

VOLUME TWO · ISSUE ONE
Secure Business Quarterly:
Defining the Value of Strategic Security

FIRST QUARTER 2002
Exclusively on the Web at:
www.s bq.com

S B Q

SECURE BUSINESS QUARTERLY



Exclusively
on the Web at:
www.s bq.com

Security in a Wireless World

The Deployment of a Wireless Network in a Hostile Environment

by David Pollino and Matt Miller

Secure Business QuarterlySM is an @stakeSM publication.



The Deployment of a Wireless Network in a Hostile Environment

by David Pollino and Matt Miller

Deploying wireless networks enable freedom of mobility, more communication channels, and limitless access to information. Combined with the ease of implementation and the relatively small amount of infrastructure required, portable wireless networks can greatly benefit emergency-response personnel, consultants, or any other type of field personnel.

It is inherently difficult to have physical control over a wireless network's entire area of coverage, therefore, it must be assumed that the network is being placed in a hostile environment—one where unauthorized outsiders can access information.

continued...

Portable wireless networks are inexpensive, ranging between \$300 and \$2000. These costs can be further minimized because outdated hardware can often be used. While implementation time can range from a few hours to a few days, preconfiguration of these networks dramatically reduces the deployment time.

Matching the Technical Solution to the Business Objectives

Confidentiality and Integrity During Communications

Confidentiality prevents eavesdropping. A malicious attacker could eavesdrop on wireless communications and compromise sensitive data, such as passwords. Confidentiality can be achieved by establishing an encrypted tunnel between the roaming stations and a portal on the wired infrastructure. There are many mechanisms that can be used to achieve this goal depending on the application. IPsec (IPSec) is a standards-based encryption infrastructure that can provide confidentiality and integrity. IPsec has been proven effective for a number of years and can provide the necessary encrypted tunnels. Other options to provide confidentiality are encrypted port forwarding using a protocol such as SSH or using an encrypted protocol such as SSL (Secure Sockets Layer) or TLS (Transport Layer Security).

Authentication of Users

Authentication is important to verify that legitimate users only use the wireless infrastructure. 802.1x is a solution that provides authentication using Extensible Authentication Protocol (EAP) to authenticate wireless stations to a wired network. 802.1x authentication is implemented using encrypted RADIUS-based authentication to a backend server for station authentication. In some implementations the WEP key is also generated on a per-session basis. In addition to providing a better authentication mechanism than the current 802.11 standard, 802.1x simplifies WEP key management among the stations.

continued...

802.11 Security Problems

Recently the 802.11 standard has been proven to be susceptible to attack methods and therefore cannot provide adequate security.

• Confidentiality or Integrity

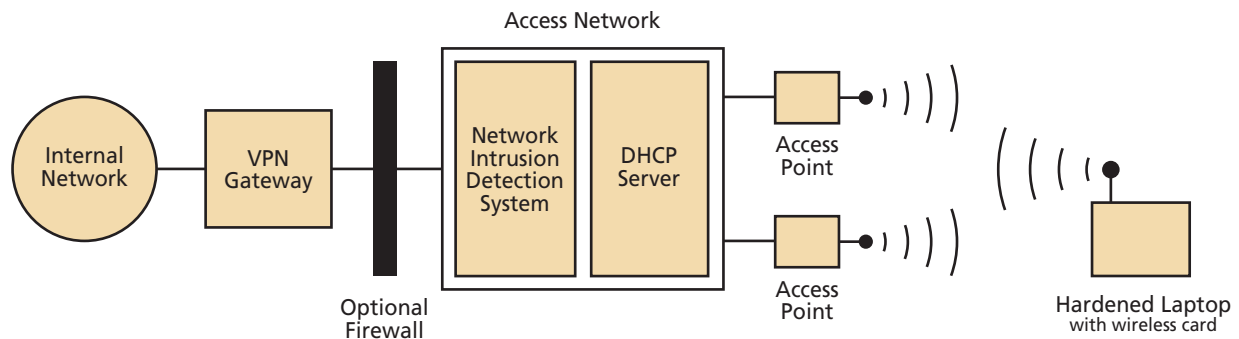
802.11 provides a recently proven flawed encryption mechanism, based on the RC4 algorithm called Wire Equivalent Protection (WEP). It is based on a shared-secret key that resides in the access point and on the mobile stations. All participants and all access points share this shared secret across the network. The integrity mechanism is nothing more than a basic CRC-32 checksum, which is more for error checking than a cryptographic mechanism for providing integrity to information in the communications channel.

• Authentication

The 802.11 standard provides a flawed shared-key authentication method that presents a cleartext challenge and a ciphertext challenge to the attacker, providing a trivial means to mount a cryptographic attack on the RC4 stream, which is needed for encryption.

• Mobility Management

While the current standard allows a distribution system to enable roaming between access points, it does not define how the distribution system should function or what to do when a client roams off a distribution system or to a different subnet, so when implementing these features you may be required to use a single vendor's product.



Mobility Management for Stations

Wireless users are often mobile and need the ability to roam around the network. This involves connection to multiple access points. Mobile IP [RFC-2002] can provide such mobility management. Mobile IP has two agents that allow roaming machines to properly route back to a home network. The first agent is the Home Agent, which is a static server that registers a static address to each mobile station. The static address is used to keep VPN connections alive while roaming. When a mobile station roams from the home network to a foreign network, the mobile station looks for a foreign agent through which the VPN connection can be re-established.

Network Architecture

Scenario 1:

- Defined area where limited mobility is needed
- Population less than 25

When the network coverage area is small, such as a conference room, an exposition area at a conference, or a quickly constructed triage center, a single access point (AP) can usually cover the affected area, and secure access is ensured when combined with a traditional VPN solution. This solution manages risk in a prudent manner assuming the stations are fixed, and not moving beyond a defined area.

Scenario 2:

- Large roaming area
- Population greater than 25

The solution for this second scenario is similar to the first, but requires the addition of a distribution system. A distribution system allows users to roam between access points without losing connectivity. Network designers should use a single subnet for the distribution system; this preempts the need for users to

change IP addresses while roaming or using Mobile IP. The 802.11 does not specify the operation of the distribution system, so in most cases all access points will need to be the same brand and capable of operating in a single distribution system.

Description of Architecture

Gateway Options

In either application, the tactical wireless network traffic will need to be sent off to another network through a gateway of sorts. This gateway may be a wired 10 or 100M/bit Ethernet interface, a telephone line, a satellite terminal, or another terrestrial wireless link. While gateways may simplify wireless integration, they are not critical in every case. For instance, if email is the only application used, then a hardened email server can provide security over SSH or SSL.

Access Points

802.11 access points provide connectivity similar to a traditional wired Ethernet. APs continuously send messages to potential wireless users to inform them about the radio network; these messages are called beacons. When configuring access points, the frequency of beacons should be minimized, beacons should be broadcast at the lowest bandwidth that is to be used by wireless users, and broadcasting too much information about the configuration of the AP, such as SSID, should be avoided. Out-of-band management should be used for all APs.

Switch

An Ethernet switch can be used to consolidate all access points. The switch should be physically separate from the network—on the other side of the gateway. This will help prevent layer-2 attacks that could be used to circumvent VLAN and other layer-2 access controls.

continued...

VPN Gateway

An IPSec or SSH-based VPN Gateway will provide confidentiality and integrity for users over the wireless link. Additional IPSec VPNs may also be used to allow users to access corporate networks remotely.

Intrusion Detection System

A Network Intrusion Detection System (NIDS) should be deployed on all wireless segments. NIDS signatures should be very easy to create, because the authorized traffic should be known, so NIDS turns up the alert to detect misuse.

Authentication Server

If possible, 802.1x should be used to authenticate users to the wireless network. 802.1x allows centralized authentication of wireless users or stations.

Firewall/Router

Depending on configuration, a firewall may be optional. Often VPN gateways serve the same function, and can be hardened. Additionally, the IDS system can be used to analyze traffic.

User Workstations


User workstations and support servers should be hardened to prevent host hopping and exploitation of available services. Personal firewalls should be used as an additional countermeasure.

Vulnerabilities

While the recommended architecture above addresses several of the security issues involved when deploying wireless networks, there are vulnerabilities that the architecture does not take into account. The design does not take into account RF denial of service attacks. It is possible to use RF flooding to disrupt a wireless network, rendering it useless but without compromising the information. Little can be done to design against RF

interference because the frequencies used for 802.11 are unlicensed. In addition, standard issues with key management are still relevant. Keys must be deployed, maintained, and revoked in a secure fashion to prevent unauthorized users from gaining access to the network. Finally, man-in-the-middle attacks are still possible, for instance, an attacker could deploy an unauthorized AP either in closer proximity to, or with more power than the authorized AP, in order to get users to associate to the unauthorized AP. Properly employed IPSec will lessen the viability of many of these attacks, but the threat will still exist.

Conclusion

Secure wireless networks can be deployed quickly and cost effectively once the architecture and hardware are procured. However, complexity increases as the amount of serviceable users and coverage area grows. When users must “roam” between different access points, new criteria enter into the equation, due to the complexities involved in configuring a network that provides users the mobility they desire. When these factors are taken into consideration, a wireless network can be designed with appropriate countermeasures, to provide both mobility and security for wireless networks in hostile environments. 

David Pollino is a Managing Security Architect with @stake.

Matt Miller is a Senior Security Architect with @stake.