WHITE PAPER

symantec™

Wireless LAN Security

Enabling and Protecting the Enterprise

INSIDE

INSIDE

- Wireless LAN Technology
- Benefits of Wireless LANs
- Security Risks and Technical Challenges
- Recommendations

Contents

Executive summary

Motivated by the need to reduce IT costs while increasing employee productivity, enterprise-wide wireless local area network (LAN) solutions are becoming increasingly viable. Proliferation of mobile computing devices has boosted employee demand for access to their organization's network beyond the tether of their office workstation. Meanwhile, accelerated wireless transmission rates and increasing vendor adherence to standards-based interoperability are enhancing the practicality of wireless LANs.

Yet the same wireless technologies that can erase the physical limitations of wired communications to increase user flexibility, boost employee productivity, and lower cost of network ownership also expose network-based assets to considerable risks. The security embedded in wireless LAN technologies falls short of providing adequate protection. Early-adopting organizations have found that evaluating, and where possible, mitigating these risks before deploying a wireless LAN is beneficial. This white paper summarizes wireless network security planning by providing an overview of the security risks and technical challenges in this area, as well as summarizing key recommendations for secure wireless LANs.

Wireless LAN Technology

In 1999, the Institute of Electrical and Electronics Engineers (IEEE) published standard 802.11, which specified a group of technologies governing wireless Ethernet connectivity between client devices—such as desktop computers, laptops, and personal digital assistants (PDAs)—and the wireless hubs connected to the physical network. Wireless LANs typically emulate the wired network's traditional hub-spoke configuration and comprise two primary components: a wireless network interface card (NIC) and an access point (AP). The 802.11 standard represents a significant step in electronic-data infrastructure evolution, which in the last ten years has proceeded from coax, token ring, and 10/100 BaseT Ethernet cabling to wireless radio transmissions.

The best known and most widely used variation of the 802.11 wireless LAN standard is 802.11b. Products conforming to the 802.11b standard are called "WiFi" (pronounced Y-Phi) for "wireless fidelity," so named by the Wireless Ethernet Compatibility Alliance (www.wi-fi.org). This alliance is an independent organization that promotes interoperability between 802.11b-based devices.

Under ideal conditions, WiFi products can receive and transmit data at speeds up to 11 Megabits per second (Mbps). However, in typical conditions, most WiFi devices operate at speeds between 1 and 5 Mbps.

Regarding security and 802.11b, transmission encryption—called Wired Equivalent Privacy (WEP)—has been incorporated into WiFi products. The goal of WEP is to provide a level of privacy (via the use of encryption) that is equivalent to wired LAN privacy, which is achieved via various physical security mechanisms. However, encrypted messages can be intercepted and decrypted. As vendors introduce new technologies and products, other security gaps are likely to be revealed. For more WEP security information, visit the UC Berkeley ISAAC Web site (www.isaac.cs.berkeley.edu) or the IEEE Web site (www.ieee.org).

IEEE and its member organizations are working to address many of these limitations and vulnerabilities. Efforts include new wireless LAN standards to increase security, bandwidth, and range, as well as reduce power consumption. For example, the 802.11a standard, scheduled for 2002 release, is expected to support speeds up to 54 Mbps. Visit the IEEE Web site for more information on upcoming wireless LAN standards.

Benefits of Wireless LANs

A traditionally wired 10/100 BaseT Ethernet LAN infrastructure for 100 people costs about US$15,000 and requires several days to install (see Figure 1). Enterprises that use such an arrangement also incur additional costs and disruptions with every change to the physical office. (Expenses vary according to the physical layout and the quality of the equipment used.) Conversely, wireless LANs are less expensive and less intrusive to implement and maintain, as user needs change.

SIMPLIFIED IMPLEMENTATION AND MAINTENANCE

Wireless APs can be placed in the ceiling, where they can accommodate a virtually endless variety of office configurations (see Figure 2). Wired LANs, in contrast, consume time and resources to run cables from a network closet to user's desktops and to difficult-to-service areas such as conference room tables and common areas. With a wired LAN, each additional user or modification to the floor plan necessitates adjustments to the cabling system.

EXTENDED REACH

Wireless LANs enable employees to access company resources from any location within an AP's transmission range. This flexibility and convenience can directly improve employee productivity.

INCREASED WORKER MOBILITY

The roaming benefits of wireless LANs extend across all industries and disciplines. The shop foreman can manage logistics from the warehouse as easily as office-based employees move about the building with their laptops or PDAs. And field sales employees can connect to public wireless LANs in coffee shops and airport lounges.

REDUCED TOTAL COST OF OWNERSHIP AND OPERATION

The cumulative benefits of simplified implementation and maintenance, an extended LAN reach, and the freedom to roam minimize expenses and improve organizational and employee productivity. The result is reduced total cost of ownership and operation.

Figure 1. Traditional 10/100 BaseT Ethernet Wired LAN

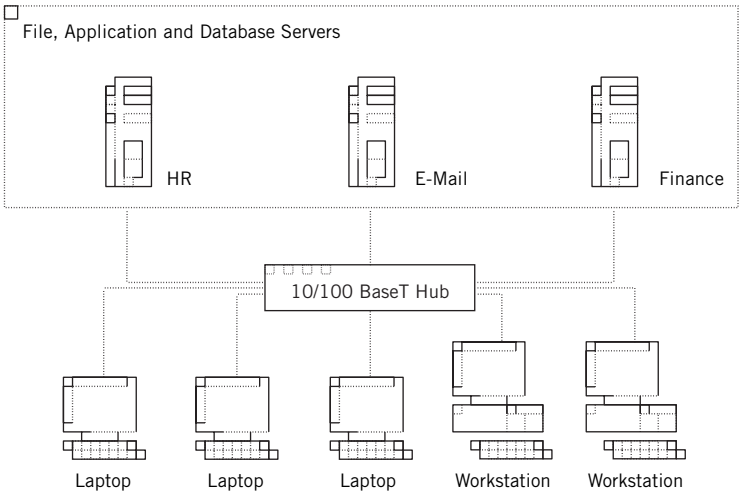
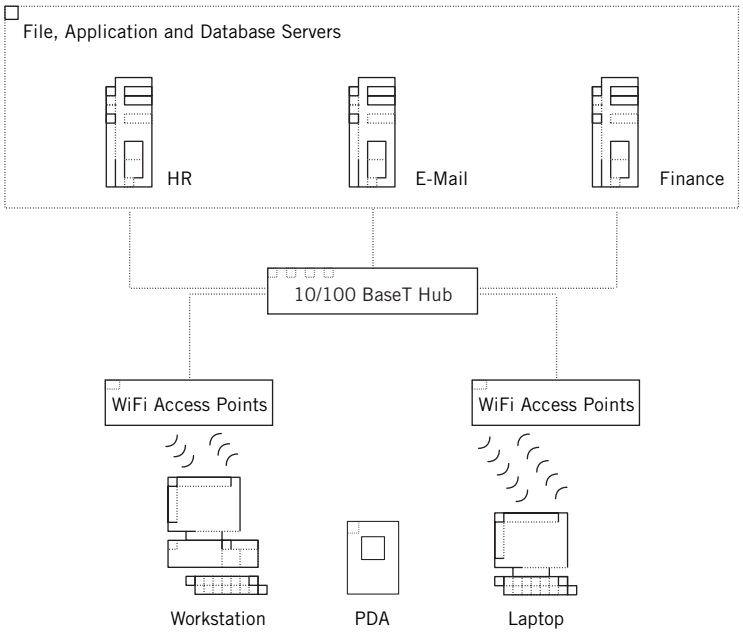


Figure 2. Typical Wireless LAN



Security Risks and Technical Challenges

Security is a principal consideration when planning, designing, implementing, and managing a network infrastructure. This is especially true for wireless LANs, which present a unique set of challenges to IT and security professionals. In addition to the typical problems that new network and device technologies engender, including incompatibilities and ongoing support issues, non-secure wireless LANs can expose an organization's network traffic and resources to unauthorized outsiders. Such individuals may capture data and exploit network-based resources, including Internet access, fax servers, and disk storage. More importantly, wireless access to a network can represent the entry point for various types of attacks, which can crash an entire network, render services unavailable, and potentially subject the organization to legal liabilities.

"LEAKY" BUILDINGS

Wireless LAN radio signals can extend beyond the intended perimeter and "leak" through the physical boundaries of a floor or building. As these transmissions seep into common, public, or private areas such as roads, parking lots, and other buildings, they may fall prey to "war driving" or a "drive-by hacking" attack. Using off-the shelf hardware and freely available Internet software, unscrupulous individuals can defeat WEP encryption capabilities and access corporate wireless data.

UNAPPROVED DEPLOYMENTS

Insiders, including employees and contractors, may choose "not to wait for the IT Department." They succumb to the low price and easy installation of WiFi starter kits (two wireless NICs and a WiFi Access Point), which can be purchased for about US$300 and set up with minimal technical know-how in under ten minutes. When unapproved technology is plugged into a corporate network, a number of challenges ensue, including end user and equipment support difficulties as well as potential disruptions to existing services.

Malicious outsiders who gain office physical access could quickly place an unobtrusive wireless AP in a conference room or lobby area. Such devices are easy to hide and simple to implement; history is replete with stories of such "bugs" even in supposedly secure foreign embassies. Operating from a nearby location, malicious outsiders can capture data, access company resources, and interrupt services.

EXPOSURE OF WIRELESS DEVICES

Many of today's laptops ship with embedded WiFi capabilities. Hackers can access a device's data and the organization's wireless LAN even if that particular device has never been used to send or receive wireless transmissions.

Most new machines, including gateway servers, do not ship with optimal security settings. The default settings are intended for easy installation and deployment, not for protecting assets.

SIGNAL INTERFERENCE

Walls, columns, and other building features can reduce signal strength between a wireless NIC and an AP, severely limiting a wireless LAN's range and connection quality. These problems may be mitigated with additional equipment. Other wireless technologies sharing the same public

spectrum—such as Bluetooth, cordless phones, and other wireless equipment—can also adversely impact transmission range and quality.

EVOLVING IEEE STANDARDS

Organizations contemplating a wireless LAN deployment can choose to implement an 802.11b-based wireless LAN today, or wait for upcoming variations, which are intended to address performance and security issues. IEEE and its workgroups are continually defining and refining standards in light of emerging needs and perceived weaknesses in existing technologies. To the extent that vendors' 802.11 implementations deviate from the various IEEE standards, their equipment can create interoperability challenges.

Recommendations

Even as new 802.11 vulnerabilities are identified and exploited, organizations can mitigate or eliminate many of wireless LAN's security risks with careful education, planning, implementation, and management. The following steps aid this process:

- Establish wireless LAN security policies and practices
- Design for security
- Logically separate internal networks
- Enable VPN access only
- Remove unnecessary protocols
- Restrict AP connections
- Protect wireless devices.

ESTABLISH WIRELESS LAN SECURITY POLICIES AND PRACTICES

The cornerstone of an effective wireless LAN strategy involves defining, standardizing, documenting, disseminating, and enforcing wireless LAN security policies and practices. These include specifying the make, model, configuration, and settings of the wireless LAN equipment authorized for use, as well as documenting and managing the APs and connected network infrastructure.

Employee education increases awareness of security risks. Some employees may not realize that deploying an unauthorized wireless LAN or using a WiFi product "out of the box" may increase security risks. Clear and frequently conveyed guidelines usually promote active cooperation.

DESIGN FOR SECURITY

When placing wireless APs for strategic coverage, installers should consider signal bleed into uncontrolled areas where transmissions can be intercepted. Wireless coverage should be implemented only where needed.

LOGICALLY SEPARATE INTERNAL NETWORKS

The LAN segments that connect to wireless APs should connect to a corporate Virtual Private Network (VPN) gateway, but not directly to the production network. Eliminating APs from the production network minimizes the risk of attack techniques such as packet sniffing.

ENABLE VPN ACCESS ONLY

Requiring users to connect to the wireless LAN via a VPN is recommended. Once authenticated, authorized users communicate using an encrypted tunnel between the connecting device and the LAN, reducing the risk that a transmission will be captured.

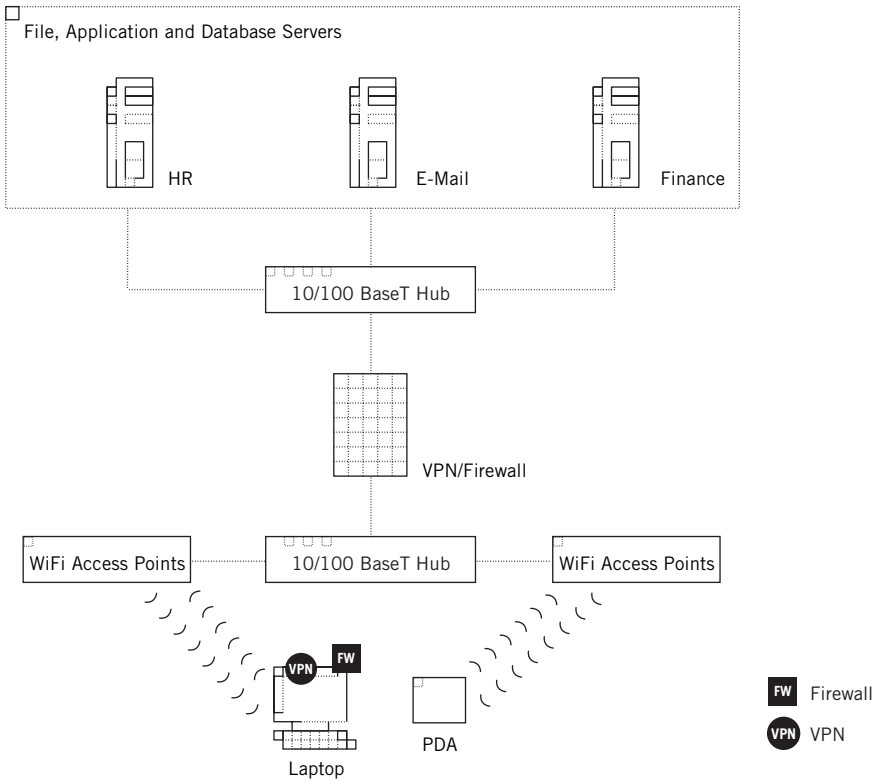
RESTRICT UNNECESSARY PROTOCOLS

Restricting unnecessary or redundant protocols from the LAN segments that connect the APs to the VPN gateway reduces the possibility of unidentified holes and vulnerabilities. Retaining the Domain Name System (DNS) and IP Security (IPSec) protocols is recommended to support the VPN.

RESTRICT AP CONNECTIONS

Administrators can use authorization tables to selectively enable LAN connections only to devices with approved NIC addresses. Each NIC has a unique address that can be added to a table of authorized users; most vendors' APs support Media Access Control (MAC) restrictions through the use of authorization tables. As a result, instead of editing each AP individually, APs can be pointed to a centrally managed database.

Figure 3. Recommended configuration of wireless LAN



PROTECT WIRELESS DEVICES

Personal firewalls can protect individual devices from attacks launched via the "air connection" or from the Internet. IT administrators should disable all unused features of new client devices (e.g., shared drive access) and reconfigure default settings according to the organization's particular needs.

Conclusion

Like most advances, wireless LANs pose both opportunities and risks. The technology can represent a powerful complement to an organization's networking capabilities, enabling increased employee productivity and reducing IT costs. To minimize the attendant risks, IT administrators can implement a range of measures, including establishment of wireless security policies and practices, as well as implementation of various LAN design and implementation measures. Achieving this balance of opportunity and risk allows enterprises to confidently implement wireless LANs and realize the benefits this increasingly viable technology offers.

Glossary

802.11: Broad heading for IEEE wireless LAN focus groups

802.11a: Improves 802.11 bandwidth to 5 GHz

802.11b: Wireless LAN standard for up to 11 Mbps at 2.4 GHz

Access Point: (AP), wireless network hub

Bluetooth: Short-range wireless technology developed by the Bluetooth Special Interest Group (www.bluetooth.org)

IEEE: Institute of Electrical and Electronics Engineers (www.ieee.org)

Ethernet Hub: A connection point between devices on a network

LAN: Local Area Network

MAC: Media Access Control

NIC: Network Interface Card

PDA: Personal Digital Assistant

VPN: Virtual Private Network

WiFi: 802.11b wireless Ethernet standard

WEP: Wired Equivalent Privacy

References

1. Nikita Borisov, Ian Goldberg, and David Wagner, UC Berkeley, "Security of the WE Algorithm," (http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html)
2. Wayne Caswell, "Wireless Home Networks: Disconnected Connectivity," Home Toys, April 2000 (http://www.hometoys.com/mentors/caswell/apr00/wireless.htm)
3. Joel Conover, "Wireless LANs Work Their Magic," Networking Computing, July 2000 (http://www.networkcomputing.com/1113/1113f2full.html)
4. Joel Conover, "First Things First—Top 10 Things to Know About Wireless," Networking Computing, July 2000 (http://www.networkcomputing.com/1113/1113f2side2.html)
5. John Cox, "LAN Services Set to Go Wireless," Network World, August 20, 2001 (http://www.nwfusion.com/news/2001/0820wireless.html)
6. Andy Dornan, "Emerging Technology: Wireless LAN Standards," 2/6/02, NetworkMagazine.com (http://networkmagazine.com/article/NMG20020206S0006)
7. Dale Gardner, "Wireless Insecurities," Information Security magazine, January 2002 (http://www.infosecuritymag.com/articles/january02/cover.shtml)
8. IEEE Working Group for WLAN Standards (http://grouper.ieee.org/groups/802/11/index.html)
9. Dave Molta, "The Road Ahead for Wireless," Network Computing, July 9, 2001 (http://www.networkcomputing.com/1214/1214colmolta.html)
10. Practically Networked, "Wireless Encryption Help" (http://www.practicallynetworked.com/support/wireless_encrypt.htm)
11. Practically Networked, "Securing Your Wireless Network" (http://www.practicallynetworked.com/support/wireless_secure.htm)
12. Practically Networked, "Mixing WEP Encryption Levels" (http://www.practicallynetworked.com/support/mixed_wep.htm)
13. Practically Networked, "Should I Use NetBeui?" (http://www.practicallynetworked.com/sharing/netbeui.htm)
14. Peter Rysavy, "Break Free with Wireless LANs," Network Computing, October 29, 2001 (http://www.networkcomputing.com/1222/1222f1.html)
15. Search Networking.com, Wireless LAN links (http://searchnetworking.techtarget.com/bestWebLinks/0,289521,sid7_tax286426,00.html)
16. Vicomsoft Wireless Networking Q&A (http://www.vicomsoft.com/knowledge/reference/wireless1.html)
17. "Wireless Within Corporate Reach" eWeek, May 3, 2000 (http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2530201-1,00.html)

SYMANTEC, THE WORLD LEADER IN INTERNET SECURITY TECHNOLOGY, PROVIDES A BROAD RANGE OF CONTENT AND NETWORK SECURITY SOFTWARE AND APPLIANCE SOLUTIONS TO INDIVIDUALS, ENTERPRISES AND SERVICE PROVIDERS. THE COMPANY IS A LEADING PROVIDER OF VIRUS PROTECTION, FIREWALL AND VIRTUAL PRIVATE NETWORK, VULNERABILITY ASSESSMENT, INTRUSION PREVENTION, INTERNET CONTENT AND EMAIL FILTERING, AND REMOTE MANAGEMENT TECHNOLOGIES AND SECURITY SERVICES TO ENTERPRISES AND SERVICE PROVIDERS AROUND THE WORLD. SYMANTEC'S NORTON BRAND OF CONSUMER SECURITY PRODUCTS IS A LEADER IN WORLDWIDE RETAIL SALES AND INDUSTRY AWARDS. HEADQUARTERED IN CUPERTINO, CALIF., SYMANTEC HAS WORLDWIDE OPERATIONS IN 38 COUNTRIES.

FOR MORE INFORMATION, PLEASE VISIT WWW.SYMANTEC.COM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
1.408.253.9600
1.800.441.7234

www.symantec.com

For Product Information
In the U.S., call toll-free
800-745-6054.

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.