Global Information Assurance Certification Paper

SANS Security Essentials GSEC Practical Assignment

By Kevin Almeida
GSEC Version 1.3
April 1, 2002

Using 802.11b to extend (mostly) secure resources to remote locations.

Abstract-

Can fast "broadband" Internet connectivity (and all the resources that comes with that connectivity) be granted to those who choose to live in a more remote location where the Central Offices cannot extend these services? There are powerful methods to connect nodes to satellites or optics that might solve the problem, but are there more flexible or configurable alternatives? What will provide the most secure, robust and reliable connection? Can it be implemented with reasonable cost? What about sharing a single Master access point with other remote Hosts- maybe even a small manufacturing business - in the same remote area? Are wireless solutions and our present and evolving 802.11x protocols efficient enough to be considered?

We will first begin by looking at a hypothetical community in need. Then will address these questions by diving into the current ideas and technologies for remotely connecting computers. We will consider the state of wirelessly connecting hosts and what that entails. Then we will look at scaling this idea into a broader geographical situation and see how to make it workable. We will dive into the current state of security and wireless and fix some of these security hurdles with more secure options.

Scenario-

I sit at my computer everyday and enjoy fast ADSL connectivity without thinking much about it as a privilege. I cannot even imagine going back to a 56kbps dial-up connection. My office is connected to my ISP via a DSL modem which bridges my digital requests through mostly analog telephone line traffic. I get decent throughput because my modem is within the 18,000 ft (linear) line length range required for basic ADSL.

A customer of mine who previously had the same privilege, moved his in-home construction business to a huge new beautiful house on the outskirts of town and suddenly realized that he had no DSL or cable service and that the utility providers had no plans to do so "at this particular time". He looked into satellite service for his site- but his southern exposure to the satellite was partially blocked, it was too expensive to justify and it left him with only a proprietary option for a Service Provider. So he's back to living with a modem and waits for

his community to grow large enough for utilities to notice them. How could he live just a few short miles away and have such a “Denial of Service” (joke) attack?

I had read an article written by Glenn Fleishman (O'Reilly Network: An 802.11 ISP on Maine's Rocky Coast [Oct. 12, 2001]) that described how a WISP (Wireless ISP) was born to solve a similar situation- and on a grand scale- this made me aware there was a precedence of success. After discovering how it had been done on a weather beaten Atlantic coastline, I was sure that we could provide wireless connectivity to my customer and the other small group of houses that made up his community. For the purposes of this Paper however, let’s construct a hypothetical (if not increasingly typical) situation. When my customer says “go”, I’ll be ready.

Our remote community model has been growing, due to its beautiful location overlooking a small valley. It’s inhabited by a few upwardly mobile couples with children and retired folks who spend some time online and one woman who works and telecommutes from home. There is an entrepreneurial fellow who doesn’t want live or work in town and is growing his successful light manufacturing business- Widget.net. He *really* wants a fat connection. Dial-up connections are available but they are painfully slow at times and inadequate. The community banded together and petitioned their utility company for ADSL to be extended to their location. They were told by the utility providers that there were plans in the works to expand their high bandwidth service to outlying areas *but*; had no plans to do so immediately. As we can well imagine, this same situation must be a reality to many. Widget.biz has hired us to explore somehow getting them a secure connection and possibly sharing it with a few others in the community.

The 802.11 wireless protocols-

First, in order to understand and plan for our extended Network, let’s look at where of the development of wireless communication has been going starting with the basic 802.11 standards as described by IEEE in 1997.

Due to the fact that the busy 2.4GHz band (2.4000GHz-2.4835GHz -about 80MHz of bandwidth) is part of the unlicensed ISM microwave spectrum, two basic methods of encoding transmissions were developed to minimize interference:

- FHSS (Frequency Hopping Spread Spectrum)- this method works by parceling bursts of the total transmission over short periods of time on selections of 75, 1MHz subchannels; “hopping” from one subchannel to the next. Both the transmitting node and the receiving node must be synchronized to allow conversation.

- DSSS (Direct Sequence Spread Spectrum)- this method sends the transmission over several frequencies at the same instant, controlled by a modulating mechanism called the “spreading code”. The receiving end must know the unique spreading code in order to understand the transmission. Included with the signal, is a bit pattern called a “chip”; a redundancy mechanism which provides a method of rebuilding information in the event the data becomes corrupted. This adds overhead to the transmission, but allows a way to add reliability in spite of the low power signal requirement of the devices.

- These two encoding methods are incompatible with each other.

FHSS was used mostly at first, because it operated more efficiently in low power devices and was less expensive to implement. As 802.11 had only an effective throughput of from 1 to 2Mbps, it was not quite enough to push 100Mbps Fast Ethernet LAN users into it for “sake of convenience”. Wired Ethernet networks work well and can carry a lot of traffic. Most now are running as a minimum 10Mbps, with the vast majority at 10/100Mbps. NICs are efficient and inexpensive and currently Cat5e cable is hard to beat. So DSSS was not as attractive at first to device manufacturers and hence to users.

Manufacturers saw the tremendous potential of the wireless niche and that it needed to be promoted with interoperability and convenience standards. So in 1999 Cisco, 3Com, Intersil, Agere Systems and Nokia got together and formed WECA (the Wireless Ethernet Compatibility Alliance). They developed their standard called Wi-Fi (for Wireless Fidelity) and based it on the 802.11b protocol. Any Vendor who that would like their product to bear the Wi-Fi label must pass a suite of interoperability tests. WECA currently has over 140 member companies who are pushing this Wi-Fi label. Here is their mission statement as taken from the official website:

> ”WECA’s mission is to certify interoperability of Wi-Fi (IEEE 802.11) products and to promote Wi-Fi as the global wireless LAN standard across all market segments.”

It appears to me as though there will be some bullying of established European standards! The popularity of wireless communication has grown considerably in the last couple of years, mostly attributable to this alliance. The problem is that for all the success the standard has had selling a wireless solution, it has done little to promote or mandate security. Manufacturers want an “out-of-the-box” implementation for their customers -not calls to the help desk. Once again, it seems as though designed-in security comes as an afterthought at a time when all should be constructed around it.

Call it what you will, the predominant communicating protocol for the last two years has been IEEE 802.11b; defined in 1999 and adopted by WECA.

Let's discuss some of its limitations:

- It shares the 2.4GHz unlicensed band with a myriad of other devices and Networks. It uses DSSS radio signaling which gives it it's greater throughput than simple 802.11 but with the trade-off of increased interference; and a sure bet for it to get worse as wireless popularity grows and other protocols (Bluetooth) and devices cram their transmissions into this narrow frequency range.
- It currently reports to have the maximum theoretical throughput of 11Mbps - Still far below fast Ethernet- and then when you factor in overhead for security and poor configurations, most testing shows a realistic throughput of between 3-7Mbps.
- Huge security concerns. Out of the box most cards, appliances and their software do not automatically enable the encryption mechanism and most implementers don't have a clue about this. Even though the current encryption WEP standard is built into 802.11, it must be enabled and configured.
- SSIDs (Service Set Identifier) and now ESSIDs (Extended SSID)–These are alphanumeric codes that are attached to all packets that Access Points transmit to provide an authenticating and synchronization mechanism for clients to join that AP's network. An AP will only recognize packets sent with its ID- so if an attacker can sniff it, he's in. Most attackers just try with the default ESSIDs as a first step; only about 30-40% of users change them!
- There are two basic methods of authentication with 802.11; Open and Shared Key. Open authentication is a method where the client has knowledge of the AP's SSID, that it's using WEP and the value of the Secret Key. This is how it is done most of the time. Shared Key authentication works by the client proving that it knows the value of the AP's Key with a CHAP-similar handshake; unfortunately this method is susceptible to plaintext attacks.

Recent 802.11b changes have improved a lot of the limitations:

Transmission collisions-

Wired Ethernet uses CSMA/CD to transmit data on a Network:

- Node1 looks to see if any other node is transmitting on the wire at that moment and if not, takes it's turn. If there is a collision because Node2 happens to also transmit at the same instant, Node1 and Node2 both wait a calculated, random time and then retransmit. This works because Ethernet can listen and transmit simultaneously.

There was not a mechanism similar to Ethernet's that worked for radio transmission until recently. Wireless signals cannot "sense" the air; if a transmission by Node1 was made and if Node2 happened to be on that frequency at that exact instant there would be interference and signal

degradation or loss. So CSMA/CA (Carrier Sense Multiple Access w/ Collision Avoidance) was developed. It uses a four-way handshake to check for an "all-clear" to transmit-

- Node1- sends out an RTS (Request To Send) packet.
- Node2- if ready, it replies back with a CTS (Clear To Send) packet.
- Node1- receives the CTS packet and transmits the Data.
- Node2- after receiving the Data sends back an ACK (Acknowledgement) packet. Node2 will send an ACK for each successful Data packet it receives.

DSSS becomes less expensive-

- In less than two years, impressive improvements in the power and speed of processors have made DSSS the more efficient and reliable choice and as such, the default.

The 802.11a standard, (promoted by WECA as Wi-Fi5) which operates in the currently more spacious 5GHz band, has been seen as an answer to the increasingly crowded 2.4GHz interference problem. It has a maximum theoretical throughput of 54Mbps (and of course, tests out at about half of this- around 28Mbps) and is being targeted at the business community. WECA is beginning a push at this too, even though it could challenge the European methodologies. The hardware is more expensive and the standard does not interoperate with 802.11b (due to the frequency differences).

802.11b and 802.11a are being joined by newer protocols. According to another article by freelance reporter Glenn Fleishman dated 4/05/02 (from O'Reilly's Wireless DevCenter) on a recent meeting of the 802.11 Task Group, the IEEE's 802.11 standards are maturing into a distinct group of more specialized protocols. Significant compromises and consensus between the Letter Task Groups (the "a, b, e, g, h, i" appends) has been solidifying the pieces into standards for reliability(h), scheduling and QoS(e), speed(a), frequency coexistence(g) (for Frequency Hopping and Direct Sequencing in Spread Spectrum methodologies) and a more robust security model(i). The idea would be to develop hardware that that would use these specialized protocols in a way that would have them "overlay" each other and provide the strengths of each for overall superior operability. This will contribute to the next generation of wireless networking.

The Solution-

We have decided to solve our broadband to remote location problem by linking the community to the Internet with a wireless RF connection. We are going to use 802.11b which will give us greater range (although much less throughput) than 802.11a. Theoretically, if we succeeded in establishing a connection with anything over 1.5Mbps we would have greater throughput than the original DSL

wish. We will set up an Access Point transceiver at the end of our land line connection ("BASE") and across the valley on the hillside we will place our AP client that will serve as the Subscriber (Point of Presence>"HOME") and divvy out links to clients. For the fattest, reliable and efficient link, BASE and HOME will need line of sight. They are approximately five + miles apart.

This type of physical wireless topology would be considered BSS architecture- Basic Service Set (or a Point-to-Point) with an extended Star. Our BASE AP will act as our wireless bridge to our Ethernet land link and form an association with the HOME client to transfer data. We could have additional clients in the area as well; but in the interest of security and management we are going to concentrate on developing our single long range client subscriber- HOME. This also means we will be sharing our bandwidth with all clients routed to HOME though a single pipe; the goal then becomes to maximize it. Since our main goal is to connect Widget.biz, this is more than acceptable.

When I first saw wireless working on a laptop I thought "Well yeah, that makes sense; it *should* be able to transfer lots of data; we're close to the access point." Witnessing web pages quickly download and knowing that there was an antenna a couple of rooms over tainted my view on the true potential of RF being able to carry data over any distance. We watch wireless fill the niche of connecting mobile computers in the office or coffee shop and figure that's what it's made for. We are told that 802.11b has a range of a few hundred feet, depending on obstacles. What we are really seeing though, is the clever hardware being built to fit the perceived use. People want to be able slip a PCI card into their laptop (or have it integrated internally) and unobtrusively connect to the Internet. PCMCIA transceivers have an almost vertical transmit/receive signal pattern. They are omni-directional and not designed to "point" at anything. FCC dictates that signal amplification for unlicensed equipment is not allowed in the 2.4GHz microwave band; and mobile devices tend to be small devices- so a few hundred feet seems pretty impressive to be moving up to around 4-7Mbps of data.

Well it turns out that with Yagi or parabolic antennas on both ends of the airspace that you can do some even *more* impressive things: Tests with off the shelf equipment by many have shown data being pushed back and forth between stations set up miles apart. Unlike a centrally placed omni-directional antenna, our Network will be using these unidirectional antennas pointed directly towards each other; which will concentrate their radiation in a targeted direction for maximum gain. In an O'Reilly article by Rob Flickenger 05/03/2001 (from O'Reilly's Wireless DevCenter) they had excellent results connecting 802.11b across a five mile distance using a parabolic dish, and preliminary testing (by padding the transmission with an attenuator) indicated that their goal of a 20-plus mile connection was possible! As indicated in this article and the other about the WISP in Maine- if our distance proved too great for our throughput or reliability needs, the other possibility would be to relay the signal to and from BASE and HOME with a station in-between.

24dB parabolic dish from Hyperlink Tech

We will use parabolic unidirectional antennas as shown. For the initial testing we will mount them on tripods. We will approximate the dishes pointing at each other and then use a strength meter tool (they usually come with the wireless card or are available for Linux http://www.schuermann.org/~dockapps/or Windows) to fine-tune for optimum signal. Both cards at either end must be tuned to the same frequency. Transmission power is measured in milliwatts. In North America, it ranges from 1mW to 100mW and directly affects the range of the signal; the higher the power, the greater the range. This means we need to choose our equipment carefully to maximize data transfers. After we are satisfied that we have achieved best orientation, we should firmly mount the dishes per manufacturer's spec on a stable building, pole or tower at that location.

Antennas and some other radio gear (it seems to depend who you talk to) use decibels to measure gain but most of the devices we have been scoping out measure power in mW. We have this nifty conversion table to compare:

dBm	Watts	dBm	Watts	dBm	Watts
0	1.0 mW	16	40 mW	32	1.6 W
1	1.3 mW	17	50 mW	33	2.0 W
2	1.6 mW	18	63 mW	34	2.5 W
3	2.0 mW	19	79 mW	35	3.2 W
4	2.5 mW	20	100 mW	36	4.0 W
5	3.2 mW	21	126 mW	37	5.0 W
6	4 mW	22	158 mW	38	6.3 W
7	5 mW	23	200 mW	39	8.0 W
8	6 mW	24	250 mW	40	10 W
9	8 mW	25	316 mW	41	13 W
10	10 mW	26	398 mW	42	16 W
11	13 mW	27	500 mW	43	20 W
12	16 mW	28	630 mW	44	25 W
13	20 mW	29	800 mW	45	32 W
14	25 mW	30	1.0 W	46	40 W
15	32 mW	31	1.3 W	47	50 W

Remember that the higher the frequency, the greater the signal loss. We can use the formula for calculating the path loss (that is, the amount of signal lost in transit along a clear line of sight) from Rob Flickenger's article and play with the variables:

The formula for signal loss is as follows:

L = 20 log(d) + 20 log(f) + 36.6
(Where L=loss in db, d=distance in miles, f=freq in MHz)

For **5** miles at **2.412** GHz (channel 1):
L = 20 log(5) + 20 log(2412) + 36.6
L = (20 * 0.69) + (20 * 3.38) + 36.6
L = 13.8 + 67.6 + 36.6
L = **118.0 dB**

For **5** miles at **2.462** GHz (channel 11):
L = **128.4 dB**

So we will try to use one of the lower channels to keep our signal strength maxed. In addition, range and throughput are inversely proportional. So we will choose equipment that auto senses signal strength and backs off the transmission rate accordingly. There are also constant reminders in wireless design to be aware of obstacles; especially trees, which are huge mountains of impenetrable water to

microwaves. Weather as well can adversely affect the reliability of our Network. We will need to be aware of these factors when scoping out our AP mounting points.

Let's move on to our radio equipment. Access Point hardware comes in many configurations. We will need to be sure it addresses our needs for power, security and flexibility of configuration. It must have external antenna connection ports. Some come with built in routers or firewalls, both of which we will need to manage traffic and security. Most inexpensive AP's are lacking in some or all of our requirements. They are inflexible and difficult to configure in ways that *could* make them more secure- hey, they are only thinking of the customer!

There is a terrific article by Michael S. DeGraw-Bertsch at www.samag.com: "Configuring a FreeBSD Access Point for your Wireless Network"
http://www.samag.com/documents/s=7121/sam0205a/sam0205a.htm

This article describes how you can set up your own Access Point using an older unused computer or laptop. As simple as it is to buy a ready made AP "appliance", there are some real advantages to consider building your own. The FreeBSD box can also be configured as a router, for directing traffic and setting up Access Control Lists and extensive filter rules- the IP and filtering abilities of a Unix-type box are much more powerful than most appliance-type devices. You would also have SSH for secure remote administration and the ability to set up a VPN. If we have some time for this, it could be worth it!

Let's look into some off-the-shelf products.

14dB Randome Yagi

This is a Yagi-design antenna from Hyperlink Technologies. This type is being used extensively for the Seattle Wireless's giant cooperative Metropolitan Area Networking project.

Here's a ready made point-to-point kit from Agere- From PC Magazine's Review- "Agere claims that the Radio Backbone Kit can provide an 11-Mbps wireless link between two LANs at distances up to 3.4 miles and a 1-Mbps link at distances up to 5.9 miles." This would probably work as well!

http://www.pcmag.com/article/0,2997,s=1711&a=24027,00.asp

A bi-directional in-line amplifier can be purchased to help improve our antenna's gain. This is an example of another product from Hyperlink - "Consisting of a low-noise receive amplifier and a

transmit amplifier, the HyperAmp™ series offers a significant improvement in operating range and performance. HyperAmp™ Amplifiers are available with or without AGC (Automatic Gain Control) and are compatible with both direct-sequence and frequency hopping spread spectrum equipment including all IEEE 802.11b equipment."

Here's the Cisco AIR-AP352E2R-A-K9 PCMCIA card- It's fully IEEE 802.11b compliant, and transmits at 100 milliwatts (mW). It has an external antenna connection and it comes with superior strength meter software for dialing in the AP. This would be an excellent card to use in our FreeBSD box to connect directly to the dish, or for a Subscriber client to associate a connection with HOME on the community side. The Cisco Aironet cards are more expensive than others, but considering our gain requirements coupled with Cisco's stronger inherent security and UNIX flavor compatibility, this would be one our best choices.

This would be a good choice for our AP's. The Lucent AP-2000 has 64-bit WEP and 128-bit RC4 encryption, with MAC control tables and built-in Radius Authentication. A web-based, full SNMP management console, with embedded Telnet/CLI support and automatic WEP key distribution. Dual slot architecture too; this means we can choose our cards and design in continuity for optimal configuration flexibility and future upgrading. This picture is from the CDW.com site.

Wireless Security: WEP and WEP2-

The Wired Equivalent Protocol used as a privacy tool in 802.11 has now been reduced to be nothing more than a minor bump in an attacker's path to network compromise. WEP was conceived to provide simple basic privacy for invasive nearby antennas; not as a fully functioning network security protocol. The idea was to promote wireless networks as a having an equivalent level of protection as a physically wired network by building WEP into 802.11. However, if you combine the development of WEP encryption cracking software like AirSnort and WEPCrack (Linux) or dweputils (OpenBSD) and the advent of the proliferation of wireless equipment coupled with their ease of installation- you suddenly have fields of ripe networks for attackers to pick. Attackers can locate in proximity to a network, passively collect packets and build enough of a sample to decrypt the key.

There are two levels of encryption in WEP:

- 64-bit encryption- a 24-bit Initialization Vector (IV) appended to a 40-bit secret key.

- 128-bit encryption- the *same* (length) 24-bit IV appended to a 104-bit secret key.

The 24-bit IV is set to one of a few known values. This gives an attacker a foot in the door and makes the computation for the remaining secret key, (and then the full WEP key values) that much easier. This is why the 128-bit encryption is not that much more effective protection; it's just a question of collecting enough additional packets. After collecting a few hundred MB of data, AirSnort can deduce the WEP key using the now widely publicized attack theorized by Fluhrer, Mantin and Shamir which allows the attacker to openly authenticate to the AP.

Another example of the weakness of the small IV can be explored. 2^24 yields about 16 million possible IV keys. An active 10+ Mbps network can use up this many combinations of keys in a matter of hours at which point you can begin to see collisions, which occur when two packets have the same value of IV and secret key. An attacker who collects these occurrences then can deduce the plaintext by XORing the identical keystreams and seeing what is left.

WEP2 encryption is more difficult to crack, but has been implemented as a temporary fix until the 802.11i Working Group comes up with a more comprehensive security mechanism. It still utilizes the same encryption mechanism as WEP, but with the IV space increased in size from 24 to 128 bits and inherent support for Kerberos V. This lessens the possibility of the XORing of identical keystreams. Some vendors have provided for firmware updates to move a device from WEP to WEP2, but because it is just an expanded version of WEP, it's just a question of the attacker being more patient.

Basic wireless security mandates-

As a basic Best Practices, if you want to start to secure an 802.11b network you have to begin with these features. This goes for our network as well.

- To start with, WEP will be enabled. It is almost ineffective currently against any determined attack, but we are building a Network with our "Defense in Depth" mindset. We have to eliminate the casual script kiddie right from the start. If you were going to rely completely on WEP (we wont) you would, at a minimum need to use 128-bit encryption and a scheduled key change weekly or even more often. There AP's as well that automate the process with a feature called "dynamic key generation" such as Agere's ORiNOCO AS-2000. We *may* want to consider using the 64-bit encryption if we need to cut some of our transmission overhead, but this would only be an option if we had additional protection in place like a VPN.

- If we purchase a commercial product, we will modify the default SSID and password. Most default SSIDs are never changed and attackers know them (they are posted on many sites) and the manufacturer's default password that

goes with them. We will also disable the SSID "beaconing"; this shuts off our SSID broadcasts and effectively disallows a rogue client from pinging our AP for a response.

- We will set up MAC association so that the AP will only accept known NICs. There's only going to be a few NICs involved and so this is a prudent, manageable configuration. MAC address spoofing is still possible by sniffing packets, but this again takes a more advanced attacker.

- If our Access Point (HOME) does our routing for us, we want to make sure that it is not acting as a DHCP server. We can use a few static IP addresses (from a subnet NOT on the default network one) to our wirelessly connected devices. These are also easy to sniff like the MACs, but an attacker would have to guess our subnet unless they sniffed traffic and so, are another small deterrent. On our private LAN for Widget.biz, we will be using a firewall device with NAT enabled to further deepen the reach.

- We will put in personal firewalls too and use the OS on the workstations to encrypt important (all?) files.

Even *better* security mandates-

In continuing to keep our Defense-in Depth mindset, we will put up as many obstacles as we can to thwart a breech. So we will add to the above Best Practices with some recent suggested defenses.

Authentication-

In order to provide superior authentication, we will use a RADIUS (Remote Authentication Dial-In User Service) server or integrated service. This is not part of the 802.11b standard, but it is included on most recent AP hardware and is a far superior authentication mechanism. RADIUS will authenticate VPN and other types of tunneling protocols. If we run our FreeBSD box as an AP we could include RADIUS as well.

VPN and SSH-

Currently, our best bet for the prevention of wireless eavesdropping is to deploy a VPN (Virtual Private Network) between BASE and HOME. It can be enforced between our two firewalls at both ends, constructing a fully encrypted IPSec tunnel across the air distance. We only have a few other clients on the HOME end, so we could include them in their own DMZ and put the first firewall in place to filter appropriate user traffic. We would want to protect Widgets.net's info all the way into the companies LAN, so the VPN needs run all the way to that gateway. Some more powerful (i.e. expensive) AP's have VPN mechanisms built into them. These can still be tricky to use! Windows 2000 and XP have a VPN

client built in too, but this still requires a server and some time and it has to leave a port in the firewall open for access. Check this link for great VPN comparisons.

http://www.pcmag.com/article/0,2997,s%253D1553%2526a%253D12376,00.asp

We could also use SSH or SSL, which would more than likely be enough encryption protection for us, since the two AP's are not associating with more than a few clients. It would be less expensive too and already be part of our FreeBSD Operating System.

Another great article by Rob Flickenger "Using SSH Tunneling" 02/23/2001:

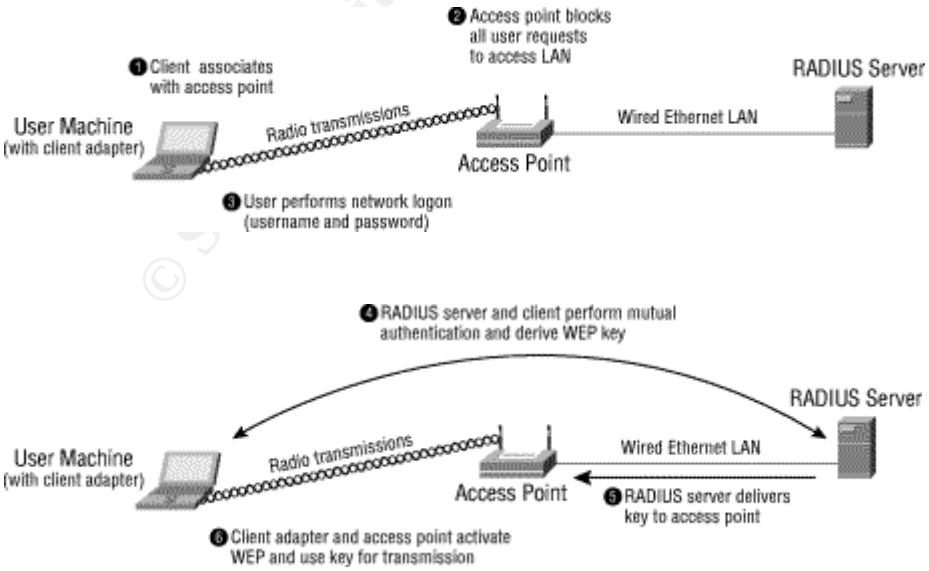
http://www.onlamp.com/pub/a/wireless/2001/02/23/wep.html

IEEE 802.1x-

IEEE is proposing 802.1x; a new standard that will be very effective for many active Wireless LANs. It combines an improved encryption scheme with easier centralized management. The EAP (Extensible Authentication Protocol) would be used by a client to authenticate a RADIUS server (with a one-time permission). The client would NOT be allowed entry into the network. The RADIUS server then assigns the client a dynamic WEP Key, which is utilized only for that session. These keys would change often enough to prevent enough sniffed traffic from being collected for decryption. Nothing is transmitted over the air in clear text.

Here is a diagram from Cisco Systems, showing their implementation of this-

Figure 1: With the Cisco security solution, authentication is based on username and password, and each user gets a unique, session-based encryption key.



Conclusion-

We have looked at a current, mostly secure method of connecting a remote LAN with a land-line resource using an RF link and the 802.11b protocol.

We have also come across some food for thought. How will future vulnerabilities affect our design? What can we do to prepare for changes in hardware and software that might make our network obsolete or ineffective? What about the crowding of the 2.4GHz band; will there be a crackdown on traffic here and will it affect us out in the wilderness? What about *SUNSPOTS?!!*

References-

The O'Reilly Network Wireless DevCenter- a constant good online source. 04/01/2002
http://www.oreillynet.com/wireless/

Fleishman, Glenn. "An 802.11 ISP on Maine's Rocky Coast "
10/12/2001
http://www.oreillynet.com/pub/a/wireless/2001/10/12/maine.html

Ellison, Craig. "Exploiting and Protecting 802.11b Wireless Networks"
author for PC Magazine, posted on Extreme Tech site 09/04/2001
http://www.extremetech.com/article/0,3396,s=1034&a=13880,00.asp

Bannan, Karen J. "Safe Passage"
author for PC Magazine 09/25/2001
http://www.pcmag.com/article/0,2997,s%253D1553%2526a%253D12376,00.asp

Schenk, Rob; Garcia, Andrew; Iwanchuk, Russ
"Wireless LAN Deployment and Security Basics" 08/29/2001
posted on Extreme Tech site
http://www.extremetech.com/article/0,3396,s=1034&a=13521,00.asp

Freed, Les. "Build your own Point-to-Point Wireless Network"
equipment review for PC Magazine 04/09/2002
http://www.pcmag.com/article/0,2997,s=1711&a=24027,00.asp

DeGraw-Bertsch, Michael S.
"Configuring a FreeBSD Access Point for your Wireless Network"
author for Sys Admin Magazine 04/2002
http://www.samag.com/documents/s=7121/sam0205a/sam0205a.htm

Fleishman, Glenn. “802.11 Task Group Update”
04/05/2002
http://www.oreillynet.com/pub/a/wireless/2002/04/05/80211taskgroups.html

Flickenger, Rob. “A Wireless Long Shot”
05/03/2001
http://www.oreillynet.com/pub/a/wireless/2001/05/03/longshot.html

Flickenger, Rob. “Using SSH Tunneling”
02/23/2001
http://www.onlamp.com/pub/a/wireless/2001/02/23/wep.html

HyperLink Technologies, Inc.
Product info for antennas and related wireless 04/01/2002
http://www.hyperlinktech.com/web/antennas_2400.html

Dubrawsky, Ido
“Wireless (In) Security” 04/2002
Sys Admin Magazine, May 2002 issue, Volume 11, Number 5
pages16-22.

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event