

Securing Wireless Networks

by By Joe Klemencic (faz@home.com)

Mon. Apr 30 2001

Many companies make attempts to embrace new technologies, but unfortunately, many of these new technologies are not mature enough to provide adequate security mechanisms to prevent unauthorized access to such services. Wireless Network Connectivity is no exception.

Wireless Networking (WLAN) provides the ability for devices to connect to a Local Area Network without wired connectivity. This allows for devices to gain access to network resources in areas where running physical wires is not possible (such in open areas), multiple access (as in conference rooms) and permits the ability to roam from one area to another without losing network connectivity. Wireless connectivity methods have grown over the years from vendor proprietary low speed operations (less than 2Mbps) to IEEE 802.11 networking standards (up to 11Mbps with 22Mbps being released later this year for multiple access, 56Mbps for point-to-point). In the most basic form, WLAN is an ordinary LAN protocol that is modulated on carrier waves. IEEE 802.11 is an extension to the existing IEEE 802.3 Ethernet standards. WLAN utilizes an Access Points (AP), otherwise known as a Wireless Bridge, to provide connectivity between the wireless devices and the wired network. These AP's allow for access ranges of up to 400 feet for 11Mbps and 1500 feet for 1Mbps connectivity. These distances and speed are implementation specific, and affected by power output and obstacles. WLANs are similar to a repeated Ethernet environment where each packet is broadcast to all other WLAN nodes. In its native form, WLANs do not provide any type of security against unauthorized access. Users may freely purchase an 802.11b Wireless network card, install it in their machine, and by utilizing DHCP services, gain access to the local network via a WLAN. Given the distances covered by the WLAN, these users do not necessarily need to be physically located within a building served by the WLAN. However, there have been some attempts to provide levels of security for WLANs, each with their own restrictions, including:

- MAC address filtering
- Vendor specific authentication
- SSID/Network ID
- Wired Equivalent Privacy (WEP)
- Emerging IEEE 802.11x

MAC Address Filtering

This technique utilizes a hand-coded list of the MAC (Media Access Control) addresses of client WLAN interface cards that are allowed to associate with an Access Point. This method is useful only in small installations where there are few access points and centrally administrated clients. This method does not scale well, for the MAC address list for allowed clients must be installed in every Access Point the client is allowed to associate to. Care must be taken to update all the lists if a client interface card is replaced. This technique is vulnerable to attackers who either steal WLAN interface cards that are allowed to access the WLAN, or by assuming the MAC address of an

allowed interface card. Utilizing a Wireless packet, these allowed MAC addresses could easily be derived.

Vendor Specific Authentication

Many vendors offer the ability to code user names and passwords into the Access Points, and provide a custom software client to be installed on the client devices. This software prompts the user to enter their login and password before allowing connectivity to the WLAN. This method requires the user logins and passwords to be installed on every installed Access point, and support for connectivity is limited only to the clients for which the authentication software is available. Attackers could gain access by either exploiting security flaws in these vendor products, brute force password cracking, or data reply/data dissection of data streams from a packet sniffer.

SSID/Network ID

The first attempt at providing a large-scale security mechanism is the addition of the SSID/Network ID. A SSID consists of seven digit alphanumeric identifier that is hard coded into the AP and client devices. This ID is transmitted by the WLAN client during AP association (initial connection attempt from a WLAN client to an Access Point, similar to establishing a Link in an Ethernet environment), and if correct, the AP allows association. This mode of operation also allows to be run in either an Open or Closed mode of operation. In Open mode of operation, any WLAN client, regardless if the SSID is correct, may associate with an AP. In the Closed mode of operation, only WLAN clients with the proper SSID may associate. Clients configured with a SSID will still connect to both Open and Closed WLANs, such as a Closed network at the office, and an Open network in their home, but only one SSID may be defined at one time. To switch between two Closed networks with different SSIDs requires a client reconfiguration. The SSID is only transmitted by the WLAN client to the AP during the initial association request, and normally is transmitted over the WLAN in clear text, and is normally stored in clear text fashion on the WLAN client device. SSIDs are vulnerable to an attacker utilizing a Wireless packet sniffer, due to the clear text nature. However, if used in conjunction with WEP, the SSID is transmitted in encrypted form to the AP, but is still stored in clear text on the WLAN client. If it is determined that a SSID has been compromised, efforts to assign a new SSID to all the AP's and WLAN clients must be manually initiated.

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP) was introduced to provide a level of data encryption for communication between a WLAN client and an AP. WEP utilizes either 40bit or 128bit encryption algorithms, via shared secret keys. Typically, four different keys (shared secret keys) may be defined, but only one key is active at any given time, and these keys are typically stored in encrypted fashion on the AP and WLAN client. WEP installations do not define the methods for distributing keys to clients. In most cases, the keys must be manually installed on each AP and WLAN client, but some vendors allow for SNMP updates. The primary drawback of SNMP updates is that a previously known key must be retained and active to allow clients to connect to the WLAN before pushing new WEP keys via SNMP. Typically in this implementation, the key updates are performed in two phases. The first phase updates three of the four keys, while retaining

the original key as active. After all the WLAN clients have been updated, a second SNMP push is made to update the last original key and change the active key to a new key. Unfortunately, with a vast number of mobile WLAN clients, updating all WEP keys can be difficult at best. WEP-enabled clients, configured to only connect to Encrypted WLANs, cannot connect to a non-Encrypted WLAN, such as a home implementation. In this scenario, the user would need to have knowledge of the WEP keys utilized and either configures their home WLAN AP to utilize the same WEP key values, or disable WEP on their WLAN client, and re-enable WEP when connecting to a WEP WLAN. This leaves the WEP keys vulnerable to being written down or communicated by the end user in other fashions to unauthorized individuals. It has recently been discovered that WEP is vulnerable to replay attacks and reverse engineering of the WEP keys utilized (<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>).

Emerging IEEE 802.11x

To overcome the shortcomings of securing WLANs in a large environment, the IEEE has been formulating the 802.11x specifications, which make use of user authentication with dynamic key exchange. Currently, this technology is supported via the Extensible Authentication Protocol (EAP) available in various RADIUS implementations. In this authentication method, authentication and key management software is loaded onto the WLAN client. Upon initial association with an AP, the software will prompt the user to enter their network credentials, such as a login/password pair. This is forwarded to an EAP/RADIUS server via the AP, which processes the authentication request. Since RADIUS is utilized, various authentication methods can be used such as PAP/CHAP and non-reusable One Time Passwords. Upon successful authentication, a set of encryption keys is negotiated between the AP and the WLAN client for the duration of the session. Upon association to a different AP, such as while roaming around a facility, the users cached credentials are forwarded to an EAP/RADIUS server via the new AP and new session keys are negotiated. In the event that a particular session key is compromised, only data captured during that session is vulnerable. These session keys are also unique between users.

Securing the Access Point

Most AP's are configured via a Telnet session, Web Browser, SNMP, custom manager software, via the serial port or any combination of the above. Care must be taken to ensure the WLAN is installed in a physically secured location, if at all possible. This will prevent unauthorized physical access to the stored configuration. If SNMP is utilized, change the SNMP community strings from the default, and ensure that the PUBLIC SNMP string is different from the PRIVATE string, and both utilize a strong password. If the AP allows, restrict configuration management access to only a few network clients, and prohibit any management access from the WLAN clients. Attackers can easily identify the vendor of the installed AP via the MAC address, which can lead to enumeration of the type of configuration management allowed. If the AP utilizes PCCARD slots, use a different vendor Wireless interface card. This alternate vendor interface card MAC address will be identified in a sniffer trace, and assist in obscuring the actual vendor of the AP. Please note that this will not entirely stop an attack against an access point, but only prevent quick vendor identification.

Rogue Access Point Identification

Since the WLAN technology is dropping in price, users are beginning to purchase their own products for personal use. Some of these may even start to spring up around your company, such as in conference rooms, unbeknownst to the IT folks. Tracking these down can be difficult at best, and the best solution is to develop a WLAN strategy and begin implementation before it gets out of hand. Nothing could be worse than a user installing an unsecured AP in a conference room that is broadcasting into the parking lot, allowing an attacker to gain direct access to the network from outside the building. In this scenario, it is next to impossible to identify the intruder. Suppose this intruder attaches to the WLAN and launches a hacking or denial of service attack against your competitor. The only information you have is an IP address originating from your local network, and if lucky, a MAC address from the DHCP file. By the time you are notified of the attack and gather the information, the attacker could be long gone, never to be traced again. There are a few tricks that can be used to identify and locate unauthorized Access Points:

- Parsing CAM and ARP entries from the switches and routers, looking for ports with multiple connections
- Parsing CAM and ARP entries looking for popular WLAN vendor MAC addresses

Roaming around the facility with a Wireless device and Wireless sniffer software, looking for Beacons from Access Points (when a WLAN client encounters an area with multiple Access Points, the client can use the Beacon to determine with AP has the strongest signal to associate with). A Beacon is the announcement that an AP is alive, and is broadcast every 10 seconds. Since a Beacon also contains the MAC address of the AP, a quick check in the network switches and routers may help to determine where the AP is located. Utilizing vendors signal strength utilities to determine the general area an AP is installed

Design Considerations

Proper network design can mitigate or eliminate the risks currently associated with securing Wireless Networks.

- Containing WLANs within their own VLANs
- Protect WLAN network touch-points with a firewall or access control lists
- Utilize VPN technologies to eliminate the need for opening multiple services through access controls. This will provide the necessary authentication, authorization and encryption to protect LANs from unauthorized WLAN clients

Utilizing VLANs

By creating a separate VLAN (Virtual LAN) strategy for the WLANs, one can deliver and contain the WLAN clients without infesting the wired network. A separate VLAN for the WLAN clients will ensure all network broadcasts (ARP, IP broadcast) will remain only on the WLAN. VLANs also offer the ability to expand a WLAN to multiple physical locations. This greatly improves the roaming ability of mobile users (such as walking from an office to a conference room on another floor). Normally, when a WLAN client associates from AP to AP, a brief network outage is experienced on the roaming WLAN client. This is due to the WLAN client associating with a new AP and establishing a new IP address (if DHCP is utilized). In a static IP environment, users would have to manually change their

client IP address to a permitted IP address services by the new AP. By retaining the AP's on the same VLAN and IP subnet, the network outage is brief, for the client will reuse the cached DHCP address, or will continue to use the configured IP address. There will be cases when many VLANs may be used to service the WLAN, but the outcome is the same.

WLAN Access Controls

By placing access controls or a firewall on the touch-point between the WLAN and the LAN will assist in mitigating risks from the WLAN. Depending on the on-site security policy, these access controls may simply block certain denial of service attempts, only allow certain services (HTTP, POP, TELNET, FTP, etc) from the WLAN to the LAN, or may be fully restrictive which allows only VPN type connections from the WLAN to a VPN server.

Utilizing VPN Technologies

For the utmost protection, a VPN solution may be considered. If your company currently utilizes VPN technologies, it may be possible to leverage the current infrastructure to the WLAN. This may also provide an additional benefit in terms of support, since support procedures for the currently installed VPN is already in place. The use of an already established VPN will also provide less confusion for WLAN clients, where they will be using the same access methods, with the same restrictions, by connecting on the WLAN or from working remotely. Access controls should be placed on the perimeter of the WLAN to allow only VPN traffic from the WLAN to the VPN server. To avoid allowing other unauthenticated traffic from the WLAN, such as DNS resolution of the VPN server name, a simple DNS server could be installed on the VLAN servicing the WLAN. Other services could also be placed on the VLAN serving the WLAN to assist users that are not yet authenticated via the VPN, such as DHCP and HTTP Proxy servers. If HTTP proxy servers are utilized at your location, a DNS server on the WLAN VLAN could translate the real name of the HTTP proxy to a local web server. Alternatively, this same web server could serve an autopxy file to web clients that are not yet VPN established. Creative configuring of the DNS and HTTP server could return an informational web page to the unauthenticated WLAN clients that VPN sessions must first be established to utilize network resources. Once a VPN session is established, the WLAN client would utilize the real DNS and HTTP servers on the LAN.

User Security

Since WLAN technology is similar to a repeated network, users are still vulnerable to compromises and denial of service attacks against their local machine. It is recommended that users are educated on the effects of running certain services on their machines, such as FTP servers and sharing drives. Personal software firewall applications may also be installed on WLAN clients to further protect their local resources from unauthorized access attempts.

Throughout this year and into the future, more Wireless vendors will start to implement IEEE 802.11x, as will authentication agents, but no one solution will ensure complete protection of the WLAN. Choosing a few of the available techniques can mitigate the

associated risks of operating a WLAN. When choosing the security mechanisms appropriate to your implementation, try to keep in mind the philosophy of ease of use for the end users, while still meeting and exceeding your security policies. Some questions to ask yourself during the WLAN planning are:

- "Do I have the support staff to install and support yet another VPN client, or can I utilize the existing VPN services?"
- "Will users need access to the WEP keys to re-configure their WLAN client after attaching to a non-WEP implementation?"
- "Can a solution be provided that allows for users to purchase and install a WLAN interface card on their own and seamlessly gain access to the WLAN?"

In time, more users will be implementing a WLAN at home, and will want to connect their WLAN client to both their home and work WLANs with little effort. Also, more companies are starting to deploy public WLAN Internet offerings, such as in airport terminals and hotels. It is inevitable that traveling users will also want to seamlessly want to utilize these resources while traveling.