Global Information Assurance Certification Paper

GSEC Practical Version 1.4 Option 1

Berant Lemmenes

Creating a Secure Wireless Community Gateway

Abstract

With the price of wireless equipment dropping many consumers and businesses are looking to implement a wireless infrastructure to complement their existing wired networks. There is also a growing grass-routes movement to capitalize on the low cost of the required equipment to create wireless hot spots, providing free high-speed internet access. The question is if you've got the home network, the broadband internet connection, what would you need to get to provide a wireless community gateway for your neighborhood and how would you set it up so as not to totally compromise the security of your existing home network?

Introduction

There are many wireless standards out there, there's Bluetooth, HomeRF, HiperLAN and then there's 802.11b and 802.11a, and 802.11g. The design uses of these protocols varies from short range inter device communication to long haul last mile Internet solutions. I'm going to focus on the 802.11 technology, of which there are currently two soon to be, three types.

First let's take a look at 802.11b, it's been established for a while, and is quite popular. It operates in the 2.4GHz range, and has a total bandwidth of 11Mbps. With 802.11b you can get a range of about 100-150 feet or so at 1Mbps, 150-250 feet at 5.5Mbps and 250-300 feet at 2Mbps. The drawbacks of 802.11b are that the 2.4GHz spectrum is quite populated with other devices, 2.4GHz cordless phones, Bluetooth devices, as well as the myriad of devices from companies like X-10. Since we're looking to provide high broadband internet access to as wide an area as possible we're going to choose 802.11b for the range and the popularity of the hardware.

Next up is 802.11a, it operates in the 5GHz frequency band, and sports a max throughput of 54Mbps. 54Mbps is just the maximum throughput devices are also required to support 6, 12, and 24Mbps as well. The drawback however is that the high bandwidth provided by the 5MHz range means that the effective range is cut down. 802.11a can deliver 54Mbps to a distance of around 60 feet, further out than that the bandwidth is reduced. This means that it takes more access points to cover the same area as an 802.11b network. And since it uses the 5Ghz range the devices are not compatible with 802.11b devices. Due to it's small effective range, and the fact that it takes different equipment, 802.11a is not very well suited for creating a wireless community gateway.

The new comer is 802.11g which is going to overcome all the problems of 802.11a, it will operate in the 2.4GHz range, so it will be backwards compatible with 802.11b devices, as well as have a longer range. This longer range also means that it will have a slightly smaller max throughput; somewhere in the 20-30Mbps area. It is however not out yet so can't be evaluated.

Network Architecture

What you would need to get depends on what you want to do, or how much you would like to spend. First off, an over view of the types of wireless network architectures. There are two basic kinds of wireless network architectures, Ad-Hock and Managed. Ad-hock networks are analogous to peer-to-peer networks where there are several clients sharing resources without a central server. Conversely managed networks look much more similar to a conventional client-server network, the access point would be the "server". This paper is going to focus on Managed networks being that they are both more common and applicable to the goal of creating a wireless community gateway.

Managed networks usually mean there is a hardware device that is the access point; it has no other purpose. You plug it into your existing wired network and it acts as a bridge between the wireless network and the wired network. Just about any company that makes a wireless network card makes a wireless access point; Linksys, D-Link, Lucent, and Cisco, to just name a few.

There is however another option; if you have an old laptop, or an old PC you can purchase a wireless card for them and turn them in to an access point. There are several products that "out of the box" create a wireless access point out of a PC with a wireless network card. Two of the companies products - Boingo Wireless, and Joltage create a access point that can function as a client node as well; the third offering Sputnik, creates a dedicated access point out of the PC it's run on.

All three company's have the goal of creating a national wireless network where a single account with them allows you to get internet from access points no matter what their location is or who they are run by. The difference between Boingo, Joltage, and Sputnik is that the former two both charge for access to their network (there is one catch to this, covered in a bit). Both Joltage and Boingo have pricing plans ranging from a fee each time you connect to the network or a flat rate for unlimited access (per month). Sputniks business model is to offer it's Community Gateway software free of charge in order to increase exposure for it's enterprise gateway products. That being the case Boingo and Joltage seem to have the much larger networks, they have access points in many hotels, airports and other businesses that people frequent and might want internet access during their stay.

There are many security problems related to wireless networks, the most immediate being the lack of control over the transmission medium. Unlike a wired network where you can have control over what drops are connected to the network, or even where the cable drops are, you have very little control over where a wireless network reaches. Proper planning of where the access points will be located can help prevent signal bleed out of the building, however the task is still difficult. However, in the scenario of creating a wireless access point for public community usage the goal is to have it reach as large of an area as possible.

To that end, consideration should be given to purchasing an external antenna to enhance the range of the chosen access point. An external omni-directional antenna is relatively cheap (about the price of a wireless PCMCIA card) depending on the dbi rating. The dbi measurement refers to the gain of the antenna; this can be thought of as the strength. A good site to find information as well as purchase external antennas and other wireless equipment is BuffaloTech (http://www.buffalotech.com/). It should be noted that not all wireless network cards have an external antenna attached to them with out serious tinkering. For the most part that just applies to PCMCIA cards, most desktop wireless cards (PCI or ISA) have small external antennas already, and can have other ones plugged in. The same restriction can applied to access points, not all access points can have an external antenna plugged in. Some you can with a little tweaking. For example Lucent Orinoco Residential Gateway products (RG-1000, RG-1100, RG-2000) don't have an external plug for an antenna however if you open up the plastic case of the unit one can be plugged into the card inside with a little trouble. What option is best for you really depends on how much you want to get your hands dirty taking apart your brand new access point.

Locating Networks

In any kind of wireless network the SSID (Service Set Identification) is used to create different wireless networks. By having unique SSID's you can have several wireless networks in the same area. This assumes that there are enough channels free. A channel is a chunk of the radio frequency spectrum used by the 802.11b network standard.

Since the SSID is the unique identifier for each and every network, you need to know this to get on the network. However SSID's are not hard to come by, many access points by default broadcast the SSID so that wireless clients that are looking for networks can find them. The ease with which you can find wireless networks has led to hobbies such as Wardriving where equipped with a laptop, and a wireless card you can drive around looking for wireless networks using a program called Net Stumbler (http://www.netstumbler.com). Using an external omni directional antenna you can greatly increase the range of the laptop. GPS receivers can also be used to provide exact locations of the access points discovered.

The Authentication Process

To get on or 'Associate' with the wireless network the host or machine must authenticate it's self. There are two methods for doing so; Open System and Shared key. Both methods are one-way authentications; they authenticate the machine to the access point only. This leaves to potential problems; one it doesn't authenticate the user with the access point so there is no event tracking on a per user basis, the 2nd problem being that it doesn't authenticate the access point to the client, where by leaving the possibility for a malicious user to plant a rogue access point.

The Open System authentication method is the default authentication method defined by 802.11b and is still some times the way access points are configured upon shipping. When a host begins authentication it does so by sending a frame identifying it's self, and requests authentication. The access point then responds allowing the host to associate with the access point. This is all done with out encryption.

Shared Key authentication is part of WEP (Wired Equivalency Privacy) and therefore WEP must be enabled. This process is very similar, and starts with the host wanting authentication requesting it of the access point. However with WEP the access point responds using the shared key to encrypt response, if the host then encrypts it's response with it's shared key and if they match the access point grants approval.

WEP Problems:

WEP (Wired Equivalent Privacy) is part of the 802.11 spec, and as the name suggests is designed to provide security equivalent to that of a wired network. WEP is an encryption/authentication protocol, offering either 64-bit or 128-bit encryption using the RC4 steam cipher. This sounds great, however the protocol design it's self is flawed. WEP only encrypts the actual data payload it doesn't encrypt the physical layer headers, this is not the real problem. The big flaw is that the initialization vector is sent in the clear. The IV (Initialization Vector) is part of the full key and is used to decrypt the packet by the receiver. The IV is 24-bits in length so there are 2^{24} possible variations of IV, this creates a problem when it is combined with the rest of the key (either 40-bit or 104-bit). Because as long as the 2nd portion of the key doesn't change (which in the current WEP implementation it does not) the overall encrypted stream will repeat when the IV exhausts the 2^{24} of possible variations. Since it is common between the 64 and 128-bit versions of WEP both are just as vulnerable to someone exploiting the IV irregardless of the full key size.

Although this is a huge security problem with the WEP protocol it doesn't really affect us since our goal is to create an open-access access point. The problems with WEP were briefly discussed so there wouldn't be a false sense of security in an access point using WEP.

Boingo Wireless:

Boingo's network is designed around the idea that airports, hotels, coffee shops or any other business that has people moving through, can provide high-speed Internet access to their patrons. They charge for usage of their access points, anywhere from per connect fee, to monthly cost for unlimited access. Their network is spreading rapidly; according to their website (http://www.boingo.com) Phase 1 of their network roll-out is complete totaling 500 wireless 'hot-spots'. They seem to have quite a large network, with several hot-spots in my state including one in a hotel in my own technologically inept Grand Rapids, Michigan.

Boingo's network uses SSL to encrypt the authentication from the client to their RADIUS authentication servers. After the client is associated with the access point all traffic is unencrypted. They recommend using your own VPN solution to encrypt the wireless traffic, as well as offering their own VPN server you can connect to. This would then provide encryption for all of the data traveling over your wireless link to Boingo.

When you create a Boingo access point - or hot-spot as they call them, you become part of the Boingo network, and your access point is advertised to all of the Boingo clients in your immediate area. If you run a Boingo hot-spot they pay you for every client that connects to your access point as well as every client that signs up for service at your access point (they provide advertising material for your location).

The one catch mentioned earlier is that Boingo does allow you to use their software to create an access point that does not charge for access (http://www.boingo.com/hso/free.html). This access point is still part of Boingo's network and will show up in hot-spot listings however Boingo will not charge for access to access points created in this way.

To create an access point on Boingo's network you either need a Windows 9x/2000 computer with a supported wireless card, OR you can buy their Hot-spot in a box product. This is a separate hardware device that is configured to be a part of Boingo's network. The 'Hot-spot in a box' product is really a Colubris CN3000 pre-configured for Boingo’s network.

Joltage Networks:

Joltage is very similar to Boingo in it's network design as well as pricing scales. They also are targeting airports, hotels and shops. Joltage also uses a PC or laptop with a wireless card to run their access point software, which they call the Joltage Provider Software (PSW). The PSW handles the authentication as well as the security of the host computer operating as the access point. The PSW handles the authentication via a proprietary system that uses SSL for the encryption. To protect the computer acting as the access point the PSW has a quasi-stateful firewall built in to prevent Joltage subscribers from accessing the provider's access point computer. The PSW package also allows them to do MAC based restrictions as well as email address based restrictions.

Sputnik Community Gateway:

Sputnik takes a different approach than the other two companies', their Community Gateway product is similar in that it takes a computer with a supported wireless card and turns it into a managed access point. However, their software and their network are free. They offer the Community Gateway to help promote their technology to help sell their other commercial products geared for the enterprise looking to setup a secure wireless network.

Sputnik also differs from Boingo and Joltage in that their software is for the most part Open Source based. Their system doesn't have any operating system requirements because they provide the operating system! The Sputnik community gateway is downloadable as an ISO (a CD-ROM image) that can be burned to a CD-R. You then just insert the CD in a PC with a compatible wireless card (currently only PRISM II based cards) and turn it on. The Community Gateway CD-ROM runs Linux, based off from the 2.4.18 kernel.

If you take a look at Sputnik's feature page (http://www.sputnik.com) you can see that every feature listed with a '*' next to it is a free Open Source component. That's quite an impressive list of features provide by the Open Source community. These include features such as 802.11p and 802.11q, which provides Quality of Service (QoS) and prioritization of traffic based on the type of traffic.

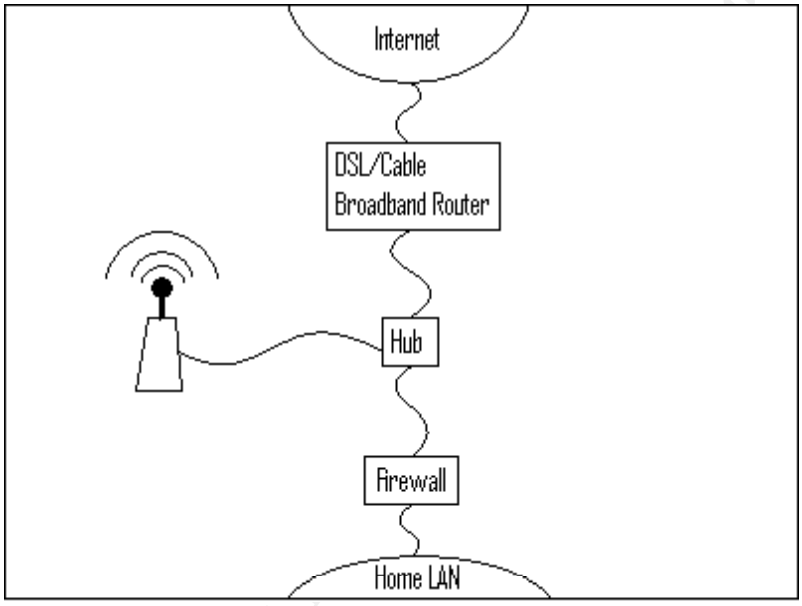
Sputnik also includes features such as automatic update of the access point via the internet when updates come out. Sputnik access points will also adjust what channel they are using to avoid interference from other access points as well as other 2.4GHz interference like that produced by cordless phones.

If you choose to go with a hardware access point from any of the many manufactures you need to keep a couple things in mind. Since your access point isn't going to be part of a large centrally managed network Like Boingo, Joltage, or Sputnik you need to make your access point as accessible as

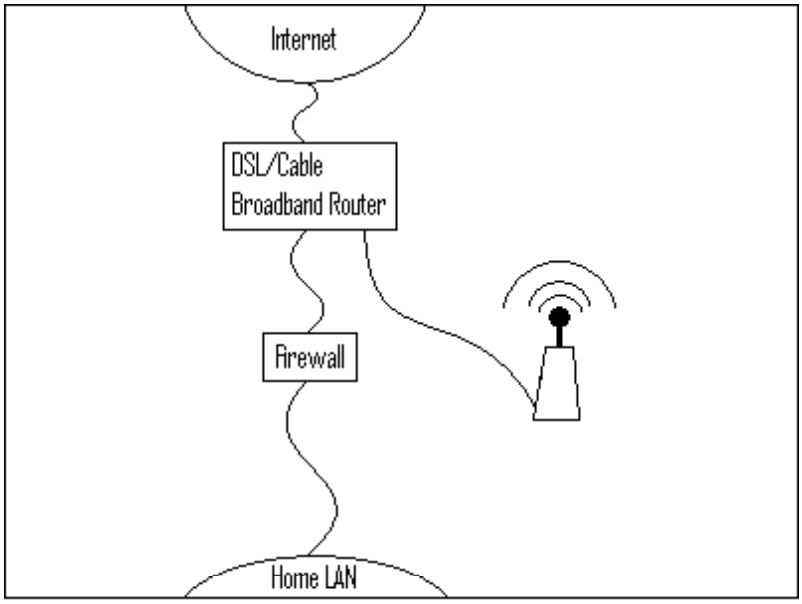
possible. When you configure your access point, make sure that it is still broadcasting the SSID as well as keeping WEP disabled.

Access Point Placement:

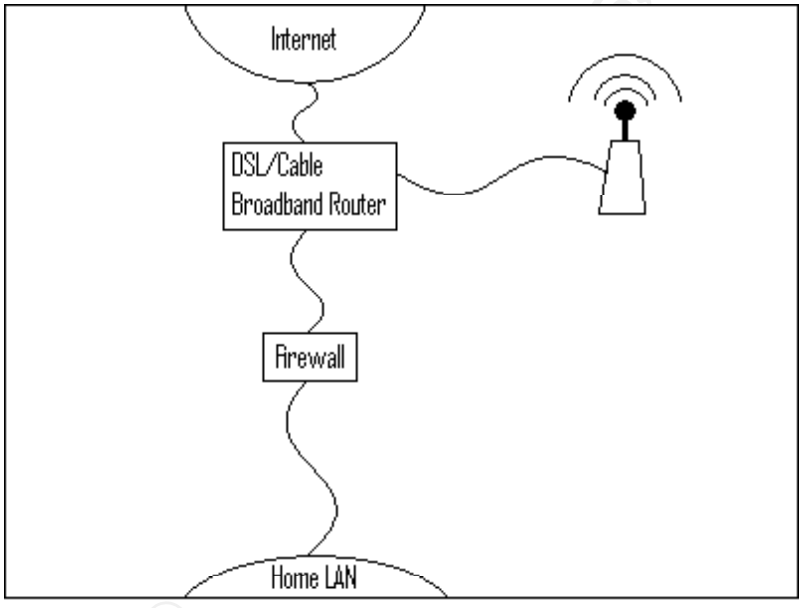
No matter what kind of access point you use, whether you create an access point out of a PC or purchase one, you need to take into consideration of how you incorporate it into your existing network. Since the goal of a community access point is to provide an open gateway to get on the internet, using restrictive access controls to provide a secure network would be rather defeating to that goal. Since you have no idea who is going to be using your access point, you really can't trust them enough to put the access point on the "inside" of your network. Your wireless network is going to be free reign, so all you can really hope to do is isolate the rest of your home network from the wireless clients. It is assumed that you already have some sort of firewall, be it a separate PC running Linux or a BSD variant or something built in to your cable modem/DSL router. Here are some sample designs showing ways to locate the access point in your network.



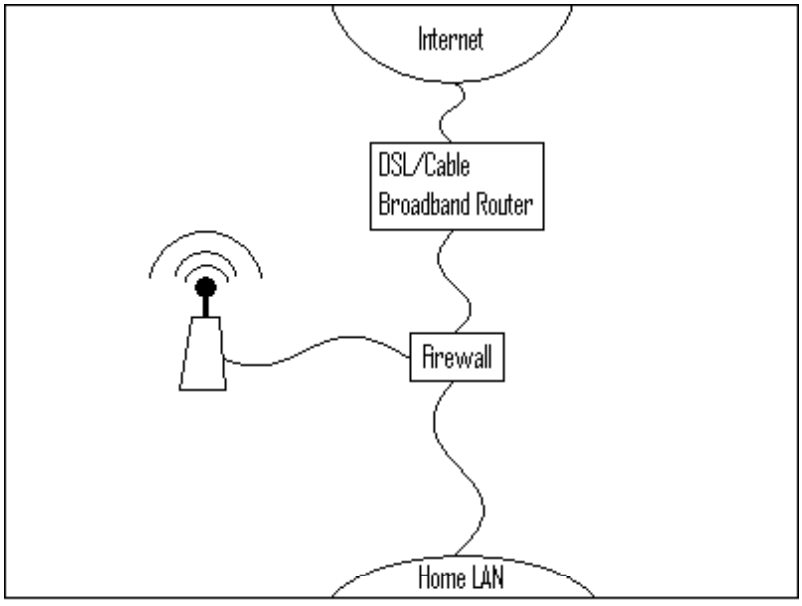
The above diagram shows a network that has the access point placed in between the Cable/DSL modem/router and the internal firewall. This isolates the wireless network between the router, which is doing NAT, and the internal firewall, which is also doing NAT. The one problem with the setup is that a hub is used to connect the three devices. That would mean that hosts on the wireless network would be able to 'sniff' all the traffic coming into and out of the wired network due to the hubs single collision domain. A setup that would eliminate that problem for the most part would be to take this same diagram and place a switch where the hub is.



Many DSL Routers or appliance firewalls have small built in switches this provides another option. As in the example above with a hub, the wireless access point is installed between the internal firewall and the router. The distinction between the router and the switch being the same device blurs that line some however.



If you have more than one external IP address with your cable modem or DSL connection you can setup the access point to do Network Address Translation for the wireless clients. This way you don't need two firewalls, all of the wireless clients are on a private network NAT'ed to the 2nd public IP address (used by your access point). This assumes your DSL/Cable router has a port for an "outside" host, or you can put a hub on the outside.



This final diagram shows the access point being setup off the third interface of the firewall. This option may not be the simplest to implement since it requires setting up that 3rd interface as well as modifying the firewall rules to properly deal with traffic to and from that interface. However setting things up this way also allows you to do traffic shaping, management. It should be noted that these are all features that Sputnik can provide since it uses a very similar method to run the access point.

Secure access:

By placing a firewall between your home network and the wireless network you put a hamper on accessing your internal network, and this may seem like a reason not to do so, there are however many ways to create VPN/secure tunnel that allow access into your home network in a secure fashion. If you are using a UNIX based operating system, such as Linux or OpenBSD/NetBSD as your firewall there are several options. Such as IPChains or its replacement IPTables for Linux. For OpenBSD there is pf, and for NetBSD there is ipf.

FreeS/WAN:

FreeS/WAN (http://www.freeswan.org) is an Open Source implementation of the IPSEC security standard, written for the Linux operating system. The IPSEC protocols were created by the ITF (Internet Engineering Task Force) to be part of the IP V6 standard -IP V6 is the next version IP. IPSEC is designed to provide secure authentication and encryption services for network traffic. FreeS/WAN is a complicated program and is outside of the scope of this document to discuss the configuration of, however it is suffice to say that if you are looking for a full and robust Authentication VPN solution FreeS/WAN has you covered.

SLAN:

If you are looking for a more simple VPN solution, another option is SLAN, which is a blowfish based VPN designed specifically to fill the gap in need between SSH and a full IPSEC VPN like FreeS/WAN.
SLAN was created because of the desire of an ISP to create a city-wide 802.11 network to it's customers and still be able to provide a secure and private connection to it's customers.

SLAN is designed to provide a secure VPN from the wireless client to the "provider network" in this case that would be your network. It supports Linux and Windows 9x clients. SLAN is not for all however, it is currently in early development and undergoing rapid changes. Currently the Linux and Windows versions are not keeping up with each other. Right now Windows is at version 0.02 while Linux is at version 0.04.

SSH:

SSH is a tool commonly used to replace telnet as secure method of remote terminal access. It uses either RSA or DES keys for authentication and 3DES, Blowfish, CAST128, Arcfour and AES the transport encryption. SSH however, has many other uses, one of which is scp or secure copy, which uses SSH to provide an encrypted method to transfer files. Another interesting feature is that if you want to encrypt the traffic for some application that doesn't have built in encryption. One such would be email, both SMTP (sending) and POP3 (receiving) can be encrypted via a SSH tunnel.

There are some restrictions, namely you have to have control of the server in question, you will not be able to check your hotmail account this way. You have to have SSH installed on your mail server as well as having an account (or even better an account plus your public DSA or RSA key on the server).

A general description of the setup would be this. SSH attaches to a local port on your computer and any traffic to that local port gets redirected to the remote server at a port you specify where SSH running on that computer decrypts it and passes it on the specified port.

If you are using a command line SSH client here would be a sample command:

testpc# ssh -L 110:**mailhost**:110 -l **username** -N **mailhost**

This would redirect the local port 110 to port 110 on the host **mailhost** using the username **username.** Not all applications and services can be tunneled

this way. For example active FTP does not transmit data over port 21, after your client connects to the server on port 21 the server makes a connection back to your host on some ephemeral port (a port above 1024).

If SSH sounds like what you need or would just like to find out more about it, there is a open source SSH server and client that is fully compatible with the commercial version. It's available at http://www.openssh.org/

The question is now that you've got an access point setup ready for people to start using it... but no one knows it's there. How do people find your access point? Well if you're in a area with a large population people may eventually find it by Wardriving, but that's no fun. One thing you can do is to post it to online databases of access points, one such database is at the NetStumbler website (http://www.netstumbler.com).

Another method, is something new called Warchalking. Warchalking is a method of chalk graffiti describing nearby access points. Or as the home page, (http://www.blackbeltjones.com/warchalking/), describes it "Collaboratively creating a hobo-language for free wireless networking." You create symbols describing the access point, things like if it's an open or closed access point, what the SSID is, and if it's a WEP enabled access point what the WEP key or contact person would be. The homepage for the Warchalking effort has a downloadable PDF file that you can print out on a small card to have in your wallet that describes the symbols used.

Conclusion

There is no right or wrong way to create your access point, it depends on what kind of clients you want to use your network. If you use Boingo or Joltage you limit your clients to Windows based computers. If you choose to use either a Joltage based, or a hardware access point from any one of the vendors that make them, anyone with a 802.11b network card can use your access point. It's all a mater of preference, what fits your goals the best.

The biggest thing to keep in mind is how you incorporate the access point into your network. If you can minimize the exposure to your home network by the wireless traffic is hostile then you don't have to worry about all of the problems associated with wireless security. You're really not trying to make a secure wireless network, you're trying to make a insecure wireless network part of an existing home network.

Bibliography:

Boingo Wireless. Inc. "Free Communities." URL: http://www.boingo.com/hso/free.html (06 Jun 27 2002)

Geier, Jim. "The BIG Question: 802.11a or 802.11b?" 24 January 2002. URL: http://www.80211-planet.com/columns/article/0,4000,1781_961181,00.html (14 June 2002).

Jones, Matt. "Warchalking." URL: http://www.blackbeltjones.com/warchalking (28 June 2002)

Proxim Inc. "802.11a: A Very-High-Speed, Highly Scalable Wireless LAN Standard." 10 August 2001. URL: http://www.proxim.com/learn/library/whitepapers/wp2001-09-highspeed.html (15 June 2002).

Flickenger, Rob. "Using SSH Tunneling." 23 Feb. 2001. URL: http://www.oreillynet.com/pub/a/wireless/2001/02/23/wep.html (25 June 2002)

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP algorithm." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (20 June 2002)

Flickenger, Rob. "A Wireless Long Shot." 05 May 2001. URL: http://www.oreillynet.com/pub/a/wireless/2001/05/03/longshot.html (10 June 2002)

Cringely, Robert X. "Bank Shot" 07 Feb. 2002. URL: http://www.pbs.org/cringely/pulpit/pulpit20020207.html (5 May 2002)

Arbaugh, William A. Shankar, Narendar. Wan, Y. C. Justin. "Your 802.11 Wireless Network has No Clothes" 30 March 2001. URL: http://www.cs.umd.edu/~waa/wireless.pdf (17 June 2002)

Cisco Systems, Inc. "Cisco Comments on Recent WLAN Security Paper from University of Maryland" 01 Nov. 2001. URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm (20 June 2002)

Other useful and pertinent sites:

http://www.openssh.org

http://www.openbsd.org

http://www.netbsd.org

http://www.joltage.com

http://www.boingo.com

http://www.sputnik.com

http://www.iptables.org

http://netfilter.samba.org/ipchains

http://slan.sourceforge.net

http://www.buffalotech.com

http://www.netstumbler.com

http://www.freeswan.org