Understanding Wireless LAN Security

A Comprehensive Solution through the ReefEdge Connect System

Overview

All signs point to the enterprise of the future as being one in which every laptop, handheld device, and desktop PC is connected wirelessly to the corporate network. Today, enterprises are rapidly deploying in-building wireless networks based on standards such as 802.11b, which offers constant access to enterprise intranet, extranet, and Internet data and services. Compared to traditional wired networks, in-building wireless networks offer mobility, giving users access to enterprise data anywhere and anytime; flexibility, reducing deployment and network reconfiguration costs; and convenience. Within the workplace, these innate benefits foster a mobile workforce that can collaborate more easily, be productive within flexible office configurations, and travel between buildings in a campus environment or across office sites worldwide. Consequently, wireless LANs have become the preferred method of connecting users within the enterprise environment.

Like any new network access technology, wireless LANs raise new concerns, the greatest of which is security. Network managers must ensure that new vulnerabilities are not introduced to the corporate network when a wireless LAN is deployed. At the same time, they must ensure that wireless transmissions are safe from eavesdropping. Finally, while enforcing security, network managers must preserve the simplicity, ease-of-use, and performance promised by the wireless LAN; when faced with burdensome security procedures, end users will naturally seek ways to simplify their use.

At first glance, the security challenge seems insurmountable. In response, some network managers have suggested that the best way to address such concerns is to simply remove the wireless LAN. Unfortunately, this is an impractical approach; end users will continue to demand the convenience and productivity afforded by wireless LANs. Instead, network managers need to deploy layered solutions that systematically address the security issues.

In this paper, we provide an overview of the security concerns introduced by wireless LANs, current approaches to wireless LAN security, their limitations, and the weaknesses of various “band aid” security solutions. We conclude by describing how

the ReefEdge Connect System provides a comprehensive solution to wireless LAN security.

Wireless LAN Security Concerns

From a security point of view, wireless LANs represent a new method for accessing the enterprise network. In much the same way that enterprise network managers have previously faced the challenges of securing local LAN access, remote LAN access from the Internet, and remote LAN access from cellular networks, network managers must consider the new challenges introduced by LAN access from an in-building wireless LAN.

Wireless LAN deployments raise a number of security concerns. Possible security threats include unauthorized use of the network, eavesdropping on transmitted data traffic, and denial of service attacks.

While these threats are present in traditional LANs, the wireless environment exacerbates these concerns significantly:

1. **Broad network exposure**. Wireless LAN range and signal propagation are largely uncontrollable, so potential intruders on the LAN need not be physically located within an enterprise's premises; 802.11b networks easily reach out into the parking lot and may even provide wireless coverage to people driving along nearby streets.[i] This concern is particularly relevant in shared office buildings.

2. **Invisible intruders.** Even within an enterprise, wireless LAN intruders can operate inconspicuously because they do not need a physical connection to the network. With the emergence of handheld devices capable of communicating over 802.11b networks, the inability to monitor user actions is of even greater concern.

3. **Guest access.** Guests and visitors increasingly expect enterprises to offer Internet access, in the same way that they ask to borrow the telephone or fax machine today. Many guests have wireless LAN-enabled laptops and handheld devices, and they seek to access the Internet using this equipment. Unfortunately, offering this access typically involves granting non-employees use of the corporate LAN.

4. **Rapid technology evolution.** Wireless LAN technologies are relatively new. The security mechanisms provided by these standards are untested, and the standards are evolving rapidly. Moreover, in the near future, enterprises will likely face heterogeneous wireless LANs encompassing multiple radio standards, including 802.11b, 802.11a, 802.11g, HiperLAN2, Bluetooth, and 802.15. Managing security in such rapidly evolving,

heterogeneous wireless LAN environments represents a considerable burden.

These security issues represent a significant challenge to IT managers who are considering the deployment of in-building wireless networks within the enterprise.

Overview of Wireless LAN Security Approaches

Current 802.11b networks define standards for encrypting data that is transmitted over the air. Data encryption prevents eavesdropping by other wireless network users. Encryption is typically implemented within the wireless hardware at each mobile device and each access point to deliver performance that can keep up with data transmission rates.

However, the standard 802.11b security mechanisms do not meet the needs of enterprise wireless LAN deployments due to their reliance on global keys. Global keys complicate management of large-scale systems, because their encryption algorithms are vulnerable to attack, and because they do not address the authentication and access control requirements of an enterprise environment. Attempts to address these issues have met with limited success, as they complicate systems management and increase cost without actually delivering security for the wireless LAN.

Wired Equivalent Privacy (WEP)

The 802.11b standard defines an encryption algorithm known as Wired Equivalent Privacy (WEP),[ii] which relies on the RC4 cryptographic process.[iii] WEP employs a 40-bit or 104-bit secret key that is shared by the wireless client and the access point. During packet transmission, a checksum is appended to the data, a 24-bit Initialization Vector (IV) is chosen at random and appended to the WEP key to form a 64-bit or 128-bit encryption key, and the data and checksum are encrypted using that encryption key. During packet reception, the Initialization Vector (IV) is retrieved from the packet, the WEP key and IV are combined to reconstruct the encryption key, the packet is decrypted using that key, and the checksum is verified. The Appendix to this paper provides a more detailed description of the WEP encryption algorithm.

The WEP key also forms the basis for a mutual authentication scheme that allows the access point to authenticate mobile clients before they are granted access to the wireless network. When a mobile client first registers with an access point, the access point issues a challenge. The client uses the WEP key to compute a valid challenge response, and upon receiving this valid response, the access point is assured that the client is a valid network user. (The mutual authentication exchange is then reversed, so the mobile client can be sure that it is communicating with a valid access point.)

WEP encryption and authentication rely on an out-of-band distribution of the shared secret key to the access point and wireless client. Traditionally, the WEP key has been distributed manually to all clients, but, as described later in this paper, newer systems generate a shared WEP key dynamically when a client connects to the access point.

Limitations of Wireless LAN Security

Though widely deployed, existing security technologies in wireless LAN environments introduce many problems within enterprise environments:

1. Reliance on global keys complicates systems management and introduces additional security exposures.

2. Insecure encryption algorithms leave the wireless LAN vulnerable to attack.

3. Limited access control and filtering capabilities prevent control of network usage.

Global Key Management

In most 802.11b networks today, the access point uses a single WEP key that is shared by all authorized mobile clients. In an enterprise environment, the integrity of the global WEP key is almost impossible to maintain, so WEP's security promise cannot be fulfilled.

First, the WEP key cannot realistically be kept secret. The global WEP key must be programmed into all authorized client devices, because that WEP key is used to grant access to the wireless network. Though an IT department conceivably could take responsibility for configuring all clients with this WEP key, this approach is impractical in anything but the smallest deployments. Instead, the WEP key must be disseminated to users, who individually enter it into their client devices; the same WEP key must be made available to guest users. Having distributed the key in this fashion, the IT manager can no longer assume that it is secret.

Second, key management is essentially impossible in this environment. The burden of changing the WEP key is significant, because it involves updating the configuration of all client devices and all access points. It is unrealistic to expect such a key update to occur in an organized fashion, particularly within a large enterprise. Once a WEP key is established, it is likely to stay.

Third, because any client device configured with the WEP key can connect to the wireless LAN, IT managers cannot block unauthorized users from gaining network access. For example, misplaced or stolen devices are likely to have the WEP key programmed into their configuration. Former employees who have recorded the WEP key can easily obtain new hardware and configure it with the key. To get temporary access to the enterprise network, guests will have programmed the WEP key into their own devices. Any of these unauthorized users may gain access to the corporate wireless network from any location having wireless network coverage—even from outside the company's offices.

Overall, WEP is so difficult to configure and manage that most 802.11b deployments do not use it at all![iv] A similar situation exists with Bluetooth networks, in which a shared key must be established between all clients and all access points. The

natural approach is to either rely on a single global key or to simply turn off encryption entirely.

Insecure Algorithms

The WEP mutual authentication and encryption algorithms have significant flaws that make them inadequate for securing enterprise environments.

Researchers from the University of Maryland have discovered that by eavesdropping on 802.11b traffic, an intruder can obtain enough information to generate valid challenge responses during the mutual authentication process *without actually obtaining the WEP key*.[v] As a result, an intruder can successfully gain access to an 802.11b network as a valid user.

Other work by researchers at Intel Corporation, the University of California Berkeley, Cisco Corporation, and the Weizmann Institute has revealed flaws in the WEP encryption and checksum algorithms.[vi,vii,viii]

The problems arise for three reasons:

- The WEP algorithm selects a new encryption key on every packet, but flaws in the key selection algorithm limit the value of this mechanism; this weakness enables an attacker to analyze encrypted traffic and recover the data even though the encryption key is changing. This situation arises for two reasons. First, regardless of the WEP key length, the WEP algorithm only selects from a limited number of actual encryption keys. In particular, because only 2^{24} Initialization Vector values are available, only 2^{24} encryption keys are possible for a particular WEP key value of any length. Second, all of the encryption keys have a similar structure because they are derived from a common WEP key. In particular, all of the encryption keys share the same 40-bit or 104-bit WEP key prefix and differ only in the 24-bit Initialization Vector suffix.

- The RC4 cryptographic algorithms underlying WEP have a significant proportion of “weak keys” which, when used, make the encrypted data particularly vulnerable to attack. In other protocols that use RC4, this flaw is not a major issue because the likelihood of selecting a weak key is minimal. However, the WEP algorithm, which generates a new encryption key for each packet by randomly generating an Initialization Vector, cycles through these weak keys frequently.

- The WEP checksum (CRC) and encryption (RC4) algorithms rely on the same computational processes; consequently, an attacker who modifies the content of an encrypted packet can also calculate how to modify the packet so that it still presents a valid checksum. Intruders therefore can modify packet transmissions without being detected. This insidious attack allows an intruder to disrupt communication or, worse, interject false information into the data stream undetected. Furthermore, an intruder can exploit the checksum weaknesses to

launch so-called “known plaintext” attacks on the WEP encryption by generating erroneous requests that solicit known responses from a server.

By listening to the 802.11b network and analyzing encrypted data relative to well-known network protocol patterns, an intruder can obtain enough information to reconstruct the full set of encryption keys used by clients and access points in the wireless network.

Limited Access Control and Filtering

The wireless LAN standards provide inadequate access control to the wired network. Network access control relies on possession of the WEP key, but once a device is authorized, it gains full access to the entire network. There is no information about who is actually using the device, whether that user should be able to access the network, and, if so, what data that user should be allowed to access. This situation is particularly problematic when trying to offer network access to guest users, whose access would ideally be restricted to the Internet or selected intranet or extranet hosts.

Some access point implementations enable an IT manager to register a list of client MAC addresses that may gain access to the network. The access point only grants access to devices that transmit using one of the registered MAC addresses. However, these filters still do not identify who is using the device and what that user is authorized to do. In addition, these filters are difficult to administer, rely on careful asset tracking to account for lost or stolen devices, and are not conducive to an environment that supports guest or other temporary access.

Attempts to Address Wireless LAN Security Weaknesses

Wireless equipment vendors and enterprise IT departments have made several attempts to address some of these security concerns. However, these solutions do not address all of the security requirements of an enterprise wireless LAN deployment. Moreover, these approaches significantly increase the overall cost of the wireless LAN system. They require the purchase of multiple system components, which are expensive to configure, deploy, administer, and maintain. Finally, many of these approaches introduce proprietary or non-interoperable extensions to the 802.11b standard.

Dynamic WEP

To improve the security provided by WEP, many access point vendors have introduced mechanisms for dynamically assigning WEP keys to clients when they start communicating with an access point; some implementations will eventually support periodically changing the WEP key while the device is using the wireless LAN. These Dynamic WEP solutions eliminate the need for distributing and

managing a global WEP key at every client. By changing the WEP key frequently, Dynamic WEP reduces the amount of traffic that is transmitted with a particular WEP key and therefore limits the amount of data available to an intruder launching a cipher attack.

However, Dynamic WEP does not address the underlying security problems with the WEP standard—namely, that given enough encrypted traffic (approximately 1,000,000 packets[ix]), an attacker can crack the key. Therefore, with WEP, the situation is simply a race between how quickly the attackers can break the WEP keys and how quickly the network manager changes them. Current recommendations call for WEP key regeneration after every 10,000 packets, which, even with normal network use, can easily occur within 30 seconds. As additional WEP vulnerabilities are exposed and as client processing power increase, the WEP key change rate must increase in lockstep.

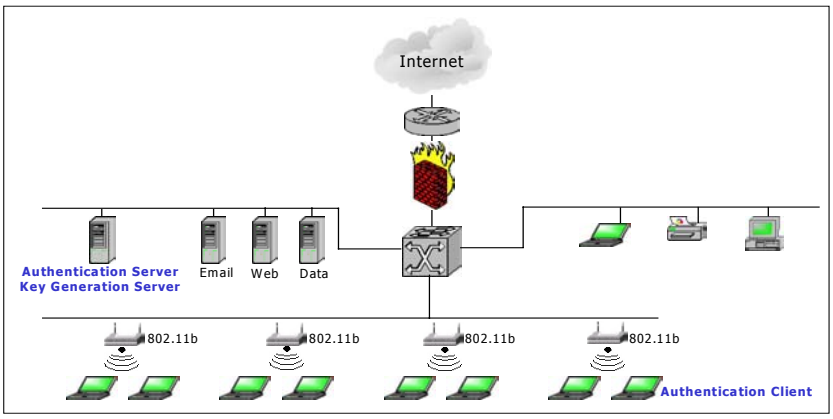
Today, Dynamic WEP solutions introduce other problems for network managers.

First, most of these solutions rely on proprietary mechanisms, therefore requiring that client hardware, access points, and authentication services come from a single vendor. Consequently, the solution is not cost-effective, limits future expansion of the wireless deployment, and is impractical to maintain. With the emergence of interoperable 802.11b equipment, enterprises are looking to select system components based on price and feature comparisons; single vendor solutions can be more expensive and can block access to the most advanced equipment on the market. Furthermore, as manufacturers begin to embed 802.11b into laptops, PCs, and PDAs, enterprises cannot guarantee that a single-vendor environment will prevail. Similarly, guest users cannot be forced into using client hardware from a particular manufacturer.

Second, Dynamic WEP does not address the security and management issues that emerge in an enterprise using multiple short-range radio technologies. A recent Mobile Insights poll of Fortune 500 IT executives revealed that 36% planned to support at least two radio technologies and an additional 21% were undecided.[x] To protect their wireless LAN investment, enterprises must deploy infrastructure that can easily extend to 802.11a, 802.11g, HiperLAN2, Bluetooth, 802.15, and other wireless standards as they emerge. The infrastructure must even enable integration with wide-area wireless access.

802.1x, EAP, and LEAP

Dynamic WEP solutions are usually combined with an implementation of the IEEE 802.1x standard, which provides for user authentication before granting network access. The user authentication process uses the *Extensible Authentication Protocol (EAP),*[xi] which enables a wide variety of actual authentication mechanisms. Cisco has developed a proprietary form of EAP, known as *Lightweight Extensible Authentication Protocol (LEAP),* that combines user authentication and Dynamic WEP key generation.



When the client first connects to a wireless LAN access point that supports 802.1x, the access point sends to the client a challenge. The client identifies itself, and, through the exchange of EAP messages, the access point brokers an authentication handshake (typically transmitting a user name and password) between the client and an external authentication server. Once the authentication server signals a successful authentication, the access point grants network access to the client. With Cisco's LEAP, the authentication server generates a WEP key for the session and delivers it to both the access point and the client.

The 802.1x authentication addresses enterprises' need to identify wireless LAN users instead of relying solely on the client's MAC address, as is required in today's 802.11b networks. It also provides a mechanism, enforced at the access points, for only granting authorized users access to the wireless LAN.

However, 802.1x does not address most of the enterprise security requirements:

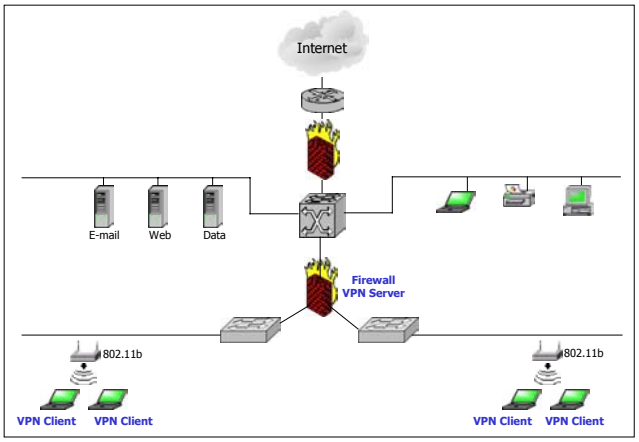
- The 802.1x system only supports an "all-or-none" model of access control. Having authenticated successfully, a user gets full access to the network. The system cannot accommodate guest users (who might get limited network access) or recognize different classes of contractors, vendors, partners, or employees.

- Because they are tied to proprietary Dynamic WEP implementations, current 802.1x systems inherit the same interoperability issues.

- Many 802.1x systems do not work efficiently with client mobility. Typically, as a user moves between access points, these schemes require a new authentication handshake. Besides creating additional load on the authentication server and therefore reducing the scalability of the system, this authentication step can reduce the perceived system performance for mobile users.

Firewalls and Encrypted Tunnels

Having concluded that wireless LANs are as insecure as the Internet at large, many enterprises have simply chosen to formally treat them that way. The resulting network architecture—"the Internet *inside* the intranet"—adopts Internet remote access technologies to control wireless LAN access to the wired LAN.



In such a system, an extra firewall separates the wireless LAN access points from the wired LAN; the access points are connected to the firewall either by a direct cable connection or by means of a VLAN. The firewall supports packet filtering and can be used as a point of control for detecting network attacks. This firewall includes Virtual Private Network (VPN) software, implementing protocols such as IPSec[xii], L2F[xiii], PPTP[xiv], or L2TP[xv]. To access the corporate LAN, the client "logs in" to the firewall and establishes a VPN tunnel. The VPN encrypts all wireless LAN data traffic using standard, well-studied algorithms.

Though it is an effective approach to wireless LAN security, the firewall/VPN solution poses several challenges.

First, the firewall/VPN introduces a significant scalability bottleneck, because all wireless traffic must pass through it. The firewall must have adequate network connectivity to support the data flow, possibly requiring a gigabit Ethernet backbone in even modest wireless LAN installations. VPN encryption requires considerable computational cycles, often demanding special hardware to provide cryptographic acceleration. Few VPN systems are designed to scale to levels capable of supporting a full enterprise user population.

Second, the firewall/VPN solution is expensive. As we have seen, the VPN software requires an expensive server with a cryptographic accelerator. The firewall and VPN, typically purchased to support only a limited percentage of enterprise users, must be scaled to support the entire enterprise. Furthermore, because the firewall/VPN is a single point of failure, the network manager must plan for rapid fail-over capability, with duplicate hardware and software configurations.

Third, the solution introduces deployment challenges. VPN software is notorious for its interoperability problems; in many cases, the VPN server is only compatible with a particular VPN client. VPN software may not be available for all wireless clients, particularly handheld devices.

Fourth, the firewall/VPN limits the flexibility of the wireless LAN. All users must authenticate to the firewall, and all wireless communication must be encrypted through the VPN. This is particularly problematic for guests, contractors, and other temporary network users who might not have the required VPN client software installed on their devices, and managing these users' registration on the VPN server represents a substantial management burden for the enterprise. In addition, it imposes encryption on traffic—such as Internet traffic—that need not be protected; this introduces additional load on the firewall server while unnecessarily complicating use of the wireless LAN for simple Internet access.

Finally, the VPN solution requires that end users be actively involved in enforcing data security. Users must be trained to launch the VPN client when accessing the wireless LAN, and they must remember to do so. Users must be trained to use the VPN client. Unless proprietary key management techniques are used with the VPN software, the enterprise must administer and disseminate shared secret keys to all users. This complexity increases the chances of mistakes or, worse, the likelihood that users will actively attempt to avoid the security measures that are in place.

Summary

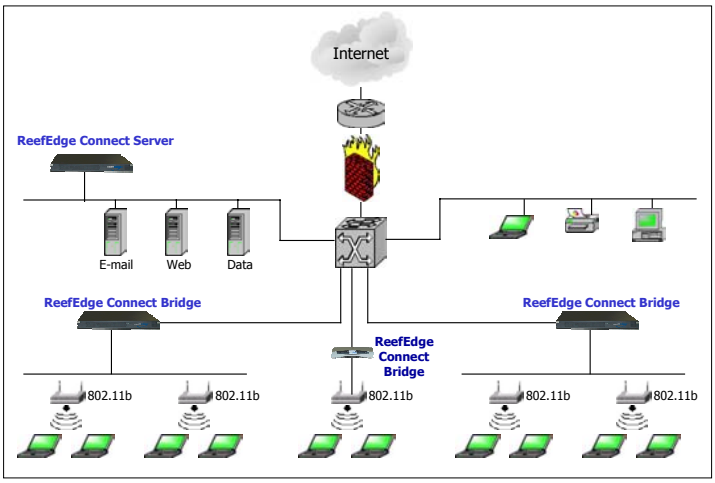
In summary, the security mechanisms available in today's short-range wireless networks are insecure, incomplete, and difficult to manage within an enterprise environment. Various "band-aids" are being used to address these concerns, but each of these falls short in terms of security, scalability, flexibility, or cost.

Enterprise wireless LANs require a security solution designed and engineered to deliver authentication, access control, and privacy services. The solution must be easy to manage, easy to use, flexible enough to adapt to changing needs, and ready to integrate with existing IT infrastructure.

The ReefEdge Connect System: Security for a Mobile Enterprise

The ReefEdge Connect System was designed from the start to address the security, manageability, and usability requirements of enterprise wireless LANs. Network administrators can designate the approved wireless LAN users, manage their security credentials and network access privileges, and ensure the encryption of their wireless transmissions in accordance with corporate policies. The ReefEdge Connect System works with existing authentication, directory, and systems management systems within the enterprise. Wireless LAN users receive the connectivity, subnet roaming, and bandwidth management required to ensure a seamless mobile communications experience. Built on innovative, patent-pending technology, the ReefEdge Connect System delivers the high performance, scalability, and reliability needed to support full enterprise deployments.

The ReefEdge Connect System addresses head-on the three axes of security—authentication, access control, and privacy. The system design recognizes that different technologies are appropriate for addressing each of these axes, that enterprises will have differing needs along each axis, and that enterprise needs will change over time. IT managers can select and implement the security controls that are appropriate for the particular situation.

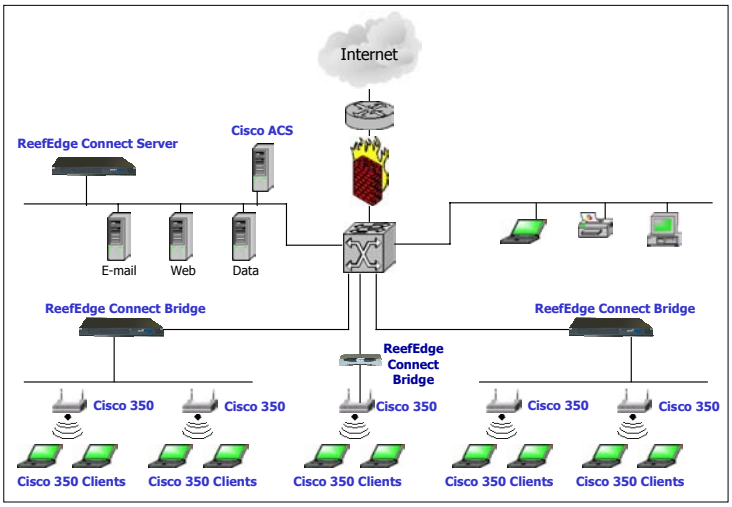


Authentication

Using the ReefEdge Connect System, enterprises control which users can access the wireless LAN. The Connect System requires all users to authenticate to the network, creating a dynamic binding between the user's identity and the device that they are using.

This authentication model offers several advantages:

- The user's identity—rather than the device or the network adapter—determines network access. Lost and stolen devices do not automatically gain access to the network. Users can share their devices with colleagues without fear of compromising the enterprise network.
- Users can easily change or upgrade devices without requiring re-provisioning by the ReefEdge Connect System administrator.
- A user may employ multiple devices simultaneously.
- The enterprise IT manager can administer and monitor the enterprise network to determine which users and devices are authorized, as well as which are currently active.



ReefEdge Connect System authentication works easily with both current and future technologies. The authentication service works with any browser-enabled device, and an automatic sign-on utility is available for Microsoft Windows clients. The Connect System also integrates with access points, including the Cisco Aironet 350, that support 802.1x authentication with EAP; in this configuration, the ReefEdge system recognizes the same authentication credentials supported by the EAP authentication server. The Connect System operates seamlessly within an enterprise environment by linking with external authentication services such as RADIUS servers, LDAP directories, and Microsoft Windows™ domains. ReefEdge enables solution providers to build custom authentication solutions that integrate with biometric security, SIM cards, secure ID tokens, and custom or legacy authentication solutions.

Access Control

The ReefEdge Connect System enables a powerful multi-tier access control mechanism through its distributed firewall implementation. Users are associated with security classes, which determine the accessible network hosts, ports, and applications. The Connect System's access control mechanism delivers to each user a personalized view of the network. Even though users share a common wireless LAN infrastructure, they are treated as individuals with individual user privileges.

For example, an enterprise might define security classes for employees, guests, vendors, contractors, and other user groups. IT managers can safely offer Internet access to guests and limited network access to other temporary workers. Many network environments use VLANs to establish so-called "Chinese Walls" separating different employee groups, but it is impractical to deploy physically separate wireless infrastructure to duplicate these policies for mobile users; however, the ReefEdge Connect System can enforce individualized network access policies, delivering the VLAN experience over the Wireless LAN.

ReefEdge Connect System access control can even be enforced on a location-specific basis, enabling wireless security to match the physical security of the enterprise premises. For example, within the reception area, guests might receive limited Internet access, but within conference rooms, guests might receive full access to the Internet and to various meeting and collaboration tools.

ReefEdge takes access control one-step further, by providing a layer of security for the mobile devices themselves. The patent-pending Mobile Masquerading™ technology deployed in the ReefEdge Connect System gives the IT manager control over whether servers may run on mobile clients, as well as who may initiate connections to those mobile servers.

Beyond controlling the flow of network traffic, the ReefEdge Connect System is part of a comprehensive access control solution. Solution providers can integrate the wireless LAN with enterprise security systems providing auditing, logging, and intrusion detection support. Through its partnership with Xcellenet and its Afaria product line, ReefEdge enables solutions that fully manage wireless LAN clients. For example, the system can enforce login scripts or applications that must be executed before a user is permitted to access the wireless LAN. These scripts might ensure delivery of upgraded software to the mobile client, execution of appropriate anti-virus software, or consistency checks of the client configuration.

Privacy

The ReefEdge Connect System delivers a scalable IPsec solution for cost-effectively supporting hundreds or thousands of simultaneous wireless LAN users. Unlike a traditional VPN server, the ReefEdge system terminates the IPsec tunnels at the edge of the network—at the wireless access points—and moves those tunnels seamlessly to the user's current access point as the user roams about the wireless LAN. ReefEdge protects the traffic where it is vulnerable—on the radio link—and improves performance by avoiding unnecessary encryption on the wired portion of the network. The system avoids the need for a centralized cryptographic processor, with its high hardware costs, complex networking requirements for routing traffic to and from that processor, fault tolerance problems, and scalability and load issues.

The ReefEdge Connect system simplifies the task of managing an encrypted wireless LAN environment. Administrators can designate for which users encryption is mandatory and for which users encryption is optional. The ReefEdge Connect system automatically configures and launches the VPN client, so users are not even aware that encryption is taking place. Key management is simplified, because all necessary shared secrets and keys are securely and automatically delivered to clients. Finally, the ReefEdge Connect system allows IT managers to leverage their existing investments because it works with existing VPN clients, including the Microsoft client that comes pre-installed in Windows 2000 and Windows XP.

In some environments, an IT manager may choose to bypass the data encryption capabilities provided by the ReefEdge Connect System and instead use the system in conjunction with an existing VPN server. The ReefEdge Connect System is compatible with most existing VPN solutions including those from Checkpoint, Cisco, Intel, and Nortel.

The ReefEdge Connect System enhances the scalability, flexibility, and simplicity of VPNs for protecting wireless LAN data transmissions:

1. The Connect System access control mechanisms distinguish which data must be transmitted through an encrypted tunnel to the VPN server and which data may travel directly to the destination host without VPN encryption. First, these mechanisms reduce the overall load on the local network and the VPN server. Second, network traffic that bypasses the VPN server encounters reduced network delay because it is routed directly to its destination. Third, guests receive a simplified user experience by avoiding the need for VPN software for basic Internet access.

2. The Connect System subnet roaming capabilities eliminate both the need to wire access points directly to the VPN server and the need to VLAN the access points into a single subnet. Besides eliminating a source of network load and scalability problems, the ReefEdge Connect System simplifies the overall network design. The network administrator can place access points anywhere and simply connect them to the existing LAN without performing a network reconfiguration.

3. ReefEdge is working with a variety of partners to ensure that the Connect System is tuned to work with a variety of VPN clients, including those for laptops, PDAs, and cellular phones.

The ReefEdge Connect System works seamlessly in conjunction with existing WEP and Dynamic WEP technologies and, through its support for 802.1x and EAP, it will support future evolution in these standards.

Conclusion

Despite their obvious potential to deliver rapid return-on-investment (ROI) through easy deployment and management, wireless LANs have been implemented primarily within small-scale installations. Before engaging an enterprise-wide rollout of the technology, IT managers must address the inherent security issues, including authentication, access control, and privacy. Unfortunately, current wireless LAN standards and security solutions fall short on all three of these areas. An inability to fully address security issues threatens to erode the ROI promise of wireless LAN technologies in the enterprise.

The ReefEdge Connect System attacks head-on the security and manageability issues of IT managers as they deploy short-range wireless networks within the enterprise. The ReefEdge solution ensures that users authenticate to the network, that the user's credentials are made available to all access points in the environment, that appropriate access control policies are enforced throughout the wireless network, and that encryption is efficiently implemented to protect enterprise data. The Connect System integrates seamlessly into existing IT infrastructure, such as directories and authentication servers, and it future-proofs the enterprise from changes to either the wireless LAN standards or the deployment of future security infrastructure. Finally, ReefEdge delivers tools that allow enterprise and solution providers to customize the security solution, with features such as single sign-on to

applications, integration with custom or legacy infrastructure, and automated scripting of the user login process.

Today's enterprises require short-range wireless networks that are cost-effective, easy to deploy and manage, and, over all, secure. With the ReefEdge Connect System, enterprises can safely deploy in-building wireless networks today, and they can be sure that the solution can grow to meet all of their future wireless networking needs. ReefEdge builds confidence in wireless networks.

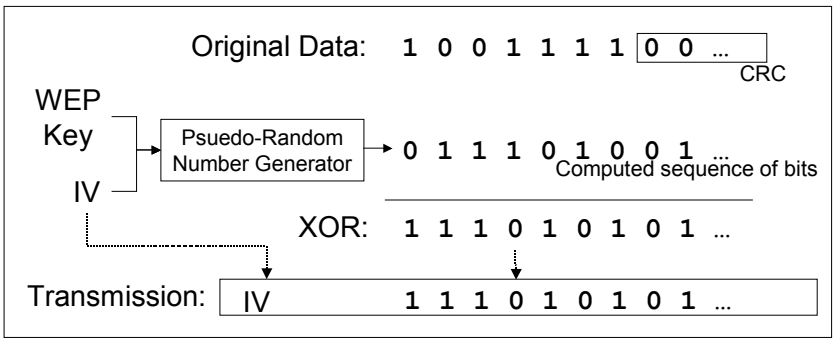
For more information about ReefEdge and ReefEdge products, contact:

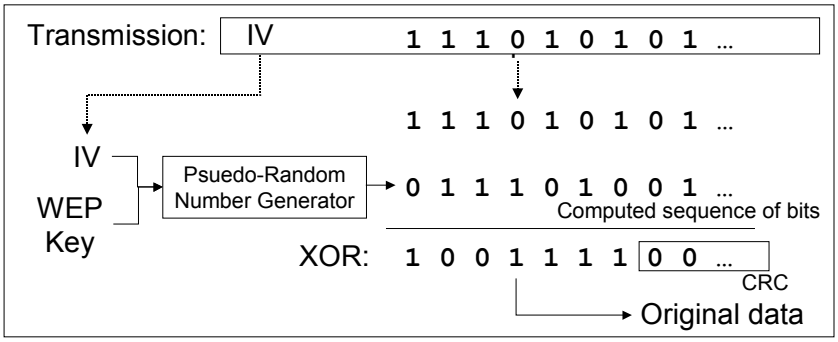
ReefEdge, Inc.
Two Executive Drive
Fort Lee, New Jersey 07024
T. +1.201.242.9700
F. +1.201.242.9760
E. info@reefedge.com
www.reefedge.com

Appendix: Overview of 802.11b WEP Encryption

The Appendix provides an overview of the WEP protocol.[xvi]

To send data, an endpoint first computes a CRC checksum against the plaintext data and appends it to the data. The sender then selects an Initialization Vector (IV). This IV is combined with the WEP key and the resulting value is passed through a pseudo-random number generator to produce a sequence of bits. These computed bits are then XOR'ed against the data and appended CRC. Finally, the IV and the XOR'ed bits are transmitted over the air to the other endpoint.





Upon receiving the transmission, the receiver extracts the IV and encrypted data. The receiver combines the IV and WEP key and then applies the pseudo-random number generator to reproduce the sequence of bits. The computed bits are then XOR'ed against the transmitted data to recover the original unencrypted data and appended checksum. Finally, the receiver verifies the CRC to confirm the integrity of the transmission.

NOTES

[i] John Leyden. "War Driving – The Latest Hacker Fad." *The Register*, 29 March 2001. Available from http://www.theregister.co.uk/content8/17976.html.

[ii] IEEE Standards Board, "802 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications."

[iii] B. Schneier. *Applied Cryptography* (Wiley), 1996.

[iv] L. Gonnes. "Often Unguarded Wireless Networks Can Be Eavesdroppers' Gold Mine." *The Wall Street Journal*, 27 April 2001. Available from http://www.msnbc.com/news/565275.asp.

[v] W. A. Arbaugh, N. Shankar, Y. C. Wan, "Your 802.11b Network has no Clothes," March 2001. Available from http://www.cs.umd.edu/~waa/wireless.pdf.

[vi] J. R. Walker. "Unsafe At Any Key Size: An Analysis of the WEP Encapsulation." Intel Corporation (document IEEE 802.11-00/362), October 20 2000. Available from http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip.

[vii] N. Borisov, I Goldberg, and D. Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." *Proceedings of the ACM SIGMOBILE Seventh Annual International Conference on Mobile Computing and Networking*, July 2001. Available from http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.

[viii] S. Fluhrer, I. Mantin, and A. Shamir. "Weaknesses in the Key Scheduling Algorithm of RC4." *Proceedings of the Eighth Annual Workshop on Selected Areas in Cryptography,* August 2001. Available from http://www.wisdom.weizmann.ac.il/~itsik/RC4/rc4.html.

[ix] A. Stubblefield, J. Ioannidis, and A. Rubin. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP." AT&T Labs Technical Report TD-4ZCPZZ, Revision 2, 21 August 2001. Available from http://www.cs.rice.edu/~astubble/wep/.

[x] T. Scannell. "MI Survey Reveals IT Execs' Plans for Wireless LAN Migration." *Computer Letter*, August 2001.

[xi] L. Blunk and J. Volbrecht. "PPP Extensible Authentication Protocol (EAP)." Internet RFC 2284, March 1998. Available from http://www.rfc-editor.org.

[xii] The IPSec suite of protocols are defined by the Internet Engineering Task Force (IETF) to enable the exchange of IP traffic through encrypted tunnels. For more information, see http://www.ietf.org/html.charters/ipsec-charter.html.

[xiii] A. Valencia, M. Littlewood, and T. Kolar. "Cisco Layer Two Forwarding (Protocol) 'L2F'." Internet RFC 2341, May 1998. Available from http://www.rfc-editor.org.

[xiv] K. Hamzeh, et al. "Point-to-Point Tunneling Protocol (PPTP)." Internet RFC 2637, July 1999. Available from http://www.rfc-editor.org.

[xv] W. Townsley, et al. "Layer Two Tunneling Protocol 'L2TP'," Internet RFC 2661, August 1999. Available from http://www.rfc-editor.org.

[xvi] For a more detailed discussion, see the IEEE specification (cited above); also see S. Weatherspoon. "Overview of IEEE 802.11 Security." *Intel Technology Journal*, 2nd Quarter 2000. Available from http://developer.intel.com/technology/itj/q22000/pdf/art_5.pdf.