Wireless Security and VPN

Why VPN is Essential for Protecting Today's 802.11 Networks

Contents

Poised for Growth

Over the past few years, the benefits of wireless networking to businesses have become clear, ranging from lower costs to increased productivity. For example, laptop users can stay connected as they move throughout the corporate campus, easily tapping into the resources of the wired network. Busy field sales people can access the corporate LAN from airport or hotel access areas, greatly increasing productivity. Many analysts believe the wireless market segment has now reached a "critical mass" where rapid growth is imminent.

The wireless vision contemplates continuous, trusted connectivity for a wide range of client devices including PCs, PDAs (Personal Digital Assistants), phones, printers and more, with seamless hand-offs between LANs and WANs. The rapid development of mobile applications is already helping to drive this vision.

According to eWeek Magazine, 802.11 will end up as the "GPS of the next decade" – that is, a technology invented for a limited purpose that mushrooms into a huge range of applications (eWeek, 2001). The market value of WLANs is forecast to approach $2 billion by the end of 2001 and more than double to almost $5 billion by 2005 (Frost & Sullivan, 2001).

With this enormous usefulness and value at stake, it is vital that WLAN communications be adequately protected from security threats, both today and in the future.

Abstract

Wireless networks are now becoming widely deployed, and manufacturers have accelerated the development of low-cost, interoperable products. Today's 802.11 wireless technology promises to open up exciting new possibilities. However, as WLANs become more numerous and widespread, more robust security solutions are required.

In particular, recent demonstrations of the vulnerability of the RC4* cipher, which forms the basis for Wired Equivalent Privacy (WEP) encryption, make it clear that WEP protection alone is inadequate. A robust and scalable security solution is available by using Virtual Private Network (VPN) technologies.

This paper examines current wireless security methods and also looks at the use of VPN to augment wireless security. At the end of the paper are sources for further information.

Wireless Technology Today

What is wireless networking?

A Wireless Local-Area Network (WLAN) uses radio frequency technology to transmit and receive data over the air, providing all the features and benefits of traditional LANs but without the limitations of a cable. Most WLANs today use the 2.4GHz (Gigahertz) frequency band (802.11b), and technology using the 5GHz band (802.11a) is rapidly emerging.

Two main types of links form the basis of the wireless network:

Interface Cards

In a WLAN, NICs provide the interface between the network operating system and an antenna to create a transparent wireless connection to the network.

Access Points

The Access Point (AP) is the wireless equivalent of a hub. An AP is typically connected with the wired LAN backbone through a standard Ethernet cable, and communicates with wireless clients by means of an antenna.

The IEEE 802.11 standard has emerged as the predominant standard for WLANs. Any LAN application, network operating system or protocol, including TCP/IP, will run on 802.11-compliant WLANs as easily as they run over wired Ethernet. In fact, WECA (Wireless Ethernet Compatibility Alliance) is now defining high-rate 802.11b as wireless Ethernet.

Security measures

To safeguard information traveling on WLANs, the 802.11 standard specifies three basic methods of securing access to wireless APs:

Service Set Identifier (SSID)

The SSID allows a WLAN to be segmented into multiple networks, each with a different identifier. For example, a building might be segmented into multiple networks by floor or department. Each of these networks is assigned a unique identifier, which is programmed into one or more APs – each network can consist of multiple APs. To access any of the networks, a client computer must be configured with the corresponding SSID identifier for that network. Thus, the SSID acts as a simple password, providing a measure of security. A weakness is that the SSID is widely known and shared.

Media Access Control (MAC) address filtering

To increase security, each AP can be configured with a list of MAC addresses associated with the client computers that are allowed access to the AP. If a client's MAC address is not on the list, the AP will deny access. This method provides good security but is only suited to small networks. The labor-intensive work of entering MAC addresses and maintaining up-to-date lists on all of the AP devices obviously limits the scalability of this approach.

Wired Equivalent Privacy (WEP)

To minimize the risk of RF interception by someone nearby – for example, in the building's parking lot – WEP is specified for encryption and authentication between clients and APs according to the 802.11 standard. WEP security is based on an encryption algorithm called RC4 from RSA Data Systems. The encryption algorithm is generated based on a key (a number sequence) entered and controlled by the user. All clients and APs are configured with the same key to encrypt and decrypt transmissions. WEP keys are 40 or 128 bits in length.

An AP can be set up to provide encryption-only protection in open-system mode, or to add authentication in shared-key mode. MAC address filtering is often used together with this encryption (Figure 1). WEP security is best suited for small networks, as there is no key management protocol. As a result, keys must be manually entered into every client. This is a huge management task, especially since the keys should be changed regularly to provide an extra measure of security.

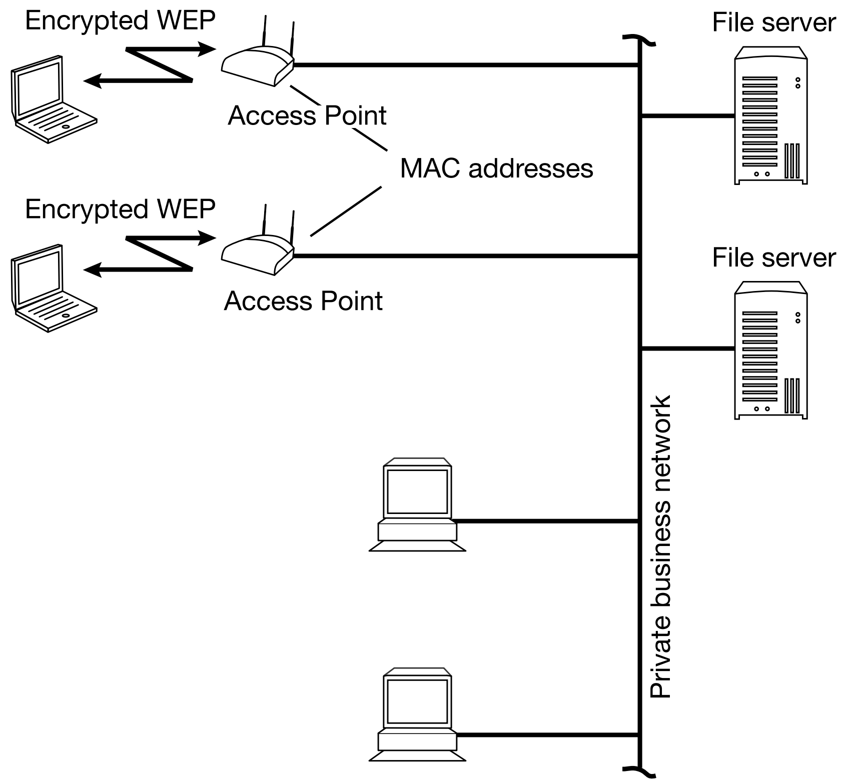

Figure 1. WEP Security with MAC Address Filtering

Vulnerability of RC4*

Recently, a paper written by three of the world's foremost cryptographers demonstrated the vulnerability of the RC4 cipher (Electronic Engineering Times, 8/2001). The attack used weaknesses in the key-scheduling algorithm of RC4 to obtain the network key. This new report shows that anyone with a wireless laptop, plus software that is readily available from the Internet, can now gain access to a WLAN in less than 15 minutes. WEP protection alone is clearly inadequate.

This is a serious blow to efforts at strengthening current security methods. Industry efforts had focused on developing a 128-bit key for WEP, which would have been a significant improvement over today's 40-bit key. The new security threat scales linearly.

RC4 is based on a cipher stream sequence, and this stream sequence contains the inherent weaknesses that proved to be devastating in the recent attack. Another approach, which uses a block sequence, is substantially more difficult to crack. Cipher block sequences are used in today's VPN solutions, and that is why VPNs offer the ideal security solution for WLANs today.

Virtual Private Networking (VPN)

This technology makes it possible for users on an un-trusted network to connect to a private network in an easy and secure manner. For business networks, a VPN solution for wireless access is currently the most suitable alternative to WEP and MAC address filtering.

VPNs are already widely used for intranets and remote access. They employ various industry-standard security mechanisms to safeguard data and ensure that only authorized users can access the network.

IPSec (Internet Protocol Security), as defined by the IEEE, is the most widely used mechanism for securing VPN traffic. IPSec can use DES, 3DES and other bulk algorithms for encrypting data, keyed hash algorithms (HMAC, MD5, SHA) for authenticating packets, and digital certificates for validating public keys. VPNs also support a variety of user authentication methods such as RADIUS, SecureID and digital certificates. These standards-based methods allow for easy integration into existing network infrastructures.

The IPSec protocol includes three principal security elements:

- **Authentication Header (AH) –** The AH provides authentication and integrity by adding authentication information to the IP datagram. This ensures that the data will not be available to an unauthorized station and will not be altered en route.

- **Encapsulation Security Payload (ESP)** – The ESP provides confidentiality. It can also provide integrity and authentication, depending on the algorithm used. With the ESP in use, part of the ESP header itself and all data contained in the datagram is encrypted. Tunnel or transport modes are available, with tunnel mode being the choice for remote access.
- **Internet Key Exchange (IKE)** – This is the key management protocol that is used to negotiate the cryptographic algorithm choices to be employed by the AH and ESP. The mechanisms used in IKE provide for an extremely scalable solution. The Diffie-Hellman algorithm also plays an important role in ensuring that the keys are exchanged securely.

The right solution

The combination of VPN (IPSec) and 802.11 is an ideal solution for today's wireless networking security needs. With this solution, the wireless APs are configured for open access with no WEP encryption, and the VPN handles security. The VPN servers provide encapsulation, authentication and full encryption over the WLAN. The result: you have fully protected, transparent access to network resources.

Since VPN servers can be centrally managed, administrative overhead is low. And unlike WEP with MAC address filtering, VPN solutions are scalable to a very large number of users. Furthermore, many organizations will already have VPN deployed on their enterprise networks, so extending these solutions to the WLAN should be easier and more economical.

The VPN approach is flexible enough to be used in a variety of different scenarios, all with the same user login interface and procedure (Figure 2):

- Using their dial-up, cable modem or Digital Subscriber Line (DSL) connection to the Internet, remote workers can establish a connection to the VPN server and WLAN.
- Public wireless access areas in airports and other locations can be used to establish a VPN connection back to the WLAN.
- On-campus 802.11 wireless access can be implemented by means of a VPN connection.

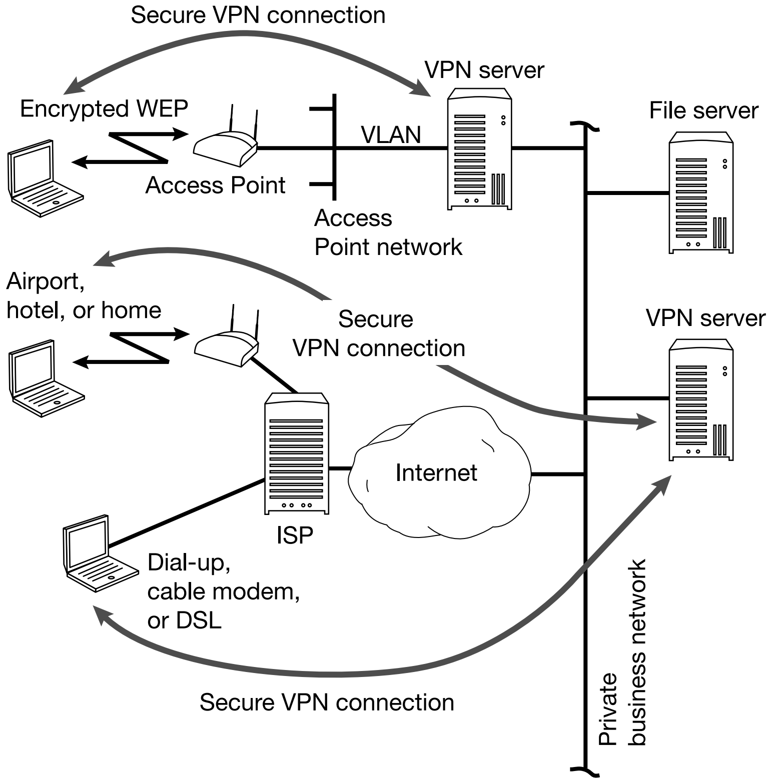

Figure 2. VPN Security for 802.11 WLANs

Conclusion

The future of wireless security

The IEEE is currently working on a new standard, 802.1x, for port-based authentication on wireless (and wired) networks. Instead of requiring a specific protocol for authentication, 802.1x specifies EAP, an encapsulation protocol that allows various authentication methods such as RADIUS*, Kerberos* and Secure IDs* to be used. AES, which is a new encryption algorithm, and TLS, which provides application security, are also recommended in 802.1x.

Some proprietary schemes are being promoted for authentication, but these have two serious drawbacks:

- They reduce the flexibility of WLAN solutions
- They lock the user into that specific vendor's infrastructure

A TGi (IEEE) solution, in which Intel plays an important role, will be forthcoming. But for now, without a complete standards-based solution, wireless 802.11 traffic is vulnerable to attack. And the best way to provide a complete, robust security solution is with VPN.

For More Information

For information about Intel's VPN solutions, see:

http://www.intel.com/network/connectivity/products/wireless.htm

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at anytime, without notice.

0402/OC/PP/PP/2.5K