GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Transmission Media Security

Charles R. Esparza

August 18, 2004

To Fulfill Requirements for SANS GSEC certification

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Abstract

When studying for any security certification the topic of transmission media is always present, it is one of the many sources of attacks that can be made by exploiting the media that the transmissions are made over. In this paper I will discuss the various types of media commonly used to connect computers into networks and analyze the many vulnerabilities of the different media types. Although my research did not uncover any new vulnerabilities (other than a newly discovered problem with WPA) it will nonetheless reiterate the importance of considering the media when planning for a secure network. All major media are discussed; copper, coax cable, fiber optic cable, and finally microwave and wireless media. The paper concludes with an overview of the new WPA standard and its recently discovered shortcomings.

Media Selection

When choosing a transmission medium, one of the first thoughts or considerations should be the security issues that could arise when choosing a medium for transferring data across the network. One of the questions that should be asked is "How valuable is the data being transferred on the network?" The typical attacker must feel like he or she has something to gain by assaulting your network, so if the data is financial information for example, the attacker or hacker might feel the risk is worth the effort. Another question to ask is "How sensitive is the data that is carried over the network segment?" If the organization identifies the accounting information as sensitive, then management must know where the information is stored and who has access to it. To protect the information and data, the work-flow path must be understood and also how it is used and who uses it. When a transmission medium is being considered, the organization needs to know if an intruder will be detected when using that media. The physical medium selected must be able to make eavesdropping and wire tampering as difficult as possible. One of the final things to consider when choosing a transmission medium is "How accessible is the backbone segment of the network?" If a would-be attacker is going to monitor your network, he or she is going to look for central nodes where they can collect the most information. Wiring closets and server rooms are prime targets because these areas tend to be junction points for many communication sessions.

Media selection is usually taken for granted; the most economical solution is usually taken as dictated by the building, which probably already has the media installed, or other considerations like radio frequency noice from nearby hospitals or manufacturing plants. Whatever security considerations have to be applied for each example of media used is normally simply accepted by the engineer designing the system and therefore not always a major point in planning the network. Inconveniences or vulnerabilities in the media are normally just "dealt with".

Copper Media

Copper media comes in various flavors; the most common is twisted pair. Twisted pair has the obvious problem that it can be tapped into at any point along which it is run. This is a nightmare for administrators since the media can run behind walls

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

and under floors where someone could tap into the cabling undetected. Twisted pair cabling also emits electromagnetic energy that can be picked up with sensitive equipment even without physically tapping into the media; this is known as cross-talk and for many years was just considered a nuisance. Now it is considered a security threat. When I was in the military we used a procedure called Tempest to try to prevent radiation of transmitted signals from reaching unwanted eavesdroppers. Tempest proofing meant that we would properly shield electromagnetic signals so they wouldn't be picked up by undesirable entities.

Twisted pair cabling is the most common used networking media in use today. Proper monitoring of the physical areas that the cabling is laid is the most effective way to deter tapping into of the media by undesirables. Use of switches in twisted pair networks also minimizes the tapping thread because signals are not broadcast as in bus networks but rather connected directly between communicating devices by the switch device. If communications of highly sensitive traffic is limited to a few nodes then only those nodes would require monitoring.

Twisted pair cabling comes in several different categories, the latest being category 6 cabling which is cable of carrying signals used in Gigabit Ethernet. Part of the threat of using twisted pair is the length of the cable runs, for most Ethernet LANs the distance between the node and the hub (or switch) normally does not exceed 100 meters or 328 feet. Exposed cabling is unsightly and can be dangerous if strewn along the walkways so it normally is concealed behind walls and through wiring closets outside the view of people. For this reason it is a security risk in that persons wishing to tap into the cable can also conceal themselves and their equipment by disguising themselves as maintenance workers or custodial personnel. Social engineering is often used in this type of disguise because most people ignore custodial personnel and will not challenge them if noticed in a wiring closet or in ceilings or false floors. The attackers could easily pretend to be performing janitorial maintenance while tapping into twisted pair cable runs.

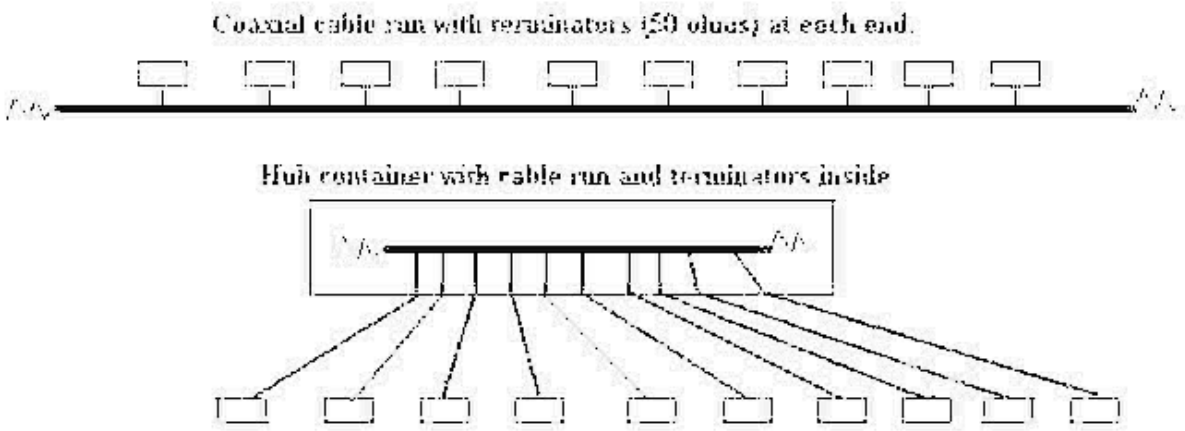
Coaxial Cable

Another copper type media is coaxial cable. Coaxial cable is made of a solid (or stranded) copper line that is surrounded by a dielectric material that aids in the establishment of the electrical characteristics of the cable (for example, the impedance at a certain frequency is partially determined by the type and thickness of the dielectric material surrounding the copper line. Around the dielectric is a woven sheath of metallic material which helps reduce electromagnetic emissions from the cable.

Coaxial cable used to be used extensively in 10Base5 and 10Base2 networks. These networks were common before 10BaseT networks replaced them. The concept of 10BaseT is not that much different from the older coaxial networks. The coaxial networks were rated on their maximum cable lengths which were 500 meters per segment for 10Base5 networks and 185 meters for 10Base2 networks. The cable segments were laid along the pathway that led to the nodes, or computers, and each node tapped into the cable as it passed the node. If any point along the cable run was broken then the entire network went down. The exact point of failure was not always easy to detect so the network could be down an indefinite period of time until the break could be found. The 10BaseT networks eliminated this particular situation by condensing the length of the cable run down to about 2 feet or less and putting it inside a container (the hub or switch) and extending the connection from the node to the cable

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

run to the current 100 meter limitation. Now the cable run could not be broken since it is only 2 feet long or less. Also, since the cable run was now contained within the hub or switch the terminators necessary on the older 10Base5 and 10Base2 networks could now be placed inside the hub so properly terminating cable runs was also no longer necessary. The individual cable connections could be broken and only the node connected to that cable connection would be affected. This improved the trouble-shooting time since the downed node could be immediately identified. See diagram below.



Coaxial cable is bulky, hard to work with, and expensive compared to twisted pair cabling. The network interface devices that are necessary to connect to coaxial cable are rarely manufactured anymore as well. For these reasons coaxial cable is seldom used but is still found in legacy networks. If used, they must be monitored in the same manner that twisted pair installations are monitored because they are easy to tap into just like twisted pair cabling.

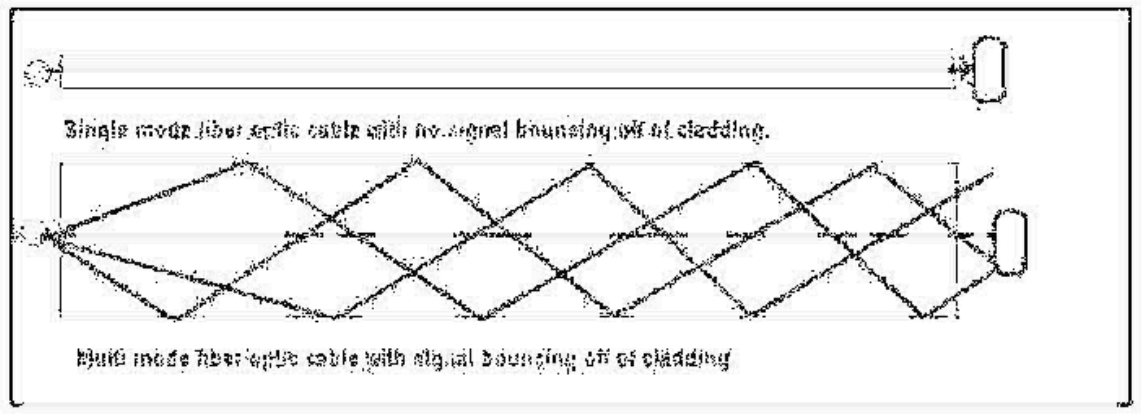
Fiber Optic Cabling

One of the transmission mediums that is considered very safe and secure is the use of fiber optic cabling. Fiber optic cabling connects networks together at a very high data rate. Of course this is determined by the capabilities and size of the fiber itself. Fiber comes primarily in 2 sizes, Single mode or Multi mode. There are several differences between Single and Multi-mode fiber. Single mode is much thinner (about 9 microns in diameter) and requires more expensive laser optics to connect nodes together. Single mode fiber is called that because the fibers are so thin that the signal takes a more direct route from end to end which avoids the loss of signal experienced when the signal bounces off of the sides of the walls of the cable (the signal gets reflected off of the cladding or outer sheath). See diagram below. The advantage of Single mode fiber is that the frequency ranges it supports are the highest available (often greater than 1-2 GHz) and the distance between repeaters is about 100 kilometers.

Conversely, Multi mode fiber is usually between 50 and 125 (or more) microns in diameter. This causes the signal to reflect off of the sides of the cable cladding so that multiple signals arrive at the distant end, often canceling each other out. The distance between repeaters for multi mode fiber is about 2 kilometers. Additionally the frequency range of multi mode fiber is much smaller than single mode (normally up to 400-500

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

MHz). However, even though Multi mode fiber has less capability than single mode it is still a very secure and robust media. The optics necessary to use are normally less expensive LED based mechanisms.



Difference between Single mode and Multi mode fiber optic cable.

Fiber Optic connections are considered very secure because the data is transmitted as beams of light; therefore no electromagnetic waves are generated. Insulation surrounds the fiber optic strands making it impossible to detect the light pulses without tapping into the actual strands.

The fiber strands are extremely thin and virtually impossible to tap into without breaking the strand, which would immediately shutdown the connection. The dielectric nature of optical fiber can eliminate the dangers found in areas of high lightning-strike incidence. Since optical fiber has no metallic components, it can be installed in areas with electromagnetic interference (EMI), including radio frequency interference (RFI). Areas with high EMI include utility lines, power-carrying lines, and railroad tracks. All-dielectric cables are also ideal for areas of high lightning-strike incidence. Unlike copper-based systems, the nature of optical fiber makes it virtually impossible to detect the signal being transmitted inside the cable. The only way to do so is by actually tapping into the optical fiber itself. This normally can be detected by surveillance systems and is usually accomplished during a sabotaged power outage or under other circumstances where detection would not be likely. These characteristics make fiber cabling attractive to organizations with major security concerns.

Even though Fiber Optics is considered the safest and secure transmission medium, security experts have known for decades that fiber-optic cabling can be tapped for interception of communications. However, until recently, such taps have been viewed as largely impractical.

The equipment used for tapping into is expensive and the number of fibers in the cables made it difficult to narrow down captured transmissions to a particular connection. In addition, physical interruption of the fibers could be detected using time-domain reflectometry, this, of course, makes taps hard to conceal. It was also common knowledge that separating the fiber strands and bending them in a tight curve would allow the escape of a small portion of the signal without revealing the data interception. Nonetheless, fiber-optic cabling was always viewed as very secure against wiretaps.

Various types of optical tapsare also used for corporate espionage, government espionage, network disruption or damage and other potential terrorist-type activities. Used secretively, optical taps allow access to all corporate or private voice and data communications transfering over a fiber link. A successful tap can be achieved with

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

merely an optical tap, packet-sniffer software, an optical/electrical-converter and a laptop. Packet-sniffer software filters through the packet headers, only extracting those packets which match a specific pattern, packet address, IP address or other characteristic such as a telephone number. Information gathered is then stored locally or forwarded to the intruder through various mechanisms, including wireless, another optical or copper line, another wavelength or channel, or other means.

Wireless Media

Wireless media is normally found in one of two configurations. One is using radio frequency transmissions for short haul communications between LANs not too far apart. The other configuration is wireless LANs which is discussed later. Use of the radio frequency spectrum is controlled by the Federal Communications Commission and all use of the frequency spectrum within the United States must be over an approved band of frequencies. The frequencies range from Megahertz (millions of cycles per second) to Gigahertz (billions of cycles per second) with newer systems going even higher. The wave lengths of these frequencies are determined by dividing the frequency into the number 1, which represents 1 meter, thus providing extremely small distances for wavelengths of the highest frequencies. For example, if a 1 megahertz frequency is divided into 1 meter then the resultant value for the wavelength (or Lambda, λ) would be 0.000001 of a meter or 1 millionth of a meter, hence the term microwave.

Microwaves are not considered secure media since the signal is transmitted over unsecure distances, often over metropolitan areas. The city of Scottsdale Arizona used a microwave system to link its northernmost offices with the main office downtown. The Maricopa Community College District (Phoenix, Arizona) also used to use a microwave to connect the various campuses to District headquarters in Tempe, Arizona. Any radio receiver along the route could pick up and decipher signals being transmitted between the two radio systems. Unless encryption techniques are utilized, the raw transmitted data is easily captured with radios purchased at any electronics store.

There is another side of transmission media considerations which is not secure or safe that many organizations use today. This type of network is wireless local area networks (WLAN) or WiFi. People generally assume that the biggest security hole in wireless communication is that the data is transmitted through air, thus allowing an intruder to catch the data with a receiver from a distance. While this is true that an intruder can catch the data, the data received is usually either encrypted or sent in spread spectrum.

WiFi

We have all heard stories of the small storefront that used wireless point of sale terminals to send sales data from the cash registers in the front of a store to the wireless access point (WAP) in the back of the store. War drivers could sit in the parking lot of the store and obtain all of the sales information to include customer credit card information. Although wireless is a great idea, used insecurely it could lead to consequences that could close your storefront for good.

In wireless LANs, the data is encrypted at a low level before it is sent to its destination, but the data could be captured and analyzed in higher levels, however, not

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

in lower levels as in copper or coaxial wired LANs. IEEE 802.11 is the approximate wireless version of the wired Ethernet IEEE 802.3 standard. Data security is an optional feature of the Media Access Control sub layer and is called Wired Equivalent Privacy (WEP), however, it doesn't supply an end-to-end privacy.

One of the concerns in a wireless LAN is that the source and destination addresses are not encrypted. Even if the data is encrypted, an intruder can see the direction and the amount of the data traffic and be able to determine the source and destination points or nodes. Also, since the data is only encrypted between stations, not on an end-to-end basis, this could be exploited if the intruder already has access on the network.

There are some new advantages in wireless transmission media now that make it not as insecure as it once was just a couple of years ago. Because each packet is examined for encryption/decryption, packet-filtering technologies can examine them right at the edge of a secure network. With the proper security policy in place, troublesome and unsecured applications can be disallowed. The resultant packets will be dropped; examples of such applications include online gaming apps, music sharing apps, and, of course, malware.

The main three ways that WEP uses to secure data are by the Service Set Identifier (SSID) using Open System Authentication, using Shared Key Authentication that is used by all stations to connect to the access point, and finally setting up your access point to accept only to accept the media access control (MAC) addresses of specific computers. All three of these paradigms are easily defeatable by downloading tools from the Internet.

Technology to the Rescue

As the areas that need encryption technology have grown and changed, the technology itself has improved in time. Once of the more advanced technologies that will provide protection for all types of media is IPSec or Internet Protocol Security. Organizations may have different reasons for using IPSec but it has proven to be a very secure methodology for improving secure transmissions regardless of the media. IPSec encryption is a powerful yet simple method to attain the security requirements that are demanded by many organizations. IPSec encryption can also enhance remote-backup and disaster-recovery systems that are used by large financial institutions. Using IPSec many enterprizes can maintain the integrity and confidentiality of customer data. IPSec can allow them to promote network security on critical network links between national, regional, and local banking centers.

WiFi Protected Access (WPA)

With the weaknesses in WEP being common knowledge along with the easily availability of tools accessed from Internet download sites it is not recommended that WEP be used in a high-security environment. A temporary or interim solution could be WiFi Protected Access or WPA. WPA has been around for about 3 years and seems to be working where WEP has failed, however, recently even WPA has been defeated. Certification for WPA devices began in February of 2003 by the Wi-Fi Alliance.

WPA uses a preshared key that is originated by the administrator of the wireless network. The two major changes that WPA uses to improve on the WEP standard is to use a new protocol called Temporal Key Integrity Protocol or TKIP. This enhanced

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

method of data encryption improves on the major points that WEP was weak in. For one, they use an extended initialization vector (IV) of 48 bits which was the major weakness in WEP's use of only 24 bits for its IV. It also includes an automatice re-keying mechanism which WEP did also not have. Finally, a new message integrity code (MIC or Michael) which guards against attempts at forgery. WEP used a 4 byte integrity check value (or ICV) to the wireless signal which was used to check the integrity of each frame. However, a cracker could change the bits in the encrypted packet without detection. WPA adds an 8 byte MIC that prevents this from happening.

Another improvement over WEP is the use of Enterprise-level User Authentication by using 802.1X and the Extensible Authentication Protocol (supported in Windows® 2000 and 2003 and XP). This provides a means to authenticate each individual user. WEP has no such feature. When used in a home or small office environment where no Enterprise level authentication server is available then the Preshared key is used to authenticate into the network.

The first condition in the switch from WEP to WPA is that all of your wireless devices must be WPA ready. That is, they must all support the WPA standards. This could mean that if your existing equipment is not WPA compliant you must upgrade all equipment by either purchasing new devices or by upgrading the firmware in the devices. Firmware upgrades are not for the faint of heart and can be rather daunting to the novice computer user. I have performed several firmware upgrades and have not had a problem yet but the risk of totally destroying your devices beyond a point of recovery exists whenever you attempt an upgrade.

WPA does not work while WEP is activated. You must decide whether you want to use the weaker WEP standard to switch to the WPA standard. They are incompatible so it is an all or nothing decision. Once you have determined that all of your equipment is WPA compatible then you are ready.

To activate WPA you simply switch over to the WPA-PSK (Preshared Key) menu and select it, you must uncheck the WEP setting unless it does so automatically. Using WEP and WPA on the same network is insecure because the weaker security scheme will allow security to be broken. In the enterprise environment you need a secure server such as a RADIUS server for authentication but in the home or small office environment you just need to create a PSK. All machines that hope to connect to this wireless access point (WAP) must also contain the same identical PSK in order for WPA to work. There are numberous compatibility issues in the relatively new industry but once you have obtained compatible devices then your home or small office network should be fairly secure.

As mentioned above, WPA provides an interim solution to the wireless security problem. It has been published in several places that the WPA-PSK security can be defeated!

At DEFCON 12, July 30-August 1, 2004, the Shmoo Group presentation bragged that it had defeated WPA wireless protection in their presentation. There is nothing specific to explain how they did it on their website as of this writing, however, there are other locations on the Internet explaining the weakness. They did allude to the fact that the weakness was in the PSK, that when the PSK was less than 20 characters long (the range is from 8 to 63 characters) that the PSK could be cracked. The article listed on the Works Cited page below by Larry Seltzer also claims that a PSK of less than 20 characters seems to be the major problem with WPA and advises everyone using WPA to use a much longer passphrase that uses special characters, numbers, and a mixture of capital and lower case letters.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

WiFi Networking News explained in an article in November 2003 (see URL link at end of this document) how the passphrase used as the Preshared Key in WPA networks could be determined by an internal attack:

> **"The Intra-PSK attack**
>
> The normal practice is to have a single PSK within an ESS. To generate any PTK, a device only needs to learn the two MAC addresses and nonces (and the selected ciphersuite). All of this is available in the initial exchange, from the ASSOCIATE through the 4-Way Handshake. Any device can passively listen for these frames and then generate the PTK. If the device missed these frames, it can send a DISASSOCIATE against the STA and force the STA to perform the ASSOCIATE through the 4-Way Handshake again.
>
> Thus even though each unicast pairing in the ESS has unique keys (PTK) there is nothing private about these keys to any other device in the ESS."

From this they determined that any station on the LAN could find the PTK, which is used to link another station to the access point using WPA. The process includes an offline dictionary attack but it would allow for intra network access and defeat of the WPA protection on that LAN.

Conclusions

Media is the common denominator on all networks. Depending on the type of media used an intruder can use various ways to detect the traffic that is being sent over the various media. When using copper based media one must be wary of eavesdropping by tapping into the cable itself or else use of sensitive devices to pick up cross-talk or other signals emanated. An improved media is fiber optic cabling, this media does not emanate any signals since it uses light sources to transmit the signals from node to node. It has proved to be the most secure media available for use on LANs today and will continue to be the most secure media until the black hats discover a way to tap it undetected. The last medium reviewed is the wireless media which uses the airways as their path from node to node. The only way to guarantee secure transmissions is to use a layered approach, or combination of techniques to try to encrypt the data. The best way currently to encrypt data over LANs is to use the IPSec protocol with any of the discussed media. IPSec security is compatible with all types of media so it is the one thing in common with all media that will almost guarantee the security of the pathways between nodes.

More and more networks are turning to wireless configurations for the advantages that they have. They virtually eliminate the cost of wire and cabling media because they use the airways as their transmission media. With the convenience of wireless media comes the threat of intrusion brought about because of weaknesses in the Wired Equivalent Privacy or WEP. A stop-gap improvement has been temporarily put in place by using WiFi Protected Access or WPA. Even though it is supposed to be the answer to WEP shortfalls for the next few years it has already been compromised, according to the Shmoo Group at their DEFCON 12 presentation on July 30th, 2004. Another article from WiFi Networking News has described how WPA can be defeated internally using captured information to extract the PTK from another workstation on the same wireless LAN.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

As mentioned in the introductory paragraph transmission media is tested in virtually all security certifications. It is often overlooked as a simple topic that many administrators could easily ignore as a "given". However, if not adequately monitored or prepared your transmission media could be the chink in the armor, the Achilles' heel, which brings your network down.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Works Cited

King, Todd, Infrastructure Security, Security + Training Guide, 2003, Que Publishing, Pps. 248-250

Zacker, Craig, Network Hardware, Network +, 2003. MSPress, Pps. 35-40

Kabay, M. E. "Tapping Fiber Optics Gets Easier." Network World Security Newsletter. 03 Mar 2003. < http://www.nwfusion.com/newsletters/sec/2003/0303sec1.html>.

The Wireless LAN Alliance: The IEEE 802.11 Wireless Standard, 16.8.1999 <http://www.wlana.com/intro/standard>

Palmquist, Scott. "Decrypt, The Keys to Wireless Security." April 2004. < http://www.wsdmag.com/Articles>.

Grimm, C. Brian, "Wi-Fi Alliance Announces Standards-Based Security Solution to Replace WEP", October 2002, http://www.wi-fi.org/OpenSection/ReleaseDisplay.asp?TID=4&ItemID=118&StrYear=2002&strmonth=10

PDF article from previous website "Overview WiFI Protected Access" http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

Higgins, Tim, "WiFi Protected Access Need to Know Part II", June 25, 2003 http://www.timhiggins.com/Sections-article50-page13.php

author unknown, Wi-Fi Alliance document, "Enterprise Solutions for Wireless LAN Security" February 6, 2003. http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Enterprise2-6-03.pdf

Mahoney, Doug, "Wi-Fi Remains a Work in Progress", January 20, 2004 http://enterprise-security-today.newsfactor.com/story.xhtml?story_title=Wi_Fi_Remains_a_Work_in_Progress&story_id=23030

Moskowitz, Robert, "Weakness in Passphrase Choice in WPA Interface", Nov. 2003, http://wifinetnews.com/archives/002452.html

Geier, Jim, "WPA Security Enhancements", March 2003. http://www.wi-fiplanet.com/tutorials/article.php/2148721

Seltzer, Larry, "Weakness Reported in Wireless Security Protocol", November 2003, http://www.eweek.com/article2/0,1759,1500082,00.asp

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.