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

WLAN Security: Insecurities of the WEP protocol and how WPA plans to overcome them

by
Kevin Sacco
December 29, 2003
GSEC Version 1.4b Option 1

© SANS Institute 2004, Author retains full rights.

Abstract

This paper takes a close look at two protocols that are used to secure wireless networks. Each protocol is examined and scrutinized on how it works, is implemented and attempts to protect the privacy of data within a wireless local area network. The design of the first protocol looked at, Wired Equivalent Privacy (WEP), is shown to have many flaws. Attacks can easily be carried out with simple tools that are readily available. Even though WEP is so insecure there are solutions to mitigate attacks against it. One of those solutions is the second protocol analyzed, Wi-Fi Protected Access or WPA. WPA significantly increases the security of a wireless network by tackling the weaknesses that were associated with WEP. By providing user authentication and stronger encryption, WPA can deter most attacks. Comparing both of these protocols, WPA can be distinguished as the protocol of choice for the future to come in secure wireless network environments.

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

1.0 WLAN Security Introduction

In the past couple of years wireless local area networking (WLAN) has exploded in the commercial world. It seems today everywhere you turn WLAN computing is taking place, from executives connecting wirelessly with a PDA to their corporate network, to the local coffee shop down the street providing Internet connectivity to anyone with a wireless network interface card. There is no avoiding it, wireless LANs are here to stay and are growing in number at a phenomenal rate. With a technology still so new and convenient, it should come to no surprise that it has particular problems, principally in the security of them. This is because like many technologies that we come to face with today, WLAN's are not inherently secure.

What makes wireless networks more vulnerable to attacks is that their network transmissions are not physically constrained to a building or its immediate surrounding area. Anyone with a wireless network card can easily connect to an insecure wireless network. The act of intentionally associating with wireless networks has led to the new hacker craze called war driving. These individuals actively search out using the appropriate tools wireless networks that they can connect to and utilizes its services. Most of the time the war driver is not actively trying to cause anything malicious in nature on the network but other times the attack may have destructive purposes. These attacks can leave our network incapacitated and wide open for just about any type of malicious activity that the attacker so chooses to perform. In this paper we will take a close look at two of the encryption algorithms that wireless LAN vendors have implemented in their products to mitigate such attacks.



Figure 1.1[1] War Driver armed with a laptop and a pringle can antenna searches for wireless networks to attack.

[1] Airtouch Networks. http://www.airtouchnetworks.com/.

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

2.0 Wired Equivalent Privacy (WEP)

To help prevent attacks the IEEE realized that there needed to be a secure way to communicate over wireless networks. In the development of the 802.11 standard, the IEEE working group proposed the following criteria for an encryption algorithm to meet the need of security:

- ✓ Exportable
- ✓ Reasonably Strong
- ✓ Self-Synchronizing
- ✓ Computationally Efficient
- ✓ Optional

At the time, WEP was the answer that was implemented. As we take a closer look at WEP in the next few sections, it will be seen that "WEP falls short of accomplishing its security goals"[2] that it intended and is not a reliable solution in today's wireless network environments.

2.1 What exactly is WEP?

WEP was designed to protect the privacy of individual transmissions from eavesdropping by intending to mirror the privacy found on wired networks. It protects against snooping by providing shared key authentication along with the encryption of data that is transmitted across wireless devices. The encryption available in WEP is from the RC4 stream cipher algorithm developed by Ron Rivest of RSA Security. The RC4 stream cipher was chosen for WEP because it was fast, strong, and simple for software developers to include in the code of their software.

2.2 How does WEP protect your data?

WEP is dependent on a key that is shared among wireless clients and an access point. The WEP secret key is an alphanumeric character string either 64 bit or 128 bit long. Using the RC4 stream cipher algorithm, the WEP key is expanded into a pseudorandom string called the key stream. This key stream is then exclusive OR (XOR) with the plaintext of the data that is ready to be transmitted to produce what is known as ciphertext. When the data is received the identical pseudorandom string is used and the ciphertext is reversed through the XOR process to achieve the plaintext of the data transmitted.

When developing WEP it was realized that the RC4 stream cipher algorithm is vulnerable to attack if there are no safeguards put in place. If the same key stream is used every time the data is encrypted, it can easily be used to determine the stream and decrypt plaintext transmissions. This is because

[2] Borisov, Goldberg, Wagner ,p.1.

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

once something is changed in the plaintext and encrypted using the XOR process with the same key stream the ciphertext will change accordingly. Gathering enough data and understanding what happens in the XOR process will allow you to decrypt all other transmissions that occur.

To defend against such attacks WEP implemented an integrity check (IC) algorithm and a 24-bit initialization vector (IV). The integrity check algorithm, CRC-32, is used to protect the integrity of the message by including a checksum within the plaintext of the data transmitted. In order to create a random key stream, the initialization vector is used. Each key stream that is generated, the IV creates a random value that gets added to the WEP key before being XOR with RC4. This random string that the 24-bit IV produces has the key space of only 2^{24} combinations. This limited key space makes the possibility of IV's being reused in a short period of time on high traffic wireless networks, as we will see later this was a major flaw in its design.

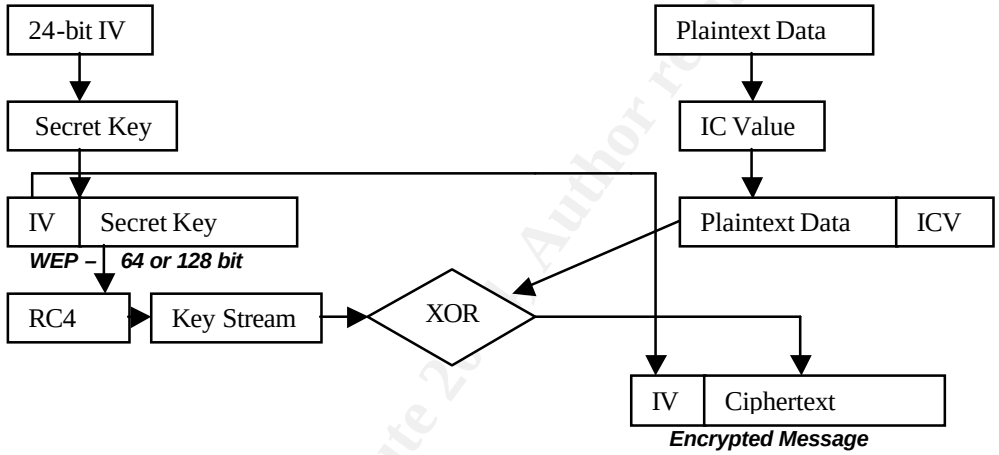

Figure 2.1 WEP encryption process

2.3 How can you implement WEP?

WEP can be implemented in either open or shared key authentication models. In open authentication, device authentication can be used with or without WEP. Without WEP there is no authentication except for knowing the appropriate service set identifier (SSID). When WEP is enabled, the WEP secret key becomes the authentication mechanism. Shared key authentication requires that all stations be validated by a shared secret, which is WEP. When a client requests association with an access point in shared key authentication the following steps occur:

1) The client sends a request to associate with the access point.
2) The access point sends a challenge to the client in the clear.
3) The client responds to the challenge by encrypting the challenge text with its WEP secret key.

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

4) The access point decrypts the encrypted challenge response with its WEP key to verify that it is the correct challenge it sent in step 2. If verified the client is authenticated to the access point and association can take place.

Though the requirement of using WEP in shared key authentication might make it seem more secure, it is not. Shared key authentication provides false security to the WLAN because of its weakness of sending the challenge in plaintext. If the plaintext is sent in the clear and then encrypted with WEP anyone sniffing the transmission can gather this information. By performing a brute force attack against the key space of the encrypted challenge, the WEP secret key can be discovered. Due to this problem, open key authentication with WEP is considered a more secure implementation of WEP.

In each model of authentication the WEP key can be used with either 64 or 128-bit encryption. This WEP key can be entered manually into every wireless device or dynamically using a centralized key server. When entering WEP keys statically every device must use the same WEP Key. If one device's WEP key is comprised every device on the WLAN must have its WEP key changed. For large Wireless networks, a centralized key server can provide much less overhead and stronger security because WEP keys can be rotated often at one centralized location for the entire WLAN.

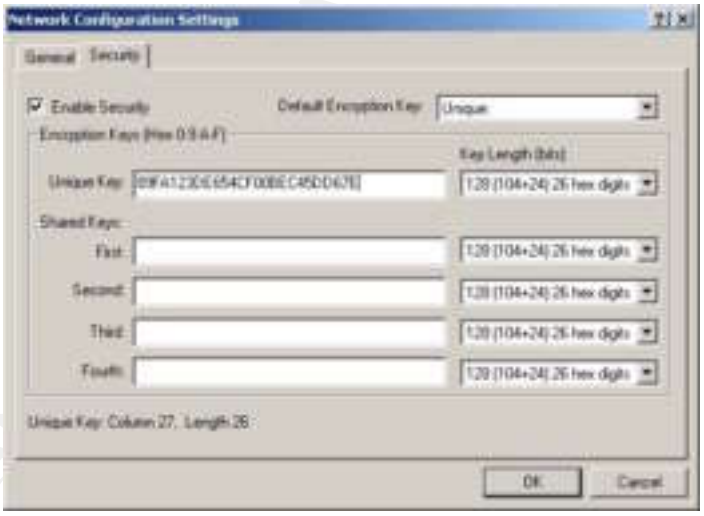

Figure 2.2 Configuring a client device with a unique WEP key

2.4 Attacking WEP's Weaknesses

The primary reason WEP is weak is due to the short initialization vector that is sent in cleartext. Having only 2^{24} combinations for the IV, "a single Access Point running at 11 Mbps can exhaust the entire keyspace within an hour."[3] It is

[3] Barnes et al.,p. 207.

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

also to note that the IV starts at 0 and increments by 1 each time a message is sent. If a collision occurs or the key space is exhausted the IV is initialized to 0. Armed with this knowledge WEP is open to several different types of attacks.

2.41 Active attack to inject new traffic

In this type of attack, the attacker injects a legitimate message by forming a new message from knowing the correct plaintext for an encrypted message. "Knowledge of both plaintext and ciphertext reveals the keystream"[4] that is needed to construct a new message. Once the keystream of a packet along with its IV is known, recreating new packets is as easy as XOR the plaintext with the keystream and adding the corresponding IV. Using this information allows the attacker to create any valid packet on the wireless network "circumventing the WEP access control mechanism."[4]

2.42 Active attack to decrypt traffic

This attack involves modifying the header information of an encrypted packet and sending it through the Internet to retrieve it as plaintext. This works by allowing the attacker to modify header information such as destination address and port number of an encrypted packet. The attacker sends the encrypted packet with the malformed header through an access point to a device he controls on the Internet. When the encrypted packet is sent through the access point and put on the wire it decrypts the packet because WEP is not used on the wired network. The attacker receives the plaintext message on the device they have set up on the Internet.

2.43 Passive attack to decrypt traffic

To perform this type of attack, an attacker sniffs wireless traffic until an IV collision occurs. Utilizing statistical analysis, the traffic can be predicated and accuracy increased to discover a packet with the same IV. When two messages with the same IV are discovered they can be XOR together to obtain information about the contents of both messages. When the plaintext of one message is found, any other messages using that IV can be decrypted also.

2.44 Table attack

For this attack to work the attacker needs to know the keystream used to encrypt a message that corresponds to each IV. The keystream is usually obtained by finding the plaintext of an encrypted message. If the attacker continues to gather keystreams that correspond to other IV's, a table can be built to decrypt traffic. Once this table contains all of the corresponding IV's it can decrypt traffic in real time.

[4] Borisov, Goldberg, Wagner , p.5.

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

2.5 Tools used to exploit WEP

- *Netstumbler* – Used to detect the presence of a wireless network, SSID and find out if WEP is enabled on the network.
- *Airsnort* – Linux tool used to passively gather wireless transmissions and crack the WEP key by using known exploits.
- *WEPcrack* – Linux tool used to crack WEP key by using known exploits in RC4 stream cipher.
- *AiroPeek* – Advanced sniffer that captures all wireless transmissions and finds exploits to attack the WLAN.
- Other sniffers – *Ethereal*, *TCPDump*, *WinDump*, *ngrep*

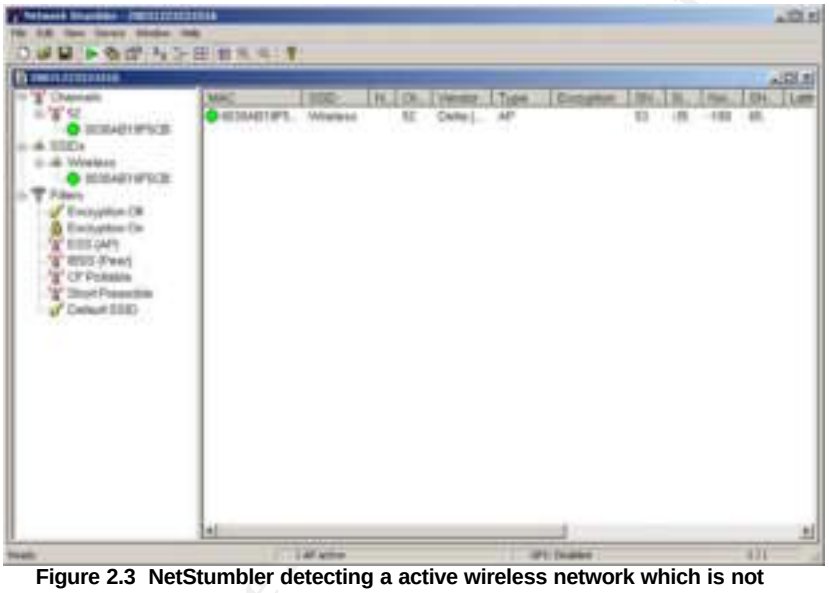

Figure 2.3 NetStumbler detecting a active wireless network which is not using WEP encryption

2.6 Preventing WEP attacks

Even though WEP contains much vulnerability, having it enabled is better then not having any encryption at all. Cracking WEP requires the knowledge and tools to do so; only persistent hackers will attempt to circumvent it. Using dynamic WEP keys as per-session or per-packet distribution from a centralized key server makes it very difficult for an attacker to predict the WEP key. Hardening the WLAN by the use of a non-broadcast SSID, MAC filtering, and protocol filtering can also enhance the overall security of the wireless network.

One of the best methods to really secure a wireless network is to encrypt its traffic through a VPN tunnel. When a client needs access through the access point to the rest of the LAN, all traffic must be authenticated and encrypted through the VPN tunnel. Combining WEP with a VPN solution adds multiple layers of security. If an attacker wanted access to the data they now would have to know the username and password for the VPN and then crack through WEP encryption.

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

3.0 Wi-Fi Protected Access (WPA)

The unsuccessful security of WEP has caused many people to be skeptical of installing wireless networks. A new protocol that could resolve these problems and bring confidence back in the security of wireless networks was needed. The Wi-Fi Alliance answered this call with the release of Wi-Fi Protected Access (WPA) earlier this year. "WPA addresses the flaws in Wired Equivalent Protocol"[5], it adds stronger encryption and user authentication to fix the vulnerabilities that plagued WEP. The next few sections will explain how WPA was built to overcome the problems of WEP and if WPA has any troubles itself.

3.1 What is this new protocol WPA?

WPA is part of the new developing standard IEEE 802.11i that will be mandatory in all wireless devices in the near future. The Wi-Fi Alliance created WPA to correct the problems of WEP and provide a solution that would be compatible with all existing and future 802.11 standards. Existing 802.11, 802.11b, 802.11a, and 802.11g hardware will have software upgrades to allow WPA to interoperate with them. WPA is a complete security replacement for the weaker WEP. All identified attacks to WEP are to be mitigated by WPA.

3.2 How does WPA protect your data?

WPA provides two main ways to secure data within the WLAN, authentication and encryption.

3.21 Authentication

802.1x authentication with Extensible Authentication Protocol (EAP) is required when using WPA. The 802.1x authentication protocol is a port-based access control method and provides a secure means to authenticate a user across the network. The EAP portion of the authentication mechanism allows for several different methods to be used to authenticate the user such as certificates, passwords, or smart cards. 802.1x authentication works in two phases within WPA:

1. Open systems authentication is used to authenticate the wireless station to an access point so it can begin to transmit frames of data.
2. 802.1x /EAP is used to authenticate the user against an authentication server in enterprise mode.

Taking in consideration home users and small organizations that don't have authentication servers, pre-shared key (PSK) mode is the alternative.

[5] Wi-Fi Alliance, p. 1.

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

Security is provided through a shared secret key in which a client authenticates with it to an access point. This secret key is essentially a password that is manually entered on the client and access point devices. In order for a client to communicate on the wireless network its password must match the access points password.

3.22 Encryption

The encryption utilized in WPA is still from the RC4 algorithm that was used in WEP but temporal key integrity protocol (TKIP) enhances it. The use of TKIP provides the following improvements in data encryption over WEP:

- *48-bit Initialization Vector (IV)* - Increases the key space for the IV to more then 500 trillion combinations and provides new rules of sequencing. This drastically diminishes the reuse and predictable of an IV preventing attacks against it. The IV is separated now from the overall key leaving the full use of the 128 bits to the WPA key.
- *Message Integrity Code (MIC)* - Increases security over the integrity check value that was used in WEP. Inhibits an attacker from performing a man-in-the-middle or replay attack by calculating an 8-byte MIC field. If the calculation of the MIC doesn't compare correctly from sender to receiver the data packet gets discarded
- *Dynamic keying mechanism* – WPA automatically creates a random key and distributes to each client. Each frame that is generated actually has a new key that it uses. When WEP was used the same key would be used for a long period of time allowing an attacker to obtain that key. Dynamic per-packet keying prevents anyone that discovers your key to be able to use it for an attack.

"By greatly expanding the size of keys, the number of keys in use and by creating an integrity checking mechanism, TKIP magnifies the complexity and difficulty involved in decoding data on a Wi-Fi network. TKIP greatly increases the strength and complexity of wireless encryption, making it far more difficult—if not impossible—for a would-be intruder to break into a Wi-Fi network. "[6]

3.3 Implementing WPA

WPA will be supported in all new wireless devices and upgrades will be provided for existing devices. Organizations that currently have 802.1x /EAP authentication servers already in use will be able to integrate WPA in to its current structure. For organizations that want to take advantage of WPA's enterprise mode a RADIUS-based authentication server must be deployed. Small Office/Home Officer users that operate WPA in PSK mode will only need to upgrade or implement WPA software and firmware into their access points and client devices. A matching password will need to be configured in PSK mode in the access point and client devices for authentication to take place.

[6] Wi-Fi Alliance, p. 4.

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

Migration to a completely WPA infrastructure can be taken in steps because it is possible for an access point to support both WEP and WPA clients concurrently. The access point establishes whether clients are using WEP or WPA when a client attempts to associate with it. Operating this way is considered to still be insecure because WEP is still open to the same weaknesses. It is recommended that the transition to WPA be conducted quickly to minimize the amount of time operating in a mixed environment.



Figure 3.1 Configuring a wireless network card for use with WPA

3.4 Is WPA vulnerable to any attacks?

WPA does a good job in correcting many of the flaws that was associated by its predecessor WEP. Even though it is a much more secure protocol, it has been pointed out in a paper written by Robert Moskowitz that WPA can be weak in its implementation of pre-shared key mode. The passphrase used in PSK is a 256-bit or 8 to 63 character hexadecimal number. This passphrase is usually one static number entered into the wireless client and access point devices. When a WPA device creates data encryption keys for the session using a four-way handshake, attackers can guess the passphrase. To exploit this weakness, attackers passively sniff out the four-way handshake key exchange and gather the passphrase from it. A standard offline dictionary attack can then be performed against the passphrase. Once the passphrase is obtained any user can join the wireless network as a trusted source. Any implementation of PSK that is using less then 20 characters could be an easy target for this attack. It is recommended to prevent this exploit that more then 20 characters randomly

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

generated be used for the passphrase. An alternative would be to implement enterprise mode by using an 802.1x authentication server. Enterprise mode protects against this type of attack because there is no passphrase that is used and the WPA key is dynamically updated.

Another vulnerability that WPA does not protect against is a denial of service (DoS) attack. A DoS attack can be carried out by sending at least two packets each second with the wrong encryption key to an access point. The access point will react to this attack by closing all connections for one minute to the wireless network. The access point does this to protect unauthorized access across the network. Continually sending these packets will repetitively deny network services to any authorized users on the WLAN.

4.0 Conclusion

After examining WEP it is clear to see that it is no longer sufficient in protecting wireless networks from determined attackers. The tools to perform attacks against WEP are easily obtained and to use. When WEP is implemented within a VPN tunnel or with 802.1x authentication it can be deterred from attackers. A more promising solution to WEP is using WPA. WPA clearly addresses all of the weaknesses that WEP has been burden with by correcting them. The backward and forward compatibility allows WPA to be implemented easily without an overhaul of an existing entire wireless network. When applied correctly both modes can be a secure means of protecting the wireless network, though enterprise mode provides a much better solution. In conclusion utilizing the full features of the WPA protocol can mitigate any attack that WEP experienced, providing a reliable solution for wireless networks for years to come.

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

References

1. Airtouch Networks.URL: http://www.airtouchnetworks.com (10 DEC 2003).
2. Arbaugh, William, Narendar shankar, and Y.C. Justin Wan. "Your 802.11 Wireless Network has No Clothes." 30 March 2001. URL: http://www.cs.umd.edu/~wea/wireless.pdf (20 OCT 2003).
3. Barnes et al. Hack Proofing Your Wireless Network. Syngress Publishing Inc., 2002.
4. Borisov, Nikita, Ian Goldberg, and David Wagner. "Intercepting Mobile Communications: The Insecurity of 802.11." July 2001. URL: http://www.cs.berkeley.edu/~daw/papers/wep-mob01.pdf (17 OCT 2003)
5. Doran, Andy. "Wireless Security: Is Protected Access Enough?." Network Magazine. October 2003: 48-50.
6. Emigh, Jacqueline. "WPA: Is Wi-Fi's Security Bandage Going to Win Over Network Admins?." 02 December 2002. URL: http://www.wi-fiplanet.com/tutorials/article.php/1550561 (23 OCT 2003).
7. Geier, Jim. "802.11 WEP: Concepts and Vulnerability." 20 June 2002. URL: http://www.wi-fiplanet.com/tutorials/article.php/1368661 (20 OCT 2003).
8. Geier, Jim. "WPA Security Enhancements." 20 March 2003. URL: http://www.wi-fiplanet.com/tutorials/article.php/2148721 (20 OCT 2003).
9. Geier, Jim. "WPA plugs holes in WEP." 31 March 2003. URL: http://www.nwfusion.com/research/2003/0331wpa.html (23 OCT 2003).
10. Grimm, Brian. "Features – WiFi's Protected Access wireless: the background." 23 November 2003. URL: http://www.newswireless.net/articles/021123-protect.html (23 OCT 2003).
11. Kane, Margaret. "Wi-Fi getting new security standard." 31 October 2002. URL: http://zdnet.com.com/2100-1105-964046.html (20 OCT 2003).
12. Moskowitz, Robert. "Weakness in Passphrase Choice in WPA Interface." 04 November 2003. URL: http://wifinetnews.com/archives/002452.html (05 DEC 2003).
13. Roberts, Paul. "Paper finds security flaws in new wireless standard." 11 November 2003. URL: http://computerworld.com/printthis/2003/0,4814,87044,00.html (05 DEC 2003).
14. Walker, Jesse. "Unsafe at any key size: an analysis of the WEP encapsulation." 27 October 2000. URL: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (17 OCT 2003).

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

15. Wi-Fi Alliance. “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks.” 29 April 2003. URL: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf (23 October 2003).

© SANS Institute 2004, Author retains full rights.