INTERLINK NETWORKS

White Paper

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. It concludes that link layer security provides a more compelling, complete solution and that network layer security enhances link layer security where additional WLAN security is required.

Introduction

Wireless networking brings a whole new meaning to networking security risk analysis and mitigation. With readily available equipment, attacks on wireless networks are very easy. Some network administrators, uncomfortable with the state of wireless LAN security, have turned to more traditional wired network security solutions to secure their wireless networks as well. Often, they will use VPNs, which operates at the network layer, to provide the required security.

Unfortunately, network layer security solutions such as VPNs do not address all of the security concerns that arise from the shared airwaves. In addition, the "per-tunnel" licensing makes VPN solutions costly and adds to the management headaches inherent in network layer solutions. Since VPNs don't provide 100% security coverage for Wi-Fi networks, the industry has standardized on 802.1X, a link layer security protocol for wireless networks.

Link layer security protects 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 (WPA), a link layer solution, was designed specifically for wireless networks using 802.1X and is particularly well suited for wireless security.

This paper examines network layer security provided by IPSec VPNs and link layer security provided by WPA and 802.1X, addressing the characteristics of each approach when applied to wireless networks. It discusses the shortcomings of IPSec when applied to wireless networking security concerns, and it demonstrates how 802.1X provides a more desirable wireless network security solution for most applications.

www.interlinknetworks.com
2500 Packard Road, Ste 202, Ann Arbor, MI 48104 USA
Phone: +1 (734) 821-1200 Fax: +1 (734) 821-1235

What is Network Security?

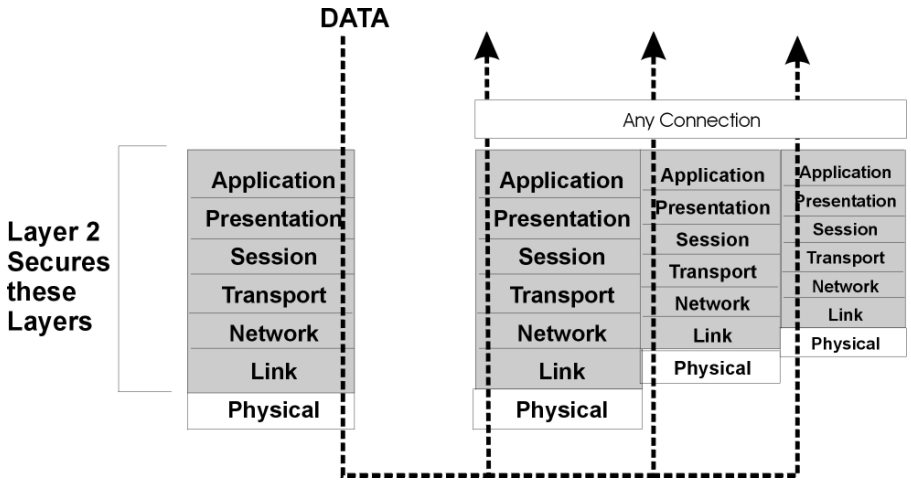
Three things must be in place to make any network environment secure: access control, privacy, and packet authentication/integrity.

- **Access control** is limiting the users who can gain access to the network. Access control can occur through any number of user authentication methods designed to verify that a user is who they claim to be and that they have network privileges. Once it is determined that users belong on the network, authorization may occur to determine what services they can have.
- **Privacy** is hiding information from those who shouldn't have it. Network transmissions are susceptible to casual browsing if the data packets aren't encrypted (encoded) so that the data is unintelligible to eavesdroppers. Encryption can be carried out at Layer 2 through 802.1X using secure key exchange, or at Layer 3 through the use of Virtual Private Networks (VPNs).
- **Authentication/Integrity** — Authentication, in this case, is verifying that devices (rather than users) are legitimate and that data packets originate from the source they claim to and have not been "spoofed" by a rogue network device using stolen credentials. Integrity is ensuring that packets have not been tampered with en route, even though they may have originated from a legitimate network device.

Link Layer Security with Wi-Fi Protected Access (WPA)

Link layer security provides point-to-point security between directly connected network devices. It 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 starts with an authentication service and includes link layer encryption and integrity services. Link layer protection secures wireless data only where it is most vulnerable, at the wireless link level and is characterized and allows higher-level protocols, such as IP, IPX, etc., to pass securely by providing security for **ALL** upper layer protocols.

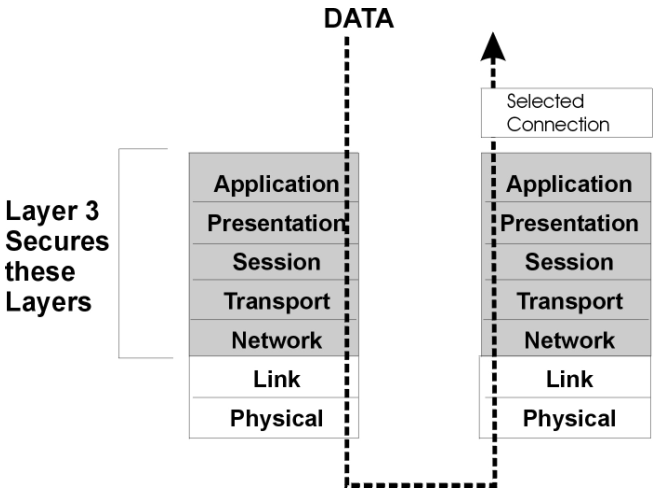


The industry recommended approach to Wi-Fi security incorporates link layer security through the 802.1X security standard. The IEEE 802.11i wireless security standard calls for 802.1X link layer security and has been adopted by the Wi-Fi Alliance in their Wi-Fi Protected Access (WPA) standard.

802.1X is the industry standard for providing strong link layer security to wireless LANs, and supports two authenticated key management protocols using the Extensible Authentication Protocol (EAP). 802.1X provides strong, robust security on wireless connections, and is used to eliminate the widely publicized security holes in older wireless LAN standards.

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. These services are only provided for specific network and transport layer services (e.g. for only IP traffic). Once the network endpoints are authenticated, IP traffic flowing between those endpoints is protected. However, all other non-IP traffic is not secured and is unprotected.



IPSec is a standard network layer security protocol that provides an extensible method to secure the IP network layer and upper layer protocols based on IP such as TCP and UDP. It is used extensively in Virtual Private Networks (VPNs) to secure network connections that extend between networks and to connect remote clients over the Internet. And while IPSec is a well-understood for providing security across wired network elements, it was not specifically designed for protecting non-IP traffic and data at lower layers in the network such as 802.11.

Why Link Layer Security is Important?

Deciding which layer of the network you should apply security needs some examination. 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.

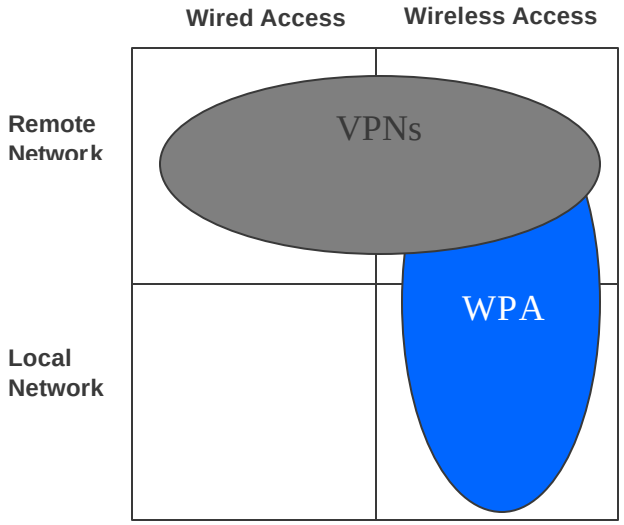
Link layer security such as 802.1X specifically operates on the data link layer to provide protection specifically for the over-the-air portion of the connection between the mobile user and wireless access point. 802.1X protects upper layer attacks by denying access to the network before authentication is completed.

VPNs and 802.1X are complement each other in Wi-Fi security applications. 802.1X provides strong, standards-level security for networks that are under the Carrier's or IT department's control.

Enterprises deploy 802.1X through a RADIUS server for user authentication to control access and encrypt data on their wireless networks. Some Carriers and service providers extend their dial-up and DSL connection services to include Wi-Fi access through 802.1X tied back to their centralized RADIUS servers as well. The value to 802.1X is best realized when access to the network can be controlled through a RADIUS server.

On the other hand, VPNs are best used in situations where Wi-Fi networks are not able to be secured. These are typically on remote networks such as public Wi-Fi hotspots that can't be secured at the link layer. In these cases, VPNs secure the IP services across the network. The user needs to be careful to limit their network access through the VPN tunnel, and avoid accessing unsecured portions of the open network.

In industries such as healthcare, financial services and certain government organizations, multiple layers of security may be deemed as offering the best solution. In this case, the best wireless security may be a combination of VPNs and 802.1X, combining both link and network layer security as shown below.



Shortcomings of Network Layer Security for Wireless LANs

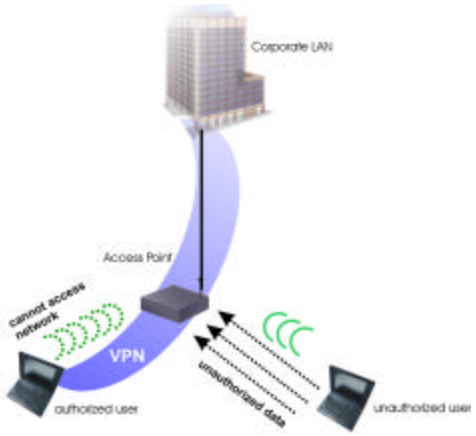
Although IPSec can be used to provide wireless LAN security, there are some drawbacks to using network layer security *alone* for securing the wireless LAN. The following four sections discuss the types of attacks that might be effective against a network layer IPSec solution.

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, the access point must bridge all traffic to the wired network. This allows legitimate users to authenticate and establish an IPSec connection, but also allows malicious users to send frames to the access point. Thus, an attacker can flood the access point with data, interrupting a legitimate user's connection.

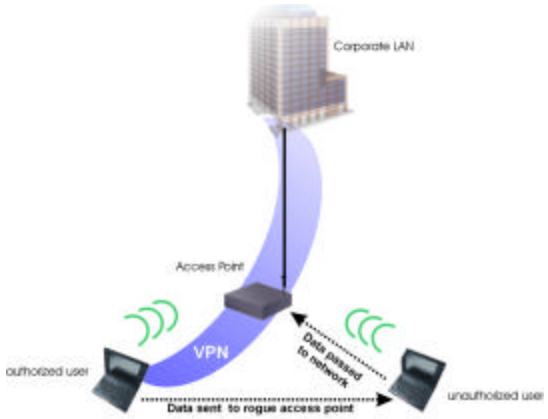
Another DOS attack could result when an attacker captures a previous disconnect message and re-sends it, resulting in the legitimate user's loss of connection to the WLAN.



Denial of Service Attack

Man-in-the-Middle Attack

As discussed earlier, IPSec does not 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

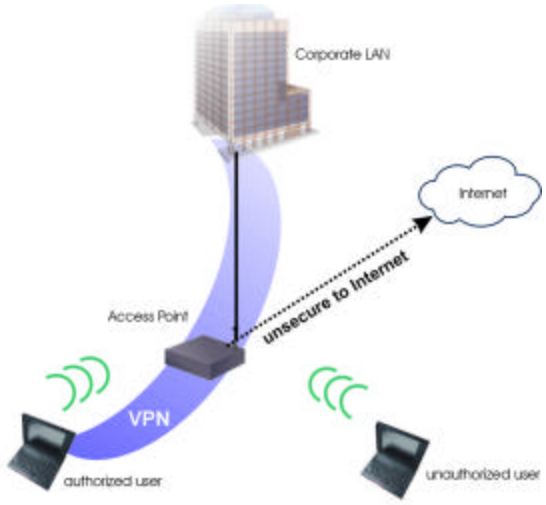
Peer-to-Peer Attack

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

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

802.1X Link Layer Security

802.1X is designed specifically for wireless networks, and provides users with data protection while allowing only authorized users to have access to the network. 802.1X not only overcomes the security vulnerabilities of WEP (an earlier, and unreliable wireless security solution), 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).

802.1X is a standards based solution, and an integral part of both the IEEE 802.11i and Wi-Fi Protected Access (WPA) standards. It works with most enterprise and Carrier level wireless network devices with delivering interoperability and reducing dependence on vendor-specific components. It provides effective link layer security, making wireless security sufficiently strong.

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.

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 security concerns that arise from wireless networks.

The link layer security provided by 802.1X is an essential component for wireless LAN security. As the Wi-Fi Alliance and IEEE recommend, 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. Link layer security used in conjunction with VPNs provide a double layer of security to meet the needs of the most security conscious organizations.

Interlink Networks delivers the most powerful, robust, and scalable RADIUS server solutions on the market. Since 1991, our RAD-Series Servers have provided access management solutions to some of the largest Carrier and Service Providers around the world.

Interlink Networks, LLC.
2500 Packard Rd, Suite 202
Ann Arbor, MI 48104

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