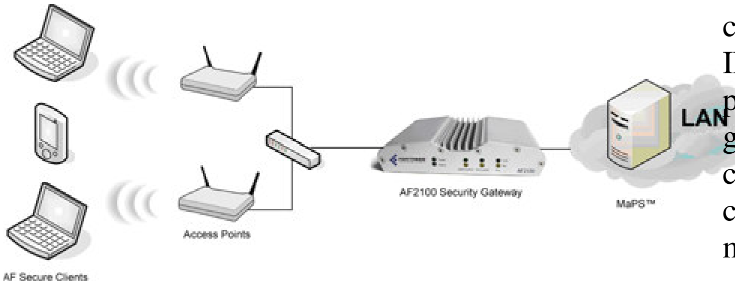


Figure 4

As you can see in Figure 4, the EEG provides a vital service to the network. By encrypting the data at layer 2 important routing information such as IP addresses are not visible to passive listeners. Although this technique provides less visibility of the network to malicious users it also limits the scalability of the solution. If encryption techniques are employed at the layer 2 level then those packets cannot be routed and thus an EEG is required within each subnet that requires external routing assistance at layer 3.

III. Network Layer Security Solutions

Network layer security almost exclusively involves the use of VPNs to provide end-to-end encryption for data. VPNs were successfully extended into the wireless world as they allow engineers to treat their wireless networks as an untrusted network, such as the Internet, and tunnel connections between two trusted locations.

The IPSec protocol is the most widely used VPN solution at the network layer. This protocol provides enhanced security features such as more robust encryption algorithms and comprehensive authentication. IPSec is divided into two principle protocols: the authentication header (AH) protocol and the encapsulation security payload (ESP) protocol.

In both AH and ESP, source and destination shake hands to generate security association (SA). IPSec supports two encryption modes: Transport mode and Tunnel mode. Tunnel mode, which utilizes ESP, encrypts not only the payload of each packet but also the header of the packet. Transport mode encrypts the data and leaves IP header untouched. Tunnel mode is generally accepted as more secure because of the masking done to the IP header. If there is no IP header encryption it is possible that malicious users could eventually find the source and destination IP, and observe, analyze and decrypt the encryption protocol of the payload part in the IP datagram. If the IP header is encrypted it is much harder to accomplish this.

VPNs can be configured to secure wireless networks in several ways; however, the most common is to configure each wireless station to use IPSec to establish a connection through an access point to a VPN server, which serves as a security gateway to the trusted wired network. This configuration typically relies on a secret string of characters for authentication and on connection management to generate and refresh the key.

IV. Comparison of Layer 2 and Layer 3 Solutions

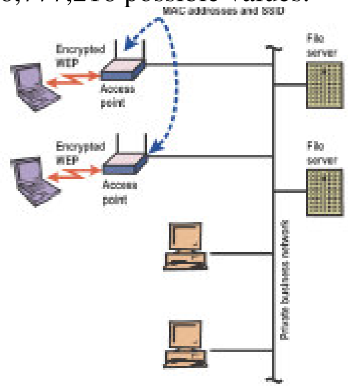
Wireless network security is a multi-faceted problem that cannot be solved by a single product. It includes protecting the traffic with advanced technology schemes, sophisticated authentication and access control mechanisms. It also requires the use of policies and security processes that moves with the user. This section of the paper will focus on several of the technologies used to provide security at layer 2 and layer 3 of the wireless infrastructure. Enterprise today must wade through a sea of security standards, layer 2 security techniques from Wired Equivalent Privacy (WEP) to Temporal Key Integrity Protocol (TKIP) to Advance Encryption Standard (AES), and layer 3 tunneling technologies such as Internet Protocol Security (IPSec) to new authentication approaches such as 802.1X.

A. ▮ u res of EP

The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the optional 128-bit standard. WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet. On a busy network, 128-bit static WEP keys can be obtained in as little as 15 minutes, according to current estimates.

WEP uses the RC4 stream cipher that was invented by Ron Rivest of RSA Data Security, Inc. (RSADSI) for encryption. The RC4 encryption algorithm is a symmetric stream cipher that supports a variable-length key. The IEEE 802.11 standard describes the use of the RC4 algorithm and key in WEP, but does not specify specific methods for key distribution. Without an automated method for key distribution, any encryption protocol will have implementation problems because of the potential for human error in key input, escrow, and management.

The initialization vector is at the center of most of the issues that involve WEP. Because the initialization vector is transmitted as plaintext and placed in the 802.11 header, anyone sniffing a network can see it. At 24 bits long, the initialization vector provides a range of 16,777,216 possible values.



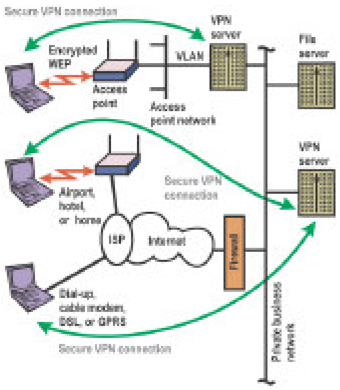
This diagram depicts WEP-based security with MAC address filtering. With the implementation of MAC address filtering, the fixed upper limit is established by the maximum number of MAC addresses that can be programmed into each AP used in an installation.

B. An ys s of PNs

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 cleartext 802.11 wireless traffic.

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 Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS) server. IPsec provides for confidentiality of IP traffic, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), or the new Advanced Encryption Standard (AES). Though IPsec is used primarily for data confidentiality and device authentication, extensions to the standard allow for user authentication and authorization to occur as part of the IPsec process.

The VPN solution for wireless access is currently the most suitable alternative to WEP and MAC addressing filtering. The VPN provides a secure dedicated path (or "tunnel") over an untrusted network. There are a number of tunneling protocols which can be used including the Point-to-Point Tunneling Protocol (PPTP) and Layer 2 Tunneling Protocol (LSTP) in conjunction with standard, centralized authentication solutions, such as Remote Authentication Dial-In User Service (RADIUS) servers, as shown in the below diagram.



Using the VPN approach can provide a number of advantages to include:

- Currently deployed on many enterprise networks
- Scalable to a large number of 802.11 clients
- Low administration requirements for 802.11 APs and clients. The VPN servers can be centrally administered.
- Traffic to the internal network is isolated until VPN authentication is performed.
- WEP key and MAC address list management becomes optional because of security measures created by the VPN channel itself.
- Consistent user interface in different locations such as at home, at work, and in an airport.

Although there are a number of advantages to VPN solution, there are drawbacks as well such as the lack of support for multicasting.

C. EEE [illegible] .

An alternative WLAN security approach focuses on developing a framework for providing centralized authentication and dynamic key distribution. This approach is based on the IEEE 802.11 Task Group "i" end-to-end framework using 802.1X and EAP to provide this enhanced functionality. The three main elements of an 802.1X and EAP approach are:

- Mutual authentication between client and authentication (RADIUS) server
- Encryption keys dynamically derived after authentication
- Centralized policy control, where session time-out triggers re-authentication and new encryption key generation

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform mutual authentication, with the client verifying the RADIUS server credentials, and vice versa. An EAP supplicant is used on the client machine to obtain the user credentials (user ID and password, user ID and one-time password [OTP], or digital certificate). Upon successful client and server mutual authentication, the RADIUS server and client then derive a client-specific WEP key to be used by the client for the current logon session. User passwords and session keys are never transmitted in the clear, over the wireless link. EAP provides three significant benefits over basic 802.11 security:

- The first benefit is the mutual authentication scheme, as described previously. This scheme effectively eliminates "man-in-the-middle (MITM) attacks" introduced by rogue access points and RADIUS servers.
- The second benefit is a centralized management and distribution of encryption keys. Even if the WEP implementation of RC4 had no flaws, there would still be the administrative difficulty of distributing static keys to all the access points and clients in the network. Each time a wireless device was lost; the network would need to be re-keyed to prevent the lost system from gaining unauthorized access.
- The third benefit is the ability to define centralized policy control, where session time-out triggers re-authentication and new key derivation.

V. Solutions / Analysis - Selected Configuration Examples

With all of the previous information on available layer 2 and layer 3 wireless security schemes, how should one proceed to put them into practice? What setup fits a given situational need? To explore this, we present three scenarios, in which differing levels of risk are acceptable to the user(s). First, there is the personal home network, consisting of fewer than five computers. Second, the small business, such as an individually owned and operated retail location with less than 50 users. Finally, a corporate enterprise system with thousands of users spread over not only a local wireless network, but across the globe, and via diverse connection-types.

A. o e Networ

For your average home user, wireless connections are becoming essential. Wireless security, however, is often an afterthought. Few hardware providers ship their wireless access points or routers with any security such as WEP enabled by default, in an effort to provide a hassle-free setup. More often than not, individuals building a home network feel that their task is accomplished once computers can connect wirelessly, and go no further in network security and administration.

WEP or TKIP (WPA) with a shared key is in most cases the best option for a small home network at this time. With a relatively quick setup, a pre-shared key can be chosen or generated for the method of encryption, often even in ASCII, and distributed to the few users of the network. With such a small network, the key is less likely to be compromised via a lost laptop, or given out to unreliable sources. However, if the key is no longer private, the process of creating a new key and removing the old key would take very little time with such a small number of connected systems.

As we mentioned before, WEP privacy can be compromised in as little as fifteen minutes with the right equipment and software monitoring a busy wireless network. This situation changes as we examine the small home network, because said network would likely be idle half the time, if not more. This hardly constitutes a "busy network". The home network is also a less likely target for such packet-sniffing attacks, as the data contained within is unlikely to provide the attacker with any significant monetary gain. Most likely electronic mail and web-pages are all mat traverse such a network.

B. Bu s ness Net-wor

In our second scenario we consider a small business, with 50 or fewer connected clients and relatively few wireless access points. With this setup, a good suggestion might be to use WEP, TKIP, or AES encryption with shared keys and MAC address filtering. Another option may be a dedicated VPN solution that could be used to connect to not only the wireless network but the wired corporate network from outside the office, reducing the number of software solutions required for such a small business. A business, no matter how small, may become a target for parties wishing to gain access to the encrypted data, or the network. Any time customer information, or proprietary business information is stored on a network share, or traveling across a wireless link, more caution should be taken it the protection of these resources.

As mentioned in the previous home network situation, WEP protection is better than no protection, although it can be cracked by the determined individual when the network experiences enough traffic to provide sufficient packets. This threat would justify the addition of TKIP or AES encryption schemes along with MAC address filtering. MAC address filtering is practical only on the small to medium-scale network, when the number of clients will never exceed the upper limit allowed by the wireless hardware. MAC addresses are unique to the wireless client, but unfortunately can easily be faked by software available today. It should be mentioned that a table of accepted MAC addresses would become difficult to maintain over time, as clients leave, and new clients arrive, unless good controls are put into place to obtain such MAC acceptance. If the number of clients is fixed, and rarely changes, and the administrator can be alerted to computers that will no longer be making use of the network, the MAC address table can be kept within reasonable limits of size.

For these reasons a simply VPN solution might be the best solution for a small business as laptop users would be able to use the VPN in connection with not only their wireless networks, but with their wired corporate network from home or external wireless hotspots without compromising security.

C. Corpor te Net-wor

Last, we can look to the large corporation, with thousands of employees. This network configuration is different in that it is rarely a centralized or contained network, and the connections to this network vary in location, security level, and speed. For large businesses, a new method is needed that does not have a single key to lose, or a database of accepted MAC addresses to maintain. Most companies with vast networks and/or roaming employees have chosen to use a VPN, which makes use of the IPsec framework described previously. VPN systems are more easily maintainable, as the security is provided by a central administration. This becomes important as the size of the network, and number of connected clients, grows. For common VPN software for businesses, such as Nortel's Contivity client, a user must provide authentication (often a username and password) to connect to the server-side VPN system. Once such a connection is established, the connection itself can be viewed as a tunnel connecting both the remote client, and the server. Regardless of the network link on which the data travels, the packets are safe, and there is no key to compromise. VPNs necessitate the installation of client software on every computer that wishes to connect, which presents an administration problem such as simultaneous software updating, however, most of the computers in a VPN configuration are fixed-build, company issue machines. Most likely these computers were designed with an upgrade scheme in place to either alert the user when a new version of their software must be installed, or to update that software seamlessly.

A VPN system can be coupled with layer 2 security such as a full IEEE 802.11i compliance distribution. However, the design of VPN software is such that the security level of the network link is of trivial importance. If a network administrator so wished, wireless-enabled PCs could be set to only connect to secured networks and then require VPN connections to reach the private network of the corporation.

Ideally, the client-server VPN setup is the most secure and desirable at this time. This is only feasible when the sizeable cost for such an implementation is necessitated by the importance of the private data. Client software distribution, username and password administration, and dedicated hardware and software on the server side are not matters to be taken lightly, and will likely require continued support and upkeep.

The future of wireless security may be driven by newer approaches to the same old problem, such as EAP, and may do away with the current problems with wireless security. The difficulty is in preserving the level of convenience that is expected by the home user, while providing the level of security expected by the business user. There is no doubt that more secure protocols are possible, within layer 2, layer 3, or even a hybrid of layers 2 and 3.

VI. Conclusion / Summary

From the above analysis of various forms of wireless network security it seems difficult to find one solution for every situation. It is apparent that each organization must understand their own security requirements and scale their solution to that need. This must also be done in order to ensure that each organization selects a solution that matches available resources as added security requires additional labor and financial expenditures.

The labor required to distribute these networks is relatively small in comparison to the amount necessary to maintain and support them. For example, a small business with fifty employees may want to employee a full IEEE 802.11i compliant network with VPN overlays, but the resources required to support that network are well beyond the limitations of such a company. For this reason many organizations choose to avoid wireless network access in their office spaces at the cost of the added benefits wireless can provide.

VII. References

[1] *C NA – Cert f ed re ess Networ Ad n str tor* *(rd ed.)*. McGraw-Hill/Osbourne, Emeryville, CA, 2005.

[2] *C P – Cert f ed re ess ecu r ty Profess on (st ed.)*. McGraw-Hill/Osbourne, Emeryville, CA, 2003.

[3] Sankar, Krishna, Sundaralingam, Sri, Balinsky, Andrew, Miller, Darrin. *C sco re ess LAN ecu r ty: E pert u d nce for ecu r ng You r . Networ s.* Cisco Press, Indianapolis, IN 2005.