Global Information Assurance Certification Paper

Doug Bulthuis
GSEC Practical Assignment
Version 1.4b (amended August 29, 2002)

Title:
A presentation to management on wireless security concepts.

Abstract:
In my position as a security analyst for a medium sized manufacturing firm, my department has seen wireless devices starting to be used in the warehouses, and even some connections to the network taking place. Currently, we have no policies in place to set any standards or provide any direction, but have recognized this medium will continue to grow, and getting in front of it is imperative. This paper will cover the background of wireless, its benefits, what the security risks are, where the future of wireless seems to be going, and then define some policies we can use to provide some direction.

Overview
It doesn't take a lot of imagination to see that connecting to the company network without being tethered to your desk by the typical wired network connection would boost productivity. The ability to just grab your laptop and work from the cafeteria or a conference room while still maintaining access to email and other network data would greatly boost efficiency.

"In November 2001, an independent study by NOP World - one of the world's largest research and business information companies - found that WLANs enabled end users to stay connected an additional 1.75 hours each day, resulting in an increase in productivity of up to 22 percent." (3) A further benefit of wireless that's not as obvious is the cost savings. The ability of the network team to add new PCs without having to string the Ethernet cable will save both the cost of the cable and time spent doing it. This also improves the flexibility of the end users, and allows them to move PCs and printers almost anywhere, ideal for companies with high employee turnover. The Gartner Group recently measured the total cost of ownership (TCO) of a medium-sized office of 250 people using wireless as an extension to their wired LAN, which would be similar to my company's situation. They determined the TCO for this wireless scenario to be $3,052 per user annually, compared to $5,000 for the fully wired. The numbers included initial investment in hardware and software, time and effort of setup, and on-going management and support. (11)

Background
If you've watched any Television lately, you have undoubtedly seen some of Intel's latest marketing blitz to promote **Centrino**, a combination of its new processor, the 855 chipset, and their Wireless Pro solution (based on 802.11b standard). While this technology isn't exactly new, the advertising to a main stream, less technical audience, will no doubt increase end users curiosity, and

most likely their desire to have the latest technology. This increases the importance of our department having standards in place.

Before we can make a recommendation to management on a wireless security policy, we need to look at some of the technology behind a wireless network, and what issues are present.

Wireless operates as a broadcast medium over open radio frequencies. This means anyone with the correct hardware is capable of eavesdropping provided they are in range of the signal. To circumvent these uninvited guests, two things must be considered namely encryption and authentication. The Institute of Electrical and Electronics Engineers, Inc. (IEEE) has developed the 802.11b standard in an attempt to address both criteria. The protocol behind this standard is WEP, or Wired Equivalent Privacy.

WEP

Wired Equivalent Privacy was developed using the RC4 encryption algorithm. RC4 is a stream cipher developed in 1987 by Ron Rivest for RSA Data security. (6) Without getting too technical, "A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce ciphertext. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the ciphertext yields the original plaintext." (7) During this encryption process, the shared key mentioned above is concatenated with a 24-bit initialization vector (IV), the output of which is a keyschedule or "seed." This "seed" is then input into a pseudo-random number generator to produce the keystream.

WEP's weakness

The weakness of WEP relates to its "relatively short IVs and keys that remain static" (8), rather than the encryption algorithm. The problem with having a short, 24-bit, initialization vector, is that on a busy network, eventually WEP uses the same IV for different data packets. The result of this is frame transmissions with very similar keystreams. Once this happens, an eavesdropper can determine the shared values among them if they are able to collect enough frames with the same IV. This may sound a bit complicated, but tools like AirSnort and WEPCrack are readily available, and will allow "a hacker with minimal technical knowledge to break into a WEP-enabled wireless network, without being detected, in no more than a few hours."(9)

Other security issues of 802.11 include:

- No per-packet authentication
- Vulnerability to disassociation attacks
- No user identification and authentication
- No central authentication, authorization, and accounting support
- RC4 stream cipher is vulnerable to known plaintext attacks
- Some implementations derive WEP keys from passwords

- No support for extended authentication; for example: token cards; certificates/smart-cards; one-time passwords; biometrics; etc. (5)

IEEE standards

When we talk about the IEEE standards, we generally are referring to 802.11b. This is due to it having the broadest array of commercial products and being the most widely deployed WLAN standard. 802.11b has a data rate of 11Mbps over 3 available channels, a range of 150 feet indoors, and uses the 2.4GHz frequency. The IEEE also has other standards that both exist and are being developed. Two we will look at are 802.11a and 802.11g. Although neither of these 2 addresses the shortcomings of WEP, they do offer improvements on 802.11b.

802.11a operates in the less crowded 5GHz radio band, and has 8 available channels. It also has a higher through put of 54Mbps, but the range is limited to 60 feet indoors. It is important to note that 802.11a and 802.11b are not interoperable. This is important because if a company has the 802.11b infrastructure in place, the move to 802.11a to gain the higher speed will be expensive due to the need to replace access points, etc. A company like ours with little or no existing wireless equipment will want to consider starting with 802.11a or 802.11g.

Due to the conflict with 802.11a and 802.11b, the 802.11g standard was developed, and is basically a combination of the previous 2. The key to 802.11g is it having backward compatibility. It will operate at the higher transmission rate of 54Mbps, and will allow organizations having 802.11b in place to upgrade without scrapping that entire original investment.

Robust Security Network

To address the limitations of WEP, the IEEE formed the 802.11i task group. This group is working on the Robust Security Network (RSN) standard. This draft standard entails 2 components: the Advanced Encryption Standard (AES) for encrypting WLAN traffic and the new 802.1x security standard for user authentication and key management.

The 802.1x standard

802.1x is port based, and utilizes EAP, Extensible Authentication Protocol. It is important to note that there are several EAP methods, some of which are less secure, and will be discussed below. A strong EAP method will use an authentication server to provide mutual authentication, and also offers dynamic per-user, per-session WEP keys. By using an authentication server such as RADIUS, authentication is based on the user rather than the device. RADIUS tends to be the overwhelming favorite due to it already existing in most networks that have users connecting remotely. With 802.1x in place, a stolen or lost laptop no longer compromises network data.

In order to utilize 802.1x, three criteria must be met:

- The user must have an 802.1x client that supports EAP
- Access points must be 802.1x complaint
- Radius server must support a strong EAP, e.g. EAP-TTLS

These three criteria can present a problem for companies with wireless equipment already in place due to the need to update the equipment. A company like ours with no equipment in place will have an advantage in that we can install the latest product, most of which comes 802.1x complaint out of the box.

EAP types

The Extensible Authentication Protocol is a general protocol for point to point authentication. The key here is that it supports multiple authentication mechanisms. This allows the selection of a specific authentication type to be postponed until the Authentication Phase, which will then permit the use of a "back-end" server like RADIUS.

There are several different types of EAP authentication, and each has different features and weaknesses, and some will work better given a set of existing criteria. The table below highlights the most popular EAP types.

The Popular EAP-over-LAN Authentication types, courtesy of Atheros Communications, Inc. (1)

EAP-MD5	- Password based authentication, widely disregarded due to no mechanism for secure key exchange
EAP-TLS (transport layer security)	- Fairly complex to setup - Requires a RADIUS server and digital certificates at both the station and RADIUS server - Windows XP supports TLS natively
LEAP (EAP Cisco Wireless)	- Effective for networks still using WEP-based devices - Password-based mutual authentication with RADIUS - Regularly refreshed WEP keys - Access point authenticator functionality limited to CISCO equipment
EAP-TTLS (tunneled TLS), similar to PEAP (protected EAP)	- Both types are supported by wide range of wireless companies - They use digital certificates, but only on the RADIUS side - Station will authenticate RADIUS using the server's certificate and then a secure tunnel can be setup through which the RADIUS server can authenticate the station

Due to the ease in administration when compared to EAP-TLS, the general consensus is that EAP-TTLS is the authentication mechanism of choice.

Example of EAP-TTLS connection

It is beneficial to look at how a connection is established using 802.1x. Here is a simplified explanation of the steps based on the EAP-TTLS. "In an 802.1x-based environment, the access point essentially acts as a conduit between the Client and the RADIUS server during the user authentication phase. So, via the access

point, the WLAN Client and the RADIUS server negotiate to determine which EAP authentication method to use. Once agreed upon, the secure tunnel is set up, through which the user's credentials are passed from Client to RADIUS server. The RADIUS server authenticates the user to determine if he is allowed access to the network. Once the user has been granted access, the RADIUS server issues an encryption key to the access point, which then sets up the secure, encrypted session. The RADIUS server may also be called upon to re-key during the session, to maintain data privacy." (14)

AES – Advanced Encryption Standard

The AES is the product of a three-year worldwide competition conducted by the National Institute of Standards and Technology (NIST). Their overall goal was to develop a replacement for the Data Encryption Standard (DES), and provide a new Federal Information Processing Standard (FIPS). The criteria for any algorithm submitted was that it be publicly disclosed and available royalty- free through out the world. Almost two dozen entries were received from 12 different countries, from which a list of five finalists were selected.

These five finalists were intensely evaluated by the international community of cryptography experts. Based on the combination of security, speed and versatility of implementation, the Rijndael algorithm was announced as the winner. Dr. Vincent Rijmen and Dr. Joan Daemen, both Belgian cryptographers submitted Rijndael.

The Future of Wireless

The future will surely involve the Robust Security Network (RSN) standard once it is adopted. For the mean time, the IEEE 802.11i task group has formulated the Temporal Key Integrity Protocol (TKIP). It was developed "as a short-term encryption solution that offers a reasonable compromise between adding security and limiting the performance of existing CPU-constrained 802.11b products." (1)

TKIP enhances the WEP algorithm by adding a message integrity check, and the ability to delete the current WEP key if an attack is detected. TKIP also has a per-packet key mixing function and replay protection. However, this added security still doesn't match AES, and should only be implemented on a temporary basis as a bandage.

Company Specific recommendations

Now that we have discussed the background of wireless, we will be looking at recommendations for our company specifically. We are a manufacturing firm, with about 1000 users at our corporate location, and roughly another 200 users located at 4 plants/distribution centers within 200 miles that are connected to corporate via a T1 line. Our corporate infrastructure consists of dual Cisco Pix firewalls that border the DMZ that house our web servers. Inside the firewall, we have a VPN server from Nortel, an RSA ACE server for token-based

authentication, and a RADIUS server. These 3 devices give us some flexibility when considering options to secure our wireless connections.

Because the different options have varying degrees of security, it is necessary to consider the risk to the business if the data being transmitted was to be compromised. To do this, we classify the data we are trying to protect into 3 different levels of risk, and we will then propose different levels of security based on that rating. The data rating is based on the following criteria:

Low—Information that may be made available to any employee or non-employee because its disclosure poses no risk to the company. Low areas of risk can be broken in to two areas:

- **Proprietary Information:** Information such as newsletters.
- **Financial Information:** Information such as annual reports.

Weighting: 9 is low, 8 is medium, 7 is high (within this category)
Example: L9 = Low Low, L8 = Low Medium, L7 = Low High

Medium—Information that may be made available to any company employee, but not to anyone else without specific authorization from the data owner because its disclosure to non-employees could expose the company to some risk. Medium areas of risk can be broken into two areas:

- **Proprietary Information**: Information such as corporate policy documents and employee telephone directories.
- **Financial Information**: Information such as parts inventories.

Weighting: 6 is low, 5 is medium, 4 is high (within this category)
Example: M6 = Medium Low, M5 = Medium Medium, M4 = Medium High

High— Information that may be made available only to a limited number of employees because its disclosure to unauthorized individuals could expose the company to significant risk. High areas of risk can be broken into two areas:

- **Proprietary Information**: Information such as engineering schematics, security codes, acquisition information, legal documents, medical data and non-public personally identifiable customer information.
- **Financial Information**: Information such as financial data, credit card numbers and employee compensation.

Weighting: 3 is low, 2 is medium, 1 is high (within this category)
Example: H3 = High Low, H2 = High Medium, H1 = High High

Specific recommendations for different Scenarios
Because our company has very limited wireless exposure currently, we are in a good position to benefit from the latest and most security intense standards without having to worry about device interoperability. Having no equipment in place will allow us, once we decide which route to go, to install the latest, and most up to date equipment.

For these installs, we will be looking at 3 different scenarios, namely:
1. Access in warehouse and distribution centers
2. Traveling Sales Force
3. Wandering Executive

The first scenario is also the simplest. Because the data being transmitted is mostly serial numbers and inventory levels, and the server this data resides on is isolated from the corporate network shares, this data is classified in the low risk range. Therefore, the policy we recommend for this is as follows.
- Enable WEP
- Change the SSID's from the default
- Use MAC filtering on the access point

Filtering of the MAC address' can be an administrative head ache if the number of users is high, but shouldn't be a problem for this scenario due to the limited number of users with this access.

The next concern is our traveling sales force. We rate the data they access in the medium to high category. For these users, we consider two scenarios. One is inside corporate headquarters, connection via company owned access point. The second is being out in the field, access via public hot spot like an airport or coffee shop. We assume these users have company owned laptops with a standard image, and a VPN client loaded.

For the users connecting within the corporate environment, we recommend:
- WEP enabled with TKIP to enhance key rotation
- Authentication via RADIUS.

This solution offers users that can't authenticate the ability to still gain internet access if we have dual-mode access points that will support virtual LANs. The AP is configured to allow secure traffic directly onto the network, and route non-secure traffic outside the firewall. This will be a nice feature for users visiting corporate that need to check email via the web, etc.

For users connecting on a public access point, we will require a VPN connection. This will provide an encrypted tunnel from their laptop to within the company firewall. Requiring a token\PIN combination validated by our RSA server will strengthen authentication.

Lastly is the recommendation for users accessing our most confidential data, the wandering executive.

- Client must be 802.1x compatible
- Encryption via AES
- Authentication via RADIUS, using EAP-TTLS

We feel that EAP-TTLS is the best fit for us when compared to the other popular EAP types, criteria being ease of administration and level of security.

General Guidelines

- The first, and probably most important recommendation will be that prior to any new wireless being rolled out, the requestor must demonstrate a clear business need. Just having wireless because it's a cool technology is not enough to justify the risk.
- Another generic recommendation is looking at our file structure, and making sure only information, drives, and computers that need sharing, are shared. The others will be kept private.

Equipment Policies

- All wireless Access Points (AP) connected to the corporate network must be registered and approved by corporate security team. Any unregistered AP is strictly forbidden and may be removed without notification.
- All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers must be registered with the corporate security team.
- AP configuration only allowed by a wired connection, and AP's are password protected.
- Service Set Identifiers (SSID's) on AP must be changed from the default.
- Access points should be powered off during non-business hours.
- WLAN hardware should be purchased from selected vendors whose products support our deployed security measures.
- Anti-Virus software installed on all laptops.

Performance Policies

- When 15 or more clients connect to any one access point, an alert will be generated to the network manager.
- The busy access points will have their data rates lowered to prevent a few clients from monopolizing bandwidth.

Financial Analysis

This paper wouldn't be complete without a look at the effect the different scenarios have on the bottom line. As is the case with most products, as the features increase, so does the price tag, and wireless is no exception. The trick becomes balancing a level of security that we as a department, and ultimately management, will be comfortable with, while at the same time offering the end user ease of access. In other words, anything too cumbersome, and they won't use it at all.

Defense in Depth
We realize that a single security initiative by itself will not provide complete protection for our wireless connections. But by combining several approaches or guidelines, we can mitigate our exposure to an acceptable level of risk. These "layers" include physical security, end-user education and awareness, technical standards, and finally policies that are well communicated. The end user needs to be aware that a policy exists, otherwise we have nothing to enforce the results of our auditing against. This is our philosophy for enterprise wide security in general, and will be our approach for wireless as well.

Conclusion
Although no one solution is going to be 100% effective, by practicing defense in depth, we can mitigate the risk to a level the business is willing to accept. We will do this by combining a well-outlined and documented policy along with the latest standards from the IEEE once they are adopted. It is worth noting that without management buy in, the policy can't be effective.

References:

1. “Building A Secure Wireless Network: How Atheros Defines Wireless Network Security Today and in the Future”, Atheros White Paper, URL: http://www.atheros.com/pt/atheros_security_whitepaper.pdf

2. Rysavy, Peter “Planning and Implementing Wireless LANs”, URL: http://www.networkcomputing.com/netdesign/wlan1.html

3. “Why Wireless LANs?” Cisco Aironet Wireless LAN Security Overview, URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

4. “Secure Authentication, Access Control, and Data Privacy on Wireless LANs” URL: http://www.funk.com/radius/Solns/wlan_ody_wp.asp

5. Ayyagari, Arun and Fout, Tom “Making IEEE 802.11 Networks Enterprise-Ready”, Microsoft Corporation White Paper, May 2001, URL: http://www.wlana.org/learn/security.htm

6. Weatherspoon, Sultan. "Overview of IEEE 802.11b Security." URL: http://developer.intel.com/technology/itj/q22000/pdf/art_5.pdf

7. Borisov, Nikita, Goldberg, Ian, Wagner, David “Security of the WEP algorithm”, URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

8. Geier, Jim “802.11 WEP: Concepts and Vulnerability”, URL: http://www.80211-planet.com/tutorials/article.php/1368661

9. Janszen, Eric, “Understanding Basic WLAN Security Issues.” URL: http://www.80211-planet.com/tutorials/article.php/953561 January 11, 2002

10. Phifer, Lisa, “Improving WLAN Security”, November 26, 2001. URL: http://www.80211-planet.com/columns/article.php/928471

11. “Learn to be free,” Wireless Reference Guide by CDW, URL: www.cdw.com/wirelessguide

12. Mishra, Arunesh and Arbaugh, William, “An Initial Security Analysis of the IEEE 802.1x Standard,” February 6, 2002, URL: http://www.cs.umd.edu/~waa/1x.pdf

13. Baily, Scott, **“**Is IEEE 802.1X Ready for General Deployment?” April 17, 2002, URL: http://www.sans.org/rr/casestudies/deployment.php

14. “Architecting Your 802.1x-Based WLAN Deployment Using Odyssey™ and Steel-Belted Radius®,” A white paper by Funk Software, October 2002 URL: http://www.funk.com/radius/Solns/architecting_wlan_wp.asp

15. McAleer, Sean, “A Defense-in-Depth Approach for Securing Mobile Devices and Wireless LANs”, January 24, 2001, URL: http://www.sans.org/rr/wireless/defense.php

16. Craiger, J. Philip, “802.11, 802.1x, and Wireless Security”, June 23, 2002, URL: http://www.sans.org/rr/wireless/80211.php

Glossary of terms:

AES – Advanced Encryption Standard
DES – Data Encryption Standard
EAP - Extensible Authentication Protocol
EAP-TTLS – EAP w/ Tunneled Transport Layer Security
EAP-TLS – EAP w/ Transport Layer Security
IEEE – Institute of Electrical and Electronics Engineers, Inc.,
ICV – Integrity Check Value
IV – Initialization Vector
MAC - Media Access Control
RSN – Robust Security Network
SSID – Service Set Identifiers
TKIP – Temporal Key Integrity Protocol
WEP – Wired Equivalent Privacy