Global Information Assurance Certification Paper

A Practical Look at Wireless Security

Arthur King

January 6 2003

Version 1.4b Option 2

Abstract

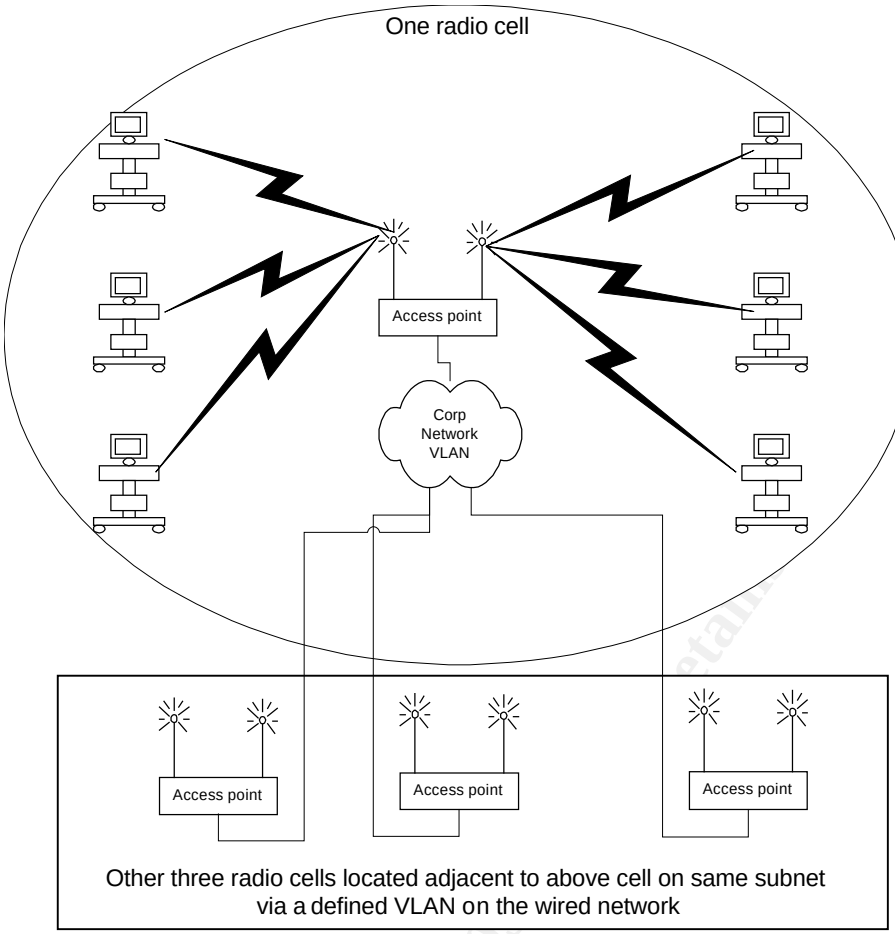
Internet Security Systems White paper states, "Without a doubt, wireless LANs have a high gee-whiz factor" (Wireless LAN, p1). Wireless networks can provide vastly improved processes and will save many companies thousands of dollars. With many companies wanting to be considered high-tech and the large savings, there is intense pressure to provide these networks. While everyone with any knowledge of 802.11 knows, wireless security is almost impossible. All security officers , myself included, would like a perfectly secure network in our dreams. Eventually we wake up and find we live in a world of budgets, limited staffing, and politics. I have titled this paper, "A Practical Look at Wireless Security", since I will look at the practical side of implementing our Wireless 802.11b network security. This paper will describe our prior configuration then go into the practical steps we took to reasonably secure our Wireless network until additional tools and resources can be budgeted. I will explain the decision processes we reviewed to decide on our level of security. Many factors were considered when deciding how many layers of security would be activated. This paper is targeted at the Cisco® product line as this is the product line we have installed. I will also only address the security settings with the assumption that the wireless network already exists.

Beginning Snapshot

Our prior 802.11b configuration was and is small and does not handle sensitive data. The fact remains that any access into our network needs to be secure so our other network subnets do not get compromised. There are only 4 wireless access points installed with 6 wireless devices being used.

To illustrate the difference between before and after network designs, I will reference the same 6 topics in both the before and after snapshots.

1) Our radio signal is not limited to our facility so public availability to our network for eavesdropping is a very large area.
2) Our SSID is not being sent out for all to hear.
3) We limited our wireless to a single subnet, but had not connected it to our wired network via a firewall.
4) As mentioned above, we were not using a firewall so IP Filtering for address and port was not being done.
5) We had not implemented MAC address filtering to limit the connection of rouge devices.
6) We had not implemented WEP encryption at all.



Before snapshot

Setting the project scope

The idea is to implement as many security layers as possible with a watchful eye on resources and cost. As taught in the basic GSEC course, layered security is a very good approach. I wanted our initial implementation to use only the standard security tools not any proprietary protocols. The user environment is also a concern. If the network administrators require authentication using one time password key phoebes or even extra logins to the wireless environment, some of the benefits of wireless that increase productivity will be lost. One of the strongest features of wireless is instant access to online data. If a user must log onto the wireless, then onto the corporate network to map data drives, and then onto the application used to access the database you can see how frustrating and inefficient this could be. A network administrator can be seen as a failure or roadblock to progress if the technology cannot be implemented with a very seamless authentication. In the current environment, the data traveling on the network is not that sensitive. The fact remains that we must do whatever we can to protect our wired network from penetration by a hacker.

Common Practice

1) Radio placement and output power
I know most papers on wireless security do not address this topic but it can really lessen your exposure to eavesdropping if you take the time to set up and place the radio properly. By placing the radio away from the outside walls of your building, you can limit the area external to your facility the signal can be eavesdropped on. If the placement of the radio is near an outside wall, most units can have the signal strength lowered to accomplish the same effect. Of course this technique is limited because you usually want as strong and as much coverage as you can.

2) Not broadcasting the Set Service Identifier (SSID)
This is the first step to configuring and securing wireless. The SSID is required for a client to connect to an access point automatically. By default most Access Points broadcast this information to allow automated connectivity by the clients. Clients can connect without this broadcast if they are manually assigned to the SSID of the access point. It is very simple to turn off the broadcast and this slows the eavesdroppers by a few minutes. It is just one layer to securing our wireless.

3) Isolate the wireless to a single subnet
By isolating the wireless Access Points to a single subnet you can attach the entire subnet to your wireless network via a filtered connection in a router or better yet a firewall. This concept can be used even across very large campus environments if your wired LAN supports VLAN technology. Although, you may not want all your wireless clients to have the same access to the wired network. You could connect each wireless environment separately to your wired network with different firewall filters.

4) Consistent hardware manufacturer
This allows for more security layers as many manufactures have some proprietary security protocols. The down side of using a proprietary protocol is the Access Points and the client radios must all be the same manufacturer. The up side is some of these protocols are very powerful.

5) Isolating the Wireless Subnet via a Demilitarized Zone (DMZ)
As mentioned above, if you limit your wireless to one subnet you can attach them to your wired network via a DMZ created by a firewall. This could be done on several subnets in your network. The more you limit the number of subnets the easier it is to maintain.

6) MAC addresses Filtering
This is a list of Media Access Control (MAC) addresses predefined in the Access Point. The Access Point will only allow the clients with one of these addresses to connect to the wireless network. This security layer may have been effective years ago when MAC addresses were burned onto the Network Interface Card (NIC) itself. Now that many devices allow for the

software addressing of the NIC these filtered addresses can be mimicked. The problem here is, as described above, this may keep out an amateur but anyone with the tools and skills can break this in minutes.

7) IP Protocol Filtering

To allow for protection from a hacker of your wireless network doing some damage to your wired network, you should limit the connections to your wired network at the point of connection. This IP filtering can be done with a router using extended ACL lists or can be more restrictive with a firewall. By using a firewall instead of a router you can restrict by network port and do logging to alarm of attempts by a hacker breaking in.

8) WEP encryption

After reviewing a document from the Wireless Ethernet Compatibility Alliance, Wired Equivalent Protocol (WEP) was designed as a standard to make wireless secure by encrypting everything sent across the airwaves. The problem is, like most security tools, there is always a group of individuals who have nothing better to do than find ways to break a security protocol. Perhaps we should thank them for exposing a weak standard. The fact remains, that with a very available tool a person can crack the encryption key. They only need to capture approximately 1 million packets by eavesdropping and to have enough information to calculate the encryption key. Once they have the encryption key, they can capture all data following on the radio network including login and passwords to other systems.

9) EAP-TLS

Extensible Authentication Protocol (EAP), which is a Transport Layer Security (TLS), is part of the new IEEE 802.1X standards for both wired and wireless security. “This standard provides WLANs with strong, mutual authentication between a client and an authentication server. In addition, 802.1X can provide dynamic per-user, per session WEP keys, removing the administrative burden and security issues surrounding static WEP keys” (Cisco Aironet, p 5).

10)LEAP

This is Cisco Wireless proprietary version of EAP. The EAP-Cisco access WLAN can also support non-wireless clients with a workgroup bridge. LEAP can provide good security and removes many of the problems of key management. To do this several pieces of hardware are necessary. When using this protocol, a network designer must consider the availability of these devices to provide connectivity for the wireless environment. Cisco’s paper entitled, “Wireless LAN Security in Depth”, states that the authentication and key management systems must be available also. To make your wireless highly available you must also make your DHCP and RADIUS services highly available. This could add additional cost to the securing of your wireless network. In the documentation I read it seems that the login process would be passed as plain text. I would do more investigation before implementing this

11) TKIP

Temporal Key Integrity Protocol (TKIP) which is a standard Cisco supports. When you couple this protocol with Message Integrity Check (MIC), per-packet key hashing, and broadcast key rotation you have a very powerful weapon against wireless network intrusion. All of these security protocols used together make for a very powerful security system.

12) Rouge Access Point Detection

Rouge access points are a problem because access points can virtually be taken out of the box and connected to the wired network in minutes. So even if a network administrator secures the known access points a rouge can be set up without his/her knowledge. Even a well-meaning employee at a remote site may bring up a wireless network for legitimate business use and cause a huge whole in your network security. I have heard of some Intrusion Detection Service (IDS) devices being able to detect rouge devices by MAC address lists. I have not, however, investigated how successfully this works. While researching for this project, I found an interesting application that is sold by "WaveLink" called Mobile Manager. In their paper on Wireless Security, they describe many ways of securing wireless with their product and one of the techniques seems very interesting. In the documentation from Wavelink they explain the process they use to neutralize a rouge AP. Upon identification of a rouge AP the Wavelink software instantly downloads a default profile to the AP. In this default profile restrictions have been configured that eliminate its ability to communicate with the network. I feel this is a very clever approach to neutralizing rouge APs. The article did not explain how they identify a rouge AP has joined the network It sounded like it might be worth investigating when budget money is available.

After reviewing the tools listed above we needed to analyze how much security we could afford to implement at this time. Of the tools listed above, several can be done with little or no cost. We decided to use the first 8 layers listed above with the following reasoning. We felt that the fact we could limit the exposure to our wired LAN severely because the wireless units we currently run are very limited as to where they need to go. The network they attach to require a login and password as does the servers they attach to. The connections made by our clients are for very short periods of time, which could limit the WEP encryption cracking because the hacker would have a hard time gathering enough packets. The time we would need to survive with less than great security would only be a few months. We would need time to develop a wireless security policy. We also would need time to implement new procedures to allow for a wireless login which would allow for the more secure protocols listed above. The following are the steps we took to secure our network to this level.

We also decided to standardize our hardware now before purchasing any more equipment. We only needed to change out 4 clients, which will prepare us for

future implementation of some proprietary security layers, if we choose to go that direction.

After studying Chapter 2 of the Cisco AVVID documentation, the radio placement and adjustment is not as easy as just checking to see if the signal extends beyond the walls of your facility and if so how far. Also, the speed can be affected by the placement of the radios. The weaker the signal the less throughput the wireless LAN has. Referring to Figure 1 below the building is represented by the rectangle and the circle is the radio coverage area. Given the signal strength begins to lessen at the fringe, this design does not serve your clients well for throughput and allows for a large area of public exposure at the top and bottom of the diagram. Referring to Figure 2 you can see that by using 2 APs instead of 1 you can get even better coverage and not expose your radio signal to as large a public area.

Figure 3 shows a solution to another concern with wireless. Because wireless APs are much like a network hub with respect to bandwidth, all clients in the same cell share the 11 or 54 Meg throughput. To solve this problem you can lower the signal strength and increase the number of cells. This will effectively lower the number of clients that are in a single cell at the same time. One concern you have, when using multiple radios in the same space is making sure that you don't use the same channel in the same overlapping space. In North America, we can use 3 channels 1, 6, and 11. Cisco automatically selects the best channel when booting up. In very complex layouts, you may want to set the channels manually for optimum performance. There is another interesting performance problem on 802.11x. As a client moves to the fringe areas of a cell the bandwidth is automatically decreased. This not only has the obvious hit on performance but also causes another problem with broadcasts and multicast packets. A broadcast or multicast packet is sent out at the lowest baud rate being used by any client in the cell. If you have just one client at a fringe signal area every client gets the broadcast at that lower rate. This can severely bottleneck traffic and care should be taken to limit broadcast traffic.
The Cisco products we used were 350 Access Points. They have several features that we liked and were only a few dollars more than the 340s. The 350 APs differ from the 340s in three ways.

- They can be line powered. We have found this to be very helpful because the location for these APs frequently does not have power available. We also believe that locating the power plugs in a network closet is more secure than having them accessible to perhaps more public areas.
- The 350 have 100 mw power output verses the 340 and many other manufacturers have only 30mw.
- The packet-forwarding rate is twice that of the 340 model.

To adjust the power settings for the Ap350 select "Hardware" on the **AP Radio** Line from the opening screen. You can then select the power setting from the pull

down menu. The choices are 1, 5, 20, 30, 50, and 100mw. Remember the plan is to reduce the signal as far as you can and still maintain a strong signal for the whole coverage area you are trying to serve.

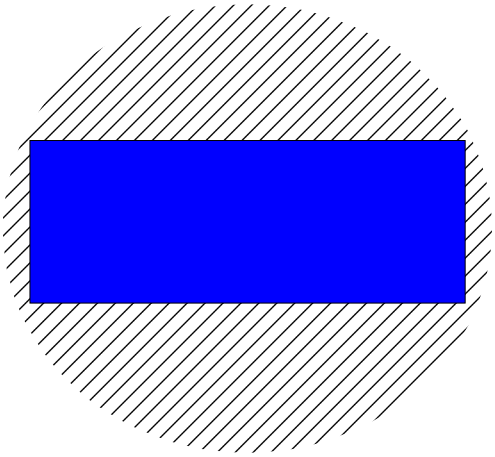


Figure 1
Using one radio leaving a large public exposure

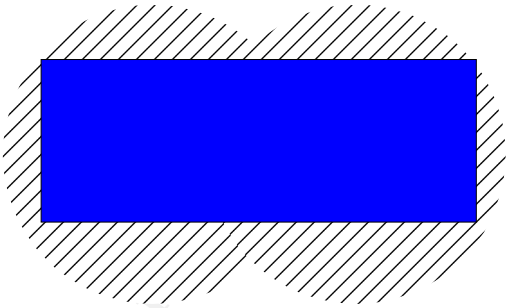


Figure 2
Using 2 radios vastly reduced public exposure

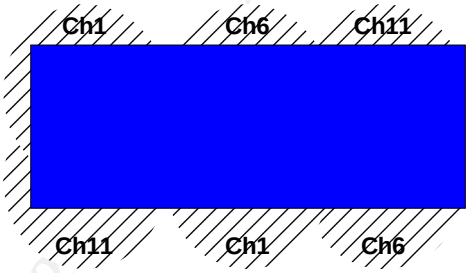


Figure 3
Showing improved throughput model with 6 radios. Still having less public exposure than figure 1

For all three of the figures above the hashed area represents radio signals. The shaded retangle represents the building

While you are on this screen, you can click one field and stop the broadcasting of the SSID. Select the second line down with the prompt “Allow Broadcast SSID” to Associate. Select the radio knob next to “NO” and that will turn SSID broadcasting off.

The concept of putting all radios on a single subnet was a lesson learned from a previous attempt to install a 2Meg wireless bridge a couple years ago. We learned, for a different reason than security, you want to isolate the wireless LAN from your wired network for performance reasons. The bridge was so slow that the broadcasts from our wired network flooded it. Because of this, we have already isolated the wireless network. As mentioned above, this is also a good concept for helping to manage your wireless network security. We then attached

our wireless subnet to our wired network through a firewall to enable the IP protocol filtering. We found that we only needed a few rules to allow the clients to get were they needed to go. We also found it helpful to think of the clients as if they were on the Internet when setting rules. I'm not going to go into the rule creation here except to say we analyzed the exact IP address and ports needed and only opened those. By blocking all ports not needed, we lessened the possibility of a Denial Of Service attack on our wired network as well as many other hacks.

We felt that even with MAC address filtering not being scalable we could maintain it for now because our wireless network is so small. Keeping the MAC addresses current could be a huge task if you had several hundred PDAs or tablets attaching to your wireless network. We have only a few addresses to manage so it should be a small task for the additional layer of security. To create a MAC address filter list, select "Address Filters" from the express Setup screen. You must decide if you want to allow or disallow the address you are entering. This is a simple concept. You want to allow only the devices you know about. We all know that the hacker out there can change his MAC to be the same as yours, yet it is still another layer he must know to crack your network. From this screen you can also remove MACs from the list if a remote unit fails or is stolen.

Using the Cisco WLAN document, we set up our wireless to use static WEP Key encryption. As you work through the documentation on activating this protocol, you will begin to see how difficult it would be to manage this manually for a large network. Each device on the same wireless network must have the same keys statically added to their configuration. One WEP key is 10 or 26 hexadecimal characters depending on your encryption level. Each device has potentially 4 keys, 4 assigned to the client transmit connection and 4 assigned to the AP transmit connection. If a unit were compromised or stolen, we would need to change 4 field entries in 10 devices. We can do this now with 10 devices, however, as we expand our network, it would be unmanageable. We originally chose the highest level of encryption, which is 128-bit, because we had all Cisco equipment. The standard is 40-bit encryption. We later dropped back to 40 bit because the long encryption keys we difficult to manage. The document walked through every step of applying the WEP key to both the client and the AP. Make sure you follow the document very carefully or the security derived from this may not be as good as you think. I know that this security measure is only a small deterrent for a skillful hacker, given the fact that we only transmit small amounts of data at a time and the non-sensitive nature of our wireless data. We will also implement a policy to select a different WEP key for client and AP transmission every month. This can be done easily as long as all the WEP key fields have been entered initially. I believe we can sleep at night until we get the funding to add additional layers. To set up WEP encryption the following must be done.

Decide what type of Authentication you want our choice was "**Open"**. That is also recommended by Cisco. The reason is, "Shared" sends a string unencrypted to

the client that is attempting connection. The client sends it back encrypted using its WEP Key. The client is authenticated if the AP can unencrypt the message using its WEP key. The problem is, if a hacker captures the plain text probe and the clients response it is very easy to formulate the WEP key. The next setting is 40 or 128-bit encryption. We chose 128-bit initially because all our radios were Cisco. It soon became apparent that maintaining the higher-level encryption keys was very difficult so we dropped down to the 40-bit level. The WEP key fields must match the clients or communication cannot take place. They must match field for field. NOTE once you "APPLY or OK", the WEP keys are not shown and the transmit radio knobs show up. This indicates which key is currently being used to transmit to the client. As soon as at least one key has been set, you can select the first field to require the clients to communicate via encryption. You do this by selecting "Full Encryption". If you select "No Encryption or Optional" a client with no key set can communicate which nullifies this security layer.

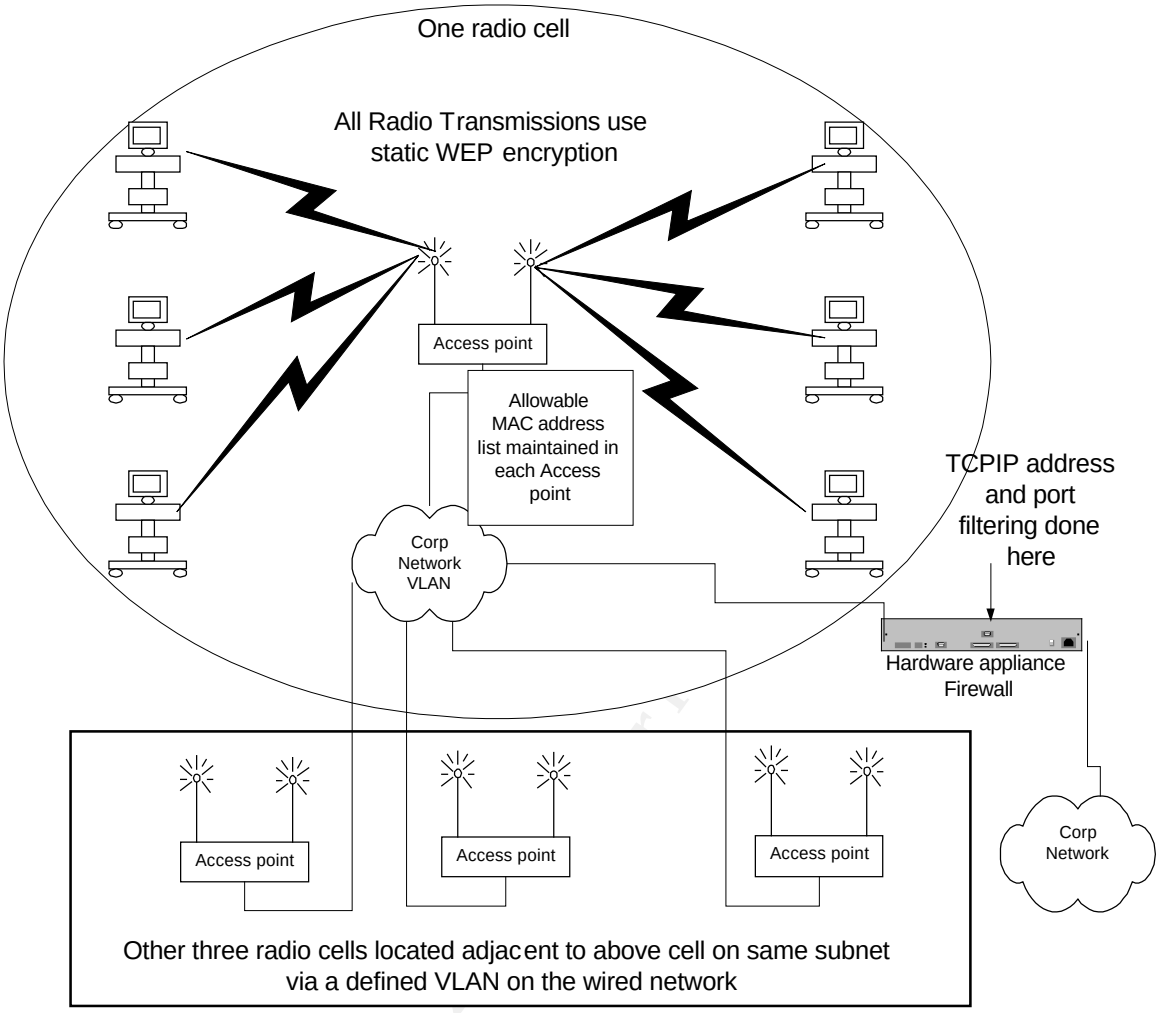
If you have a small network like ours you may want to populate all four of the WEP keys. To explain this lets say your company wants to change active WEP keys on a monthly or even weekly basis. You could log into each AP and move the check next to a different KEY. The caution here is that you would need to make sure all the fields on all devices were typed in exactly the same when they were added to the network. Of course if you have a lot of equipment activity on your network this would be a very heavy administrative burden. IF a device were stolen you would need to change all fields on all devices.

After Snapshot

As you can see from the following diagram, we did not need to do many physical modifications to the network to connect it to our firewall. If you compare the before and after diagram, we only added one piece of hardware. The rest of the security was enabling software already built into the Cisco equipment. If you compare the list of security features we turned on, it is obvious that we are better off than we were.

To recap what we have done.

1) Our radio signal is limited beyond our facility so eavesdropping is limited.
2) Our SSID is not being sent out for all to hear
3) We limited our wireless to a single subnet and connected it to our wired network via a firewall.
4) Using the firewall we limited our wired network exposure using IP Filtering both address and port.
5) We implemented MAC address filtering to limit the connection of rouge devices.
6) We implemented WEP encryption only at the 40 bit level because maintaining the WEP keys at a higher level proved difficult.



After snapshot

Summary

I fully understand that these are all crackable layers of security. If someone were that intent upon breaking into our network, they most likely would find a way even if wireless were buttoned up tight. I personally feel that having this many layers of security makes for reasonable security for minimal risk data. The security measures described in this paper only allow for minimal security. In my opinion, these security measures should be used even on a small home wireless system to at least keep the next-door neighbor from using your DSL or Cable connection. If a small business cannot afford to do at least this level, they should strongly consider just staying wired. I don't feel we are done securing our wireless network however, given resources and funding we are limited to the steps we have taken to secure our WLAN installation. I want to further investigate the use of proprietary protocols. My concern is that we, as a company, may choose a device that does not conform to Cisco proprietary protocols. I will need to start all over again securing our wireless using only the protocols that this new device supports. My job now is to convince the management, which I am part of, that we

need more security. This will require personnel time, a Cisco Authentication Control System, and an upgrade to our current Steel Belted RADIUS to allow for dynamic WEP key and Per Packet keys. We have nearly finished the approval of our wireless security policy, which will require authentication to the wireless network. As soon as that policy is adopted we will be able to obtain the additional resources required to secure our network. The other battle is requiring a step to log into the Authentication device.

References

Architecting your 802,1x. “Architecting Your 802.1x-Based WLAN Deployment Using Odyssey and Steel-Belted Radius” 01/09.2003 URL: http://www.funk.com/radius/SolIns/architecting_wlan_wp.asp

Cisco Aironet. “Cisco Aironet Wireless LAN Security Overview” 01/09/2003 URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/s350w_ov.htm

Cisco AVVID “Cisco AVVID Network Infrastructure Enterprise Wireless LAN Design” Copy write 2002 , 01/10/2003 URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns178/c649/ccmigration_09186a00800d67eb.pdf

Cisco WLAN “Configuring Wired Equivalent Privacy (WEP) – Cisco Systems” 01/09/2003 URL: http://www.cisco.com/en/US/tech/tk722/tk809/technologies_tech_note09186a0080094581.shtml

WaveLink, “Wireless Network Security” 01/15/2003 URL: http://www.wavelink.com/news/securitypaperregistration.asp

WEP Security. “WEP Security Statement Wireless Ethernet Compatibility Alliance” 09/7/2001 , 01/14/2003 URL: http://www.wlana.org/pdf/security_weca.pdf

Internet Security Systems “Wireless LAN Security” , 01/10/2003 URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

Convery,Sean and Miller,Darrin “Wireless LAN Security in Depth” Copy Write 2002 , 02/09/2003 URL: http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

Last Updated: September 25th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event