Wireless Security

Protection

In a Logistic Environment

Case Study

Ferran Gallego
GSEC Practical v.1.4b
May 28,2003

Table Of Contents

Introduction:

Logistic companies must control and manage thousand of parcels, packets and products, a facility to track them without having to move the infrastructure is a time saving and by consequence, a cost saving.

Logistic companies began working with wireless networks, to be able to implement their applications for management and package control, from any point of their warehouse/s with no need to create a wired network of an uncountable cost.

Therefore the implantation of wireless systems, to be able to give network connectivity to multiple mobile devices in a warehouse/s has contributed in providing flexibility and agility for the manipulation and management in real time, of stock.

Unfortunately it is not so simple and easy. It has been demonstrated that wireless solutions (following standard 802.11) are NOT as safe as we would like and in addition has become one of the main paths for hackers to access to corporate networks. As a consequence we developed this project to secure sites already using such systems and to create a pre-requisite list for possible future implantations.

Overview:

Our case study is based on a Logistic Company where they have implemented wireless LANs (WLANs) to all their Warehouse sites. Wireless mobile devices are able to open a session to their application for managing stock, receiving and shipping. This application was developed and based on an IBM Host environment. This is accessed using an industry standard terminal emulation called TN3270. This is a program designed to emulate an IBM 3270 terminal connected to a host or Physical Unit (PU) via IP link.

The Company had decided to implement the Wireless IEEE 802.11b standard because it was the most extensive and cost effective technology in the market place. They decided to work with a specific TN3270 gateway product at every site. This gateway provides TN3270 sessions to the wireless devices. But the main surprise was, we found the wireless implementation at each location was with different vendors, NO specific vendor selected.

Every site was connected to the Head or Central Office with a private Wide Area Network link. This enables the connection between local Gateways and the Host.

The Overall AIM?

This project is proposing a way to secure the wireless LANs, allowing authorized and authenticated wireless users to gain access to their host application, creating a security task list for implementation elsewhere. Some implementations cannot be corrected because of existing Hardware and/or Software is incompatibility issues.

However, we have found diverse WLAN designs, all of them under the 802.11b standard, but multi-vendor. This was stopping us from standardizing the security policy applicable to all Sites.

Solution

Based on multiple studies, presentations and white papers, we have decided to minimize the impact of any possible Wireless attack. The idea is to isolate our Wireless LAN from the rest of the corporate network, and ONLY allow the Wireless devices to have access to the local TN3270 gateway for opening Host sessions.

At this point we can start to analyze possible security vulnerabilities, from the existing design in our sites, we can apply different rules to resolve them, these follow in this document.

We have split our rules in three different groups:

First the Access Points (AP),
Second Wireless devices
Third guidelines for LAN design.

Group 1 Access Points

In this group we're defining some rules for configuring their Access Points (AP).

Unfortunately, it is quite easy to get access to a Wireless LAN. Quite often, the administrators leave vendors "default" parameters like SSID or password for administration access in the AP configurations.
Leaving vendors default parameters will make "life" easier for hackers to get to their prize: to get access to your Wireless LAN and afterwards to your corporate LAN.

Therefore, we place some doubt on any "default" parameter, in any Access Point configuration.

Choose a strong name string, for the Service Set Identifier (SSID) name.

Short for Service Set Identifier, an alphanumeric unique identifier (usually 32 characters) attached to the header of packets sent over a WLAN that acts as a password, when a mobile device tries to connect to the BSS (Basic Service Set). The SSID differentiates one WLAN from another; so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. A device will not be permitted to join the BSS unless it can provide the unique SSID. Because an SSID can be sniffed in plain text from a packet it does not supply any security to the network. [1]

An SSID is also referred to as a Network Name because essentially it is a name that identifies a wireless network.

Usually you'll find in the SSID string is the vendor's name by default. This rule must be applied together with the next one.

Set Service Set Identifier (SSID) broadcast to "NO".

The SSID was not originally designed to be used as a method of securing your WLAN; however if the SSID is kept secure by removing it from the access point's broadcast then it effectively becomes an additional level of security.

[1] http://www.webopedia.com/TERM/S/SSID.html

SNMP traffic

Disable any SNMP traffic, but consider using SNMP Read Only, with a strong community string, if your management infrastructure requires SNMP.

The Simple Network Management Protocol, SNMP, is a commonly used service that provides network management and monitoring capabilities. SNMP offers the capability to poll networked devices and monitor data such as utilization and errors for various systems on the host. SNMP is also capable changing the configurations on the host device, allowing the remote management of the network device. The protocol uses a community string for authentication from the SNMP client to the SNMP agent on the managed device. The default community string that provides the monitoring or read capability is often "public". The default management or write community string is often "private". The SNMP exploit takes advantage of these default community strings to allow an attacker to gain information about a device using the read community string "public", and the attacker can change a systems configuration using the write community string "private". The opportunity for this exploit is increased because the SNMP agent is often installed on a system by default without the administrator's knowledge.

The principle of least privileges is the best method to avoid the SNMP exploit. SNMP should not be enabled on devices that do not require it. It is more secure to push the information from the managed devices using SNMP traps rather than polling the devices using SNMP agents. SNMP community write strings can be disabled if the network management platform only poll devices and does not change the remote devices configuration.

If SNMP is needed the community strings should be set at their maximum length and include a combination of letters, numbers, and special characters to avoid a brute force attack. All network devices should be scanned using an SNMP vulnerability scanner to ensure that they do not use the default community strings.

SNMP access should also be limited to only the devices that require SNMP for monitoring. This can be accomplished by allowing only authorized clients to access UDP port 161.[2]

Broadcast Traffic.

Disable any insecure and nonessential management protocols provided by the manufacturer (for example CISCO CDP).

Using Protocols like CDP (Cisco Discovery Protocol), a device can advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN or WLAN. Can you imagine how "valuable" this information is, to anybody sniffing a WLAN?

[2] http://www.sans.org/resources/idfaq/snmp.php

Management Traffic.

Limit management traffic to a dedicated wired subnet & protected console access.

Normally AP requires one of the following to perform a custom installation, configuration or maintenance:

- Simple Network Management Protocol (SNMP) – refer point 3.
- Wired or Wireless LAN workstation with Telnet Client or Web browser
- Terminal or computer with RS-232 connection and ANSI emulation

Restrict the terminal emulation and console access to the wired network management subnet and the administrator User group in the authentication process.

Protect your administrator user group with a correct password, following the Global Company Password Policy or use a template such as :-
http://www.sans.org/resources/policies/Password_Policy.pdf

Enabling the web server permits the use of a web based browser to access the management console. Be sure your web server is using Secure Sockets Layer (SSL) or Secure HTTP (S-HTTP) protocols.

Connecting to the web server via HTTP automatically redirects the client browser to use HTTPS. This ensures that the username and password and all data entered by a user will not be sent in clear text

Use Secure Shell (SSH) instead of Telnet access:

Telnet transmit sensitive data, including passwords, in plain readable text, which is readily intercepted by unknown, unauthorized parties. With unencrypted transmissions comes the increased probability of network account thefts. Once your password has been compromised, your AP administration access is accessible by unauthorized parties, sometimes without you knowing it.

SSH clients work just like traditional Telnet clients. You can use SSH to do anything you might typically do with Telnet session with the assurance that your password and other sensitive information are more difficult to "wiretap".

IP addresses for Access Points.

Disable BOOTP[3] and DHCP[4] options to obtain a leased IP address, network configuration information and additional configuration options from a remote server. All AP are going to be considered like servers and we'll assign a static IP address to help us for monitoring & managing them.

Confidentiality and privacy in our communications are fundamental for a secure system, and the usual way to obtain this is by using ENCRYPTION.

WEP encryption keys.

The most basic form of security is the encryption of any user data moving over the network. Their are now many forms of encryption available, and the designers of the IEEE 802.11 standard had the forethought to include encryption in their original standard as released in 1997. Unfortunately, the so-called "Wired Equivalent Privacy" (or "WEP") capability included in 802.11 has a number of critical weaknesses. Perhaps, most notably, the key length in 802.11 is only 40 bits. This limit was included to meet export restrictions in place at the time 802.11 was ratified. A 40-bit key is known to be quite weak given the inexpensive computer power available today to break encryption schemes. As a consequence, most vendors have implemented 128-bit (or greater) keys providing some added security.

While the 40-bit limitation in the standard will be removed in an update to 802.11 (currently under development by 802.11 "Task Group i", or "TGi"), other problems remain. These include the lack of key distribution, key management (both must be done manually), key rotation (an added security technique which changes security keys on a regular or irregular basis), and the fact that WEP only encrypts data over the air, between the access point and the client. A more end-to-end approach is required, ensuring that data appears in the clear only on authorized clients and servers. WEP also shares security keys among users, creating a big opportunity for keys (and thus the entire network) to be compromised.

Finally, in a highly-publicized recent series of technical papers and articles, it has been demonstrated that WEP (which is based on the well-known and widely implemented RSA RC4 algorithm) can be broken in close to real time, and can no longer be relied upon when subject to a dedicated attack (and, of course, it can be very difficult to determine if such an attack is underway in a wireless environment). Thus, WEP cannot be relied upon for complete security, and therefore network managers need to consider alternatives.

WEP is better than nothing and should be used as the first line of defense.

[3] http://80211-planet.webopedia.com/TERM/B/BOOTP.html

[4] http://80211-planet.webopedia.com/TERM/D/DHCP.html

Encryption of Management traffic.

Usually the way to manage the AP is by using HTTP, Telnet or Console port. Disable any HTTP or Telnet access if it's possible and enable HTTPS and SSH protocols to protect your management traffic. Refer item 5.- *Limit management traffic to a dedicated wired subnet & protected console access.*

This controlled access will permit us to be sure ONLY authenticated users will have access to our network resources.

Filtering and Access Control.

The AP provides facilities to limit our wireless Units (or Portable Data Units) that associate with it and the data packets that can forward through it. Filters can provide network security or improve performance by eliminating broadcast/multicast packets from radio transmissions.
The access control list contains the MAC addresses for Wireless Units allowed to associate with the AP. This provides security by preventing unauthorized access.
Depending on the settings, the AP can keep a list of frame types that it forwards or discards. Filtering out unnecessary frames can also improve performance.
An Access control list (ACL) is not viewed as an extremely secure method. Because MAC addresses, can be stolen and replicated (spoofed).

User authentication for the WLAN access & management interface.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point and to your network. But remember, this is the most important point in protecting the corporate network from hackers so this information should be sent in encrypted packets with the highest level of encryption level as possible.
For that reason, many of the larger WLAN vendors offer complete Wireless network implementations that patch the weaknesses in 802.11b security with a mixture of open standards and proprietary hardware and software.
In our case study we should consider implementing the IEEE 802.1x security standard because they are the only ones that can be applied in our existing infrastructure. Future implementations should be planned under the new WLAN security standard 802.11i, when the 802.11 Working Group ratifies this.

802.1X[5]

In theory, IEEE's 802.1X provides a vendor-independent way to control access to wireless networks by port control. In practice, it's not that simple.

While parts of 802.1X are indeed standard, it uses port control with dynamically varying encryption keys that can be automatically updated over the network with the Extensible Authentication Protocol (EAP)6 to enable user, not machine, authentication. To make all this happen, 802.1X uses RADIUS servers.

However, 802.1X doesn't require the use of Remote Authentication Dial-In User Service (RADIUS)7 authentication. Instead a variety of authentication methods, such as certificates, Kerberos8 and public key authentication can be supported. Which, in turn, means that your laptop, even if has 802.1X enabled and is trying to connect with a open WLAN won't be able to connect. Unless your client PC is running the same authentication method used by the 802.1X authenticator software behind the access point. For example, if you're using Cisco's Lightweight EAP (LEAP) on your laptop and the local access point uses Microsoft Point-to-Point Encryption (MPPE), there is no hope of making a connection.

How it works ?

802.1X Authentication for wireless LANs provides centralized, server-based authentication of end users.

[5] http://www.80211-planet.com/tutorials/article.php/1490451

[6] http://80211-planet.webopedia.com/TERM/E/EAP.html

[7] http://80211-planet.webopedia.com/TERM/R/RADIUS.html

[8] http://80211-planet.webopedia.com/TERM/R/RADIUS.html

1.- A client sends a “start” message to an access point, which request the identity of the client.
2.- The client replies with a response packet containing an identity, and the access point forwards the packet to an authentication server.
3.- The authentication server sends “an accept” packet to the access point.
4.- The access point places the client port in authorized state, and traffic is allowed to proceed.

802.11i

Task group "i" within the IEEE 802.11 is responsible for developing a new standard for WLAN security to replace the weak WEP (Wired Equivalent Privacy). The IEEE 802.11i standard utilizes the authentication schemes of 802.1X and EAP (Extensible Authentication Protocol) in addition to a new encryption scheme - AES (Advanced Encryption Standard)[9] and dynamic key distribution scheme - TKIP (Temporal Key Integrity Protocol).

TKIP, also known as WEP key hashing. This feature defends against an attack on WEP in which the intruder uses the unencrypted initialization vector (IV) in encrypted packets to calculate the WEP key. This removes the predictability that an intruder relies on to determine the WEP key by exploiting IVs.[10]

[9] http://www.rsasecurity.com/rsalabs/aes/

[10] Cisco Aironet 1200 Series Access Point Software Configura tion Guide. Page 8-4

Group 2: Wireless Devices

The following rules will help us to protect our clients or Wireless devices. This protection is necessary not only to allow our devices to be used like "relay devices" and see our network it compromised.

Disable Ad hoc or Peer to peer mode.

An 802.11 networking framework in which devices or stations communicate directly with each other, without the use of an access point (AP). Ad-hoc mode is also referred to as peer-to-peer mode or an Independent Basic Service Set (IBSS). Ad-hoc mode is useful for establishing a network where wireless infrastructure does not exist or where services are not required [11] but using widely available tools, hackers can force unsuspecting stations to connect to an undesired 802.11 network or alter the configuration of the station to operate in ad-hoc networking mode.
The malicious association attack shows that wireless LANs are subject to diversion and stations do not always know which network or access point they connect to.

Assign static IP or Filtered DHCP.

Even if an intruder is capable of associating with an access point by using the correct SSID, they must often have an applicable IP address before they can directly access resources (user PCs, servers, etc.) on the network. Many wireless LANs, though, use DHCP (dynamic host configuration protocol) to automatically assign IP addresses to users as they become active. With DHCP enabled, a hacker receives an applicable IP address just as other legitimate users do. This provides freedoms to the hacker you'd rather not share.[12]

But DHCP implementation will be allowed in case our Firewall will be able to interoperate with it.

DHCP is used to lease out individual IP addresses to anyone who configures their system to request one. Other vital information such as subnet mask, default gateway, and name server are also given to the client at this time. DHCP will perform with the additional ability to dynamically remove hosts from the firewall access list when DHCP releases a lease for any reason (client request, time-out, lease expiration, and so on).

The DHCP server will be configured to only listen on the subnet interface of the wireless network. This prevents anyone from the wired network to obtain a wireless IP address from this server. As an added security measure, packet filters prevent any DHCP requests coming in on any other interfaces.

[11] http://www.webopedia.com/TERM/a/ad_hoc_mode.html

[12] http://www.80211-planet.com/tutorials/article.php/1457211

Client Device Protection

If a hacker is successful in compromising a WLAN connected device they may be able to utilize that Client workstation as a relay device and further attack our network.

I've selected these two GIAC research projects because they are explaining in deep how to protect your home network and computer from Internet attacks. In our case, consider to substitute its Internet connection to our Wireless LAN and home computers for Laptops & PDAs with WLAN cards.

"In addition to destructive viruses, your computer could provide an excellent host for a distributed denial of service (DDoS) attack. In this scenario your computer is one of many computers being infected with a malicious program that could be used to flood another network, website, etc. with data, causing the attacked network to be unable to respond to legitimate requests."[13]

Security & Privacy at Home

"The purpose of this document is to provide some details of how to implement a layered security model that will provide "Security in Depth" for a small home network with an "always-on" internet connection." [14]

Security In-Depth for Home-based Networks with an "Always-on" Internet Connection

In our case study this is not applicable in most of our Wireless data collector terminals for Hardware and Software incompatibilities. But this item must be taken in consideration for new implementations and future client devices.

[13] http://www.giac.org/practical/Brian_Porter_GSEC.doc

[14] http://www.giac.org/practical/David_Gibson _GSEC.doc

Group 3: LAN Design

Our main goal will be to segregate or isolate each WLANs from the corporate Network and to provide our authenticated WLAN users access to the TN3270 server. This is covered in more detail in the following sections.

Isolate Wireless LAN.

Isolate your Wireless LAN installing the Access Points into a dedicated and separated LAN Infrastructure. Install a specific LAN infrastructure to plug your Access Points. This one should not be connected to the internal wired network or Corporate Network.

Assign a non routable sub-net to your Wireless LAN. Our Wireless LAN has to be completely isolated; this means it doesn't know how to get your Corporate Network.

Firewall installation between Corporate Network and Wireless LAN.

Firewalls protect organizations on the Internet by providing secure access: ensuring that valid users can access the network resources they need. Determining "who" is a valid user is the job of authentication, and determining "what" resources they can access and “how-is” are particulars of authorization, or Access Control.[15]

We will give the same treatment and importance to the Wireless LAN that is given to the Internet, and the Wireless LAN will be treated in a similar way to the Internet.

This Firewall will protect our Corporate Network and resources to direct Hacker attacks from the Wireless LAN. We are going to filter and restrict all traffic to our internal LAN services from any non-authorised user.

[15] http://www.checkpoint.com/products/protect/firewall -1_access.html

Our Firewall will have minimum three different areas or interfaces:

-Wireless Network: This interface will be connected to the Wireless LAN with all the AP's. It has to accept traffic from Wireless devices for the DHCP process, Authentication process and enable the TN3270 application ports (transport OSI layer ports) for those authenticated devices.

-DMZ area: This is called the demilitarized area and all services we would like to offer to our Wireless devices must be installed and running in the DMZ Servers.

-Corporate Network: This is our internal network. Our Administrators will have access from here to other Networks (WLAN & DMZ) to manage and monitor their devices and Servers but NOT vice-versa.

Our main goal will be to permit traffic from any "KNOWN" wireless device to our TN3270 Gateway. "KNOWN" device will be any authenticated Wireless device.

The access to authorized network resources will be managed & filtered by our Firewall applying access control lists (ACL). Any packet sent from the Wireless LAN will be accepted or denied based on packet type and other variables.

Following this configuration our Wireless devices will ONLY have the option to communicate through some specific ports with our server in the DMZ zone. They are not going to be allowed to access to any other server or service, and of course, all traffic to our Corporate Network will be dropped or blocked.

Administration.

Install a Wireless LAN monitoring mechanism capable of alerting administrators to attackers and rouge networks.

Wireless LAN Intrusion Detection System (WLAN IDS or WIDS) should permit the system administrators to monitor wireless LAN activity for denial of service attacks, rogue networks, accidental associations and several other system risks.

There is a well-known list of WLAN vulnerabilities but new wireless LAN hacking tools are introduced every day and are widely available to download on the Internet for everyone. So, our WIDS implementation must be based on a dynamically updated rule set.

WIDS, like Airdefense solution consists of distributed sensors and server appliances. The Remote Sensors sit near the 802.11 Access point to monitor all wireless LAN activities and report back to the server appliance, which analyzes the traffic in real time. [16]
Server Appliance will be our data collector and must be installed inside the firewall in a safest network because our sensors will be the attacker's first target.

[16] http://www.airdefense.net/products/airdefense_ids.shtm

Virtual Private Networking (VPN)

VPN is the most flexible method for creating secure end-to-end connection between stations. The data that is transmitted is encrypted: Data is encrypted at the source endpoint; rides the VPN scrambled WLAN, and are decrypted at the destination endpoint.

In our case study the Wireless Virtual Private Network (WVPN) creates a secure link or “tunnel” from a mobile PC, through the WLAN, and to the Firewall on the DMZ network. Through the use of end-to-end encryption, authentication, and access control, the WVPN enables authorized mobile users to reach ONLY their TN3270 sessions wirelessly while preventing unauthorized access to private network.

This is not applicable in most of our actual Wireless data collection terminals because our vendors are not supporting a VPN client Software. But this must be our standard solution for new WLAN implementations or all new WLAN client devices like Laptops or PDAs.

Conclusion

In this organization it is impossible to plan a Warehouse without a Wireless solution because they have experienced a tremendous growth in their availability and productivity.

Unfortunately with Wireless 802.11b standard implementation we've discovered so me security holes, which force us to securize and isolate our Wireless solution from the Corporate LAN. In this document we are creating a security strategy that could even be remotely described as impenetrable. Our main goal is to make it at least extremely difficult for unauthorized individuals to obtain access network resources and information.

It's important to point out here that no matter how good a given authentication & encryption technique might be, hackers and crackers are getting smarter all the time, and that's why is important to develop an Intruder Detection System strategy for monitoring and analyzing what is happening in your LAN/WLAN.

Next step will be to check how vendors will apply the new IEEE Security Wireless standards 802.11i, how fast are hackers to crack it, and which optional solutions we'll have to protect our new implementations.

References

Beyond WEP -By Steven J. Vaughan-Nichols - October 29th, 2002
http://www.80211-planet.com/tutorials/article.php/1490451

SAFE VPN - IPSec Virtual Private Networks in Depth - Jason Halpern – August 16th, 2001
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safev_wp.htm

Webcast: Top 3 Attack Tools Threatening Wireless LAN's – Joshua Wright – March 5th, 2003
http://www.sans.org/webcasts/030503.php

Microsoft Solution for Securing Wireless LANs – Microsoft Corp.- May 2003
http://go.microsoft.com/fwlink/?LinkId=14843

Wireless Security & Hacking - Danny aka Dr.T - July 2002
http://www.hackinthebox.org/article.php?sid=7948

Wireless LAN Security. What Hackers Know That You Don't – Airdefense - 2002.
http://www.airdefense.net/whitepapers/index.html

Understanding the Layers of Wireless LAN Security & Management – Airdefense – 2003
http://www.airdefense.net/whitepapers/index.html

Configuring the Cisco Wireless Security Suite – Cisco Systems Inc. – January 23rd 2003
http://www.cisco.com/en/US/netsol/ns110/ns175/ns176/ns178/networking_solutions_white_paper09186a00800b3d27.shtml

Wireless LAN Security Crackdown - Jason Brooks - May 6, 2002
http://www.eweek.com/article2/0,3959,9204,00.asp

Ten Steps to a Secure Wireless Network - K. Karagiannis, PC Magazine, - February 25, 2003
http://www.pcmag.com/article2/0,4149,844020,00.asp

Spectrum24 Access Point AP-302X: Product Reference Guide
Symbol Technologies – September 2000

Wireless Security exposed - By IT Manager Special, CNETAsia.- December 9th, 2002
http://asia.cnet.com/itmanager/specialreports/0,39006603,39100800,00.htm

Wireless Security: IT's like securing your Home – Intermec - 2002
http://epsfiles.intermec.com/eps_files/eps_wp/WirelessSecureWPWEB.pdf

Wireless LAN Basics – Intermec- 2002
http://epsfiles.intermec.com/eps_files/eps_wp/WirelessSecureWPWEB.pdf

Cisco SAFE: Wireless LAN Security in Depth Version 2 – Cisco Systems Inc - Sean Convery (CCIE #4232), Darrin Miller (CCIE #6447), and Sri Sundaralingam http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml

802.11 Wireless Networks: The Definitive Guide - By Matthew Gast
April 2002

Seven Security Problems of 802.11 Wireless -Matthew Gast – May 24th 2002
http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html