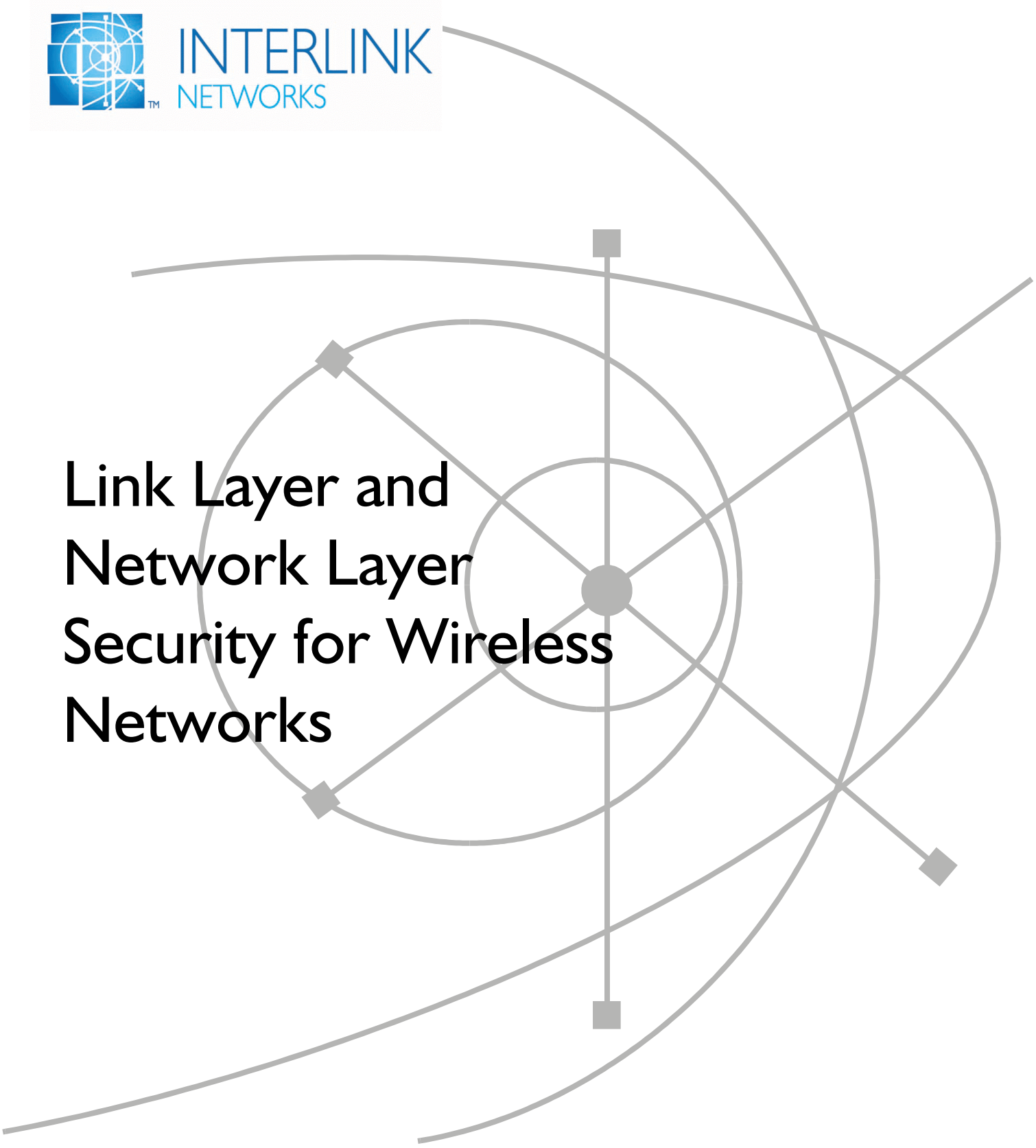


Link Layer and Network Layer Security for Wireless Networks

Interlink Networks, Inc.
May 15, 2003

Link Layer and Network Layer Security for Wireless Networks

Abstract

Wireless networking presents a significant security challenge. There is an ongoing debate about where to address this challenge: at the link or network layer (OSI layers 2 or 3, respectively). This paper looks at the basic risks inherent in wireless networking and explains both approaches, but concludes that link layer security provides a more compelling, complete solution and that network layer security serves well as an enhancement in applications where additional WLAN security is requested.

I. INTRODUCTION

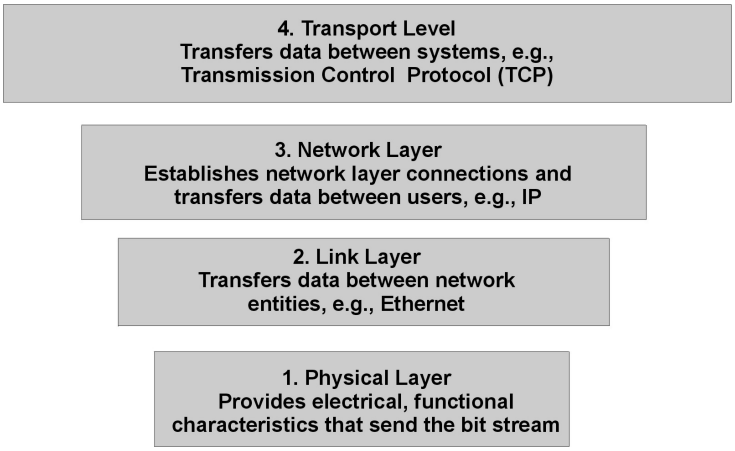
Wireless networking brings a whole new meaning to networking security risk analysis and mitigation. With readily available equipment, attacks on wireless networks have never been so easy. Network administrators, uncomfortable with the state of wireless LAN security, have turned to more traditional methods to secure their wireless networks. Often, they will use IPSec, which operates on the network layer, to provide the required security.

Unfortunately, network layer security solutions such as IPSec do not address all of the security concerns that arise from the shared airwaves. In addition, the "per-tunnel" licensing of commercial IPSec solutions makes the network layer solution somewhat costly, and adds to the management headaches inherent in network layer solutions. Since network layer security is not a complete solution for wireless networks, standards bodies such as the IEEE have focused on 802.11, a protocol that provides security at the link layer.

Link layer security can protect a wireless network by denying access to the network itself before a user is successfully authenticated. This prevents attacks against the network infrastructure and protects the network from attacks that rely on having IP connectivity. Wi-Fi Protected Access, a link layer

solution, was designed specifically for wireless networks and is particularly well suited for wireless security.

This paper examines network layer security provided by IPSec and link layer security provided by WPA, addressing the characteristics of each approach when applied to wireless networks. It focuses on the shortcomings of IPSec when applied to wireless networking security concerns, and it demonstrates how WPA provides a more desirable wireless network security solution for most applications.



OSI Layers 1 through 4

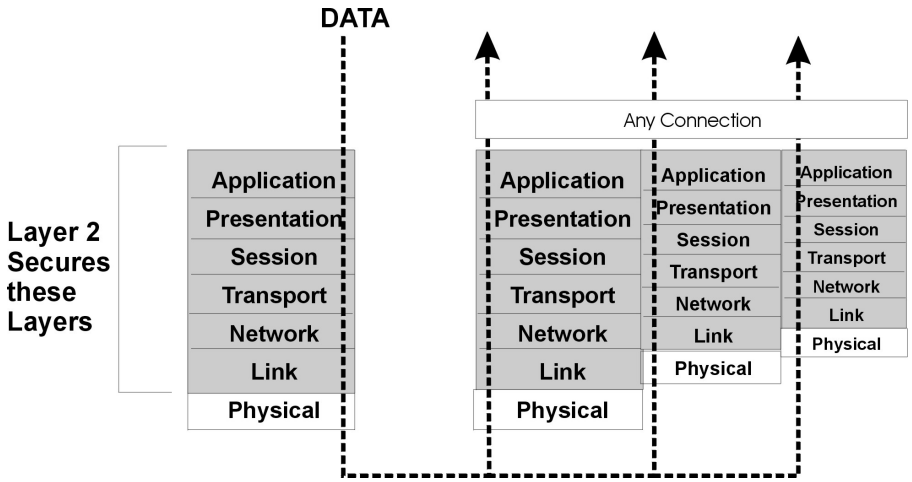
2. LINK LAYER SECURITY WITH WI-FI PROTECTED ACCESS

Link layer security provides point-to-point security between directly connected network devices. Link layer security provides secure frame transmissions by automating critical security operations including user authentication, frame encryption, and data integrity verification.

In a wireless network, link layer protection defines a network that is secure to outsider intervention. Link layer protection starts with an authentication service and includes link layer encryption and integrity services. As a result, only authenticated users can actively use the link layer, and all data traffic on the link layer is encrypted and authenticated.

Link layer protection secures wireless data only where it is most vulnerable, on the wireless link. Link layer security is also characterized by:

- Small footprint that can be easily integrated into network interface cards, access point devices, and mobile devices. Link layer security mechanisms are often integrated into the network hardware.
- Allows higher-level protocols, such as IP, IPX, etc., to pass securely. This provides security for all upper layer protocols.

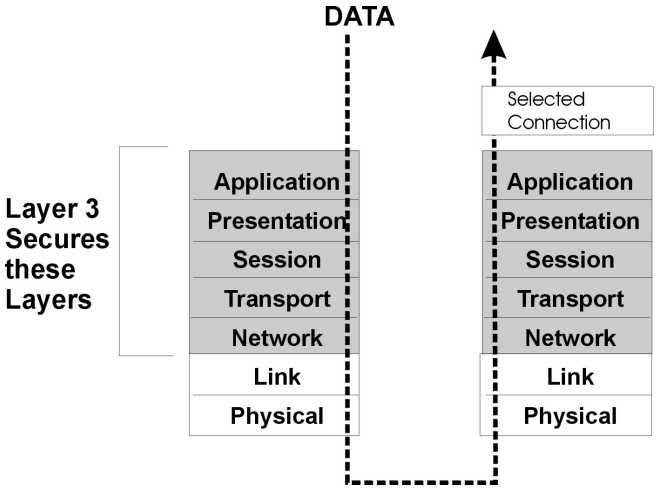


The Wi-Fi Alliance has taken work done by the IEEE 802.11TGi and adopted key portions to create a new standard called Wi-Fi Protected Access (WPA). WPA is an industry standard for providing strong link layer security to WLANs, and supports two authenticated key management protocols using the Extensible Authentication Protocol (EAP). WPA also requires data frame encryption using TKIP (Temperal Key Integrity Protocol) and message integrity using a Message Integrity Check (MIC) called Michael.

WPA provides strong, robust security on wireless connections, which addresses some widely publicized security holes in older wireless LAN standards.

3. NETWORK LAYER SECURITY WITH IPSEC

Network layer security provides end-to-end security across a routed network and can provide authentication, data integrity, and encryption services. In this case, these services are provided for IP traffic only. Once the network endpoints are authenticated, IP traffic flowing between those endpoints is protected.



IPSec is the standard network layer security protocol, and provides a standard and extensible method to provide security to network layer (IP) and upper layer protocols such as TCP and UDP. It is used extensively to secure network connections that extend from network hosts to both IPSec gateways and to other hosts. It can also be used between network entities such as routers or IPSec gateways.

IPSec is a well-understood and widely used mechanism for providing security between wired network elements, but it was not designed for protecting lower layer protocols such as 802.11.

4. WHY LINK LAYER SECURITY IS IMPORTANT

Deciding which layer of the network you should apply security to can be confusing. Some network administrators may feel justified in relying on IPSec for WLAN security. But given the underlying shared medium (the radio frequency spectrum), IPSec is not an optimum solution. Older, widely deployed network layer security methods face new threats today that they were not designed to address. While it is possible to supplement network layer security to appear to provide wireless security, these complex solutions will always need to be reviewed in light of new risks.

IPSec security protects data beginning with the network layer. It provides protection for only selected network connections, and leaves the network open to attacks that work outside of this limited security method. In addition, network layer protocols often use authentication mechanisms that require that the network be completely open to all wireless devices, ultimately leaving the network vulnerable.

Link layer security such as WPA operates on the data link layer to provide protection specifically for the over-the-air portion of the connection between the mobile user and wireless access point. WPA protects upper layer attacks by denying access to the network before authentication is completed.

5. SHORTCOMINGS OF USING NETWORK LAYER SECURITY FOR WIRELESS LANS

Although IPSec is often used to provide wireless LAN security, there are some serious drawbacks to using network layer security alone for securing the wireless LAN. First and foremost, there are security vulnerabilities that must be addressed. In addition, managing an IPSec installation can be much more difficult that deploying a WPA solution. There are also some integration and usability concerns that stem from using IPSec differently from how it was intended. Finally, it must be noted that the Total Cost of Ownership (TCO) is likely much greater for an IPSec solution.

5.1. SECURITY VULNERABILITIES

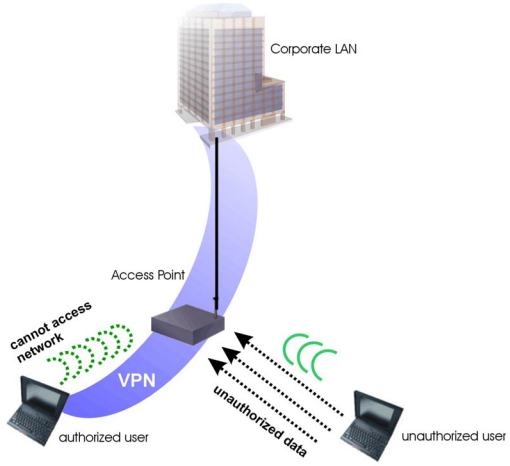
IPSec was not designed specifically for WLAN usage. Since it protects only the network layer and upper layer protocols, it leaves the link layer vulnerable. The following four sections discuss the types of attacks that might be effective against a network layer IPSec solution.

5.1.1. Denial of Service Attack

Denial of service (DOS) attacks often attempt to monopolize network resources. This type of attack prevents authorized users from gaining access to the desired network resources.

In a wireless network that relies solely on IPSec for security, an access point must bridge all traffic to the wired network. This allows legitimate users to authenticate and establish an IPSec connection, but it also allows malicious users to send frames that the access point may accept. Thus, an attacker can flood the access point with data, interrupting a legitimate user's connection.

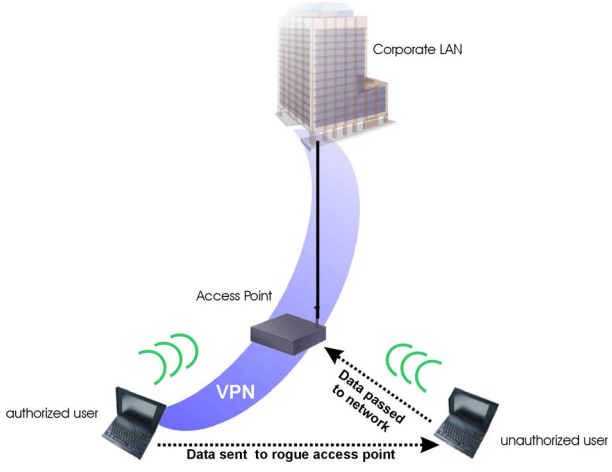
Another DOS attack could result when an attacker captures a previous disconnect message and re-sends it, resulting in the legitimate user's loss of connection to the WLAN.



Denial of Service Attack

5.1.2. Man-in-the-Middle Attack

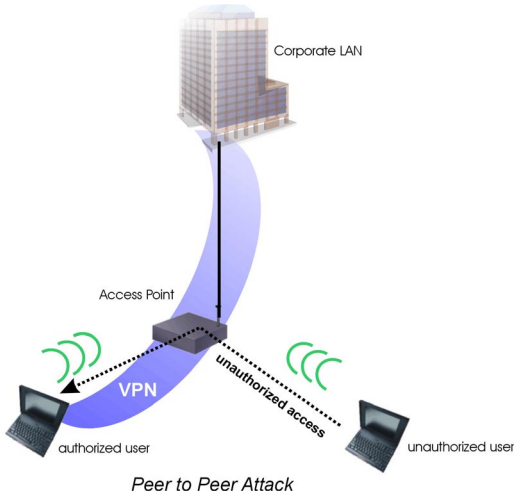
Network layer security does not typically provide protection for protocols other than IP, leaving other protocols unprotected and vulnerable to attacks. One such attack uses the Address Resolution Protocol (ARP) to fool a client into sending data to a malicious peer. An attacker could launch a man-in-the-middle (MITM) attack by using forged ARP messages to insert a rogue entity into the data path.



Man-in-the-Middle Attack

5.1.3. Peer-to-Peer Attack

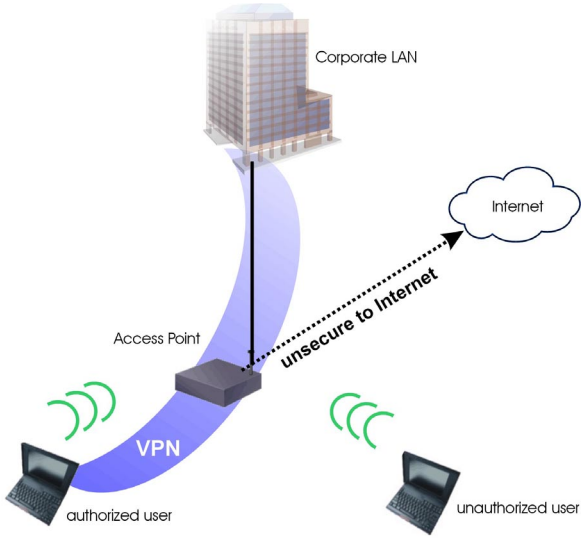
Often, IPSec is used to protect network layer connections between a user and a gateway. Without link layer security, however, the access point will bridge frames initiated from both authorized and unauthorized users. Thus, an unauthorized user could monitor the wireless traffic to capture information such as the IP address of a neighboring peer, and then use it to attack the wireless interface on neighboring peer hosts.



Peer to Peer Attack

5.1.4. Limited Network Access Protection

IPSec protects the traffic only between the wireless user and the end-point. Any connection outside of the tunnel is not secure. A business user connecting to a personal email account, for example, may be surprised to learn that browsing to an Internet site is not secure. Corporate users with a network layer IPSec tunnel providing security at a public access hotspot have nothing protecting the traffic that is not destined for the corporate IPSec gateway.



Limited Network Access Protection

5.2. TOTAL COST OF OWNERSHIP(TCO)

There are a number of factors to consider in calculating TCO, including hardware/software acquisition and maintenance, component installation and monitoring, and user training. The costs and complexities associated with IPSec typically drive the TCO of network layer security well above that of link layer security. In addition to cost considerations, network layer security solutions also present challenges when trying to scale for larger WLAN enterprise installations.

	Link Layer	**Network Layer**
Hardware/Software	802.1x enabled APs RADIUS server EAP modules (typically included) Personal firewall (optional)	VPN Gateway(s) Firewall(s) VPN authentication server All APs wired 'outside' of Firewall VPN client Personal firewall
Installation	AP replacement (or firmware upgrades) RADIUS server and user database EAP client module and RAS configuration Personal firewall install (optional)	VPN gateway and firewall install. User policy configuration VPN authentication server and VPN client configuration Personal firewall install
Training	RADIUS support, user management RAS usage	VPN support, user management VPN client usage

5.3. MANAGEMENT

- Client software deployment and configuration is a significant issue in the enterprise
- Can be incompatible with other traditional security devices. For instance, incoming packets are reviewed by network firewalls before being allowed to enter the network. Because VPNs hide packet data, the encrypted packets are rejected by the firewall as potentially dangerous.
- VPNs increase reliance on vendor-specific components and can decrease system performance
- Granting and revoking privileges presents on-going maintenance issues

5.4. INTEGRATION AND USABILITY

- Guest users may have difficulty being allowed onto the network
- VPN sessions may be broken when users move among access points since the IP address changes. This can cause other applications to freeze, requiring users to reboot their machines.

6. THE WPA APPROACH

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 (e.g., Denial of Service attacks) and targeted attacks (e.g., 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

6.1. COMPARISON OF LINK LAYER AND NETWORK LAYER PROTECTION

	Link Layer	**Network Layer**
Authentication Services	Authenticates interface to the network. Normally based on user of the system.	Authenticates an IP address to the network. Normally based on user of the system.
Authentication Vulnerabilities	Dictionary	MITM, Replay, Dictionary
Data protection	Protects all data frames into and out of the NIC.	Protects all IP datagrams based on the source or destination address.
Unprotected data	Management frames	Other IP addresses directed to NIC. Non-IP datagrams (e.g. ARP)
Scope of data protection	Link only	From system to gateway or endpoint
Interaction with other security layers	None	Potential problem if same layer (e.g. IPsec within IPsec)
Mobility Support	Re-authentication typically needed for each new link	Authentication stability across links and link state changes
Wireless System vulnerabilities	To other authenticated systems	To any other wireless system, authenticated or not
Provider Service theft	None practical	Authenticated system providing proxy services
Availability	Now: WPA, WPA2 in Q4 2003	Now: IPsec, L2TP, PPTP

7. CONCLUSION

Wireless security can be addressed at the link layer (layer 2), network layer (layer 3), or a combination of both. By understanding both types of security, network administrators can make decisions that are appropriate for their own environments.

Some enterprises have deployed popular IPsec solutions such as VPNs to protect their wireless users. However, VPNs provide protection for traffic only between the user and a private network, and do not protect against other security risks associated with wireless networks. Since VPNs were developed to protect users on a wired network, they leave wireless users open to many security concerns that arise from wireless, shared Radio Frequency (RF) media.

The costs and complexities associated with a VPN are often well above that of a link layer solution such as WPA. Added to other concerns, such as management and integration / usability issues, VPN solutions are not the best choice for securing wireless data. In order to address these concerns, network administrators must secure the wireless link layer using WPA.

The link layer security provided by WPA is an essential component for wireless LAN security. As the Wi-Fi Alliance recommends, network administrators should secure access to the wireless link layer by using EAP for user authentication and encryption key generation. This provides a baseline of security that is necessary to protect wireless users and the wired network they are accessing.

Network layer security will remain important to the wireless user in an untrusted (e.g., hot spot) 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 (WPA2, expected later this year) is likely to meet the security needs of most organizations.

Interlink Networks, Inc.
5405 Data Court, Suite 300
Ann Arbor, MI 48108

Main - (734) 821-1200
Sales – (734) 821-1228
Fax – (7340 821-1235

Website: www.interlinknetworks.com

Interlink Networks is a leading developer of access control and security software for wired and wireless networks. Our standards-based solutions enable secure and trustworthy WLAN networks through strong 802.1x authentication. Interlink Networks provides software solutions for carrier-class, enterprise, and small business/home office users.