Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

An Overview of 802.11 Wireless Network Security Standards & Mechanisms

The 802.11 wireless networks is one of the most attractive and fast growing networks. Because of its easy and fast deployment and installation, there are more and more users considering using this type of network than the wired version. In this document, you will find out how to secure an 802.11 wireless network by understanding its security protocols and mechanism. We will describe security protocols such as WEP, WPA and 802.11i, and mechanisms such as MAC access control list; their vulnerabilities and tools available...

Copyright SANS Institute
Author Retains Full Rights

AD

An Overview of 802.11 Wireless Network Security Standards & Mechanisms

GIAC Security Essentials Certification (GSEC)
Practical Assignment 1.4c

Luis Carlos Wong
21 October 2004

Table of Contents

1. Abstract 2

2. Basic Wireless Lan Concepts 2

3. IEEE 802.11 Security 4

3.1. Access Control List 4
3.2. WEP (Wired Equivalent Privacy) 5
3.2.1 WEP Key recovery 7
3.2.2 IV collision 8
3.2.3 Dynamic WEP 8
3.3. WPA (Wi-Fi Protected Access) 9
3.3.1 TKIP (Temporal Key Integrity Protocol) 9
3.3.2 MIC (Message Integrity Code) 10
3.3.3 802.1x Port based Network Access Control 11
3.3.4 WPA-PSK (WPA Pre-Shared Key) 11

4. 802.11i 12

4.1. AES-CCMP (Advanced Encryption Standard – Counter mode CBC MAC Protocol) 12

5. Wireless Networks Tools 13

5.1. MAC spoofing 13
5.2. Wireless Analysers 13
5.3. WEP Cracking Tools 13

6. Conclusions 14

7. References 14

© SANS Institute 2005, Author retains full rights.

1. Abstract

The 802.11 wireless networks is one of the most attractive and fast growing networks. Because of its easy and fast deployment and installation, there are more and more users considering using this type of network than the wired version.

In this document, you will find out how to secure an 802.11 wireless network by understanding its security protocols and mechanism. We will describe security protocols such as WEP, WPA and 802.11i, and mechanisms such as MAC access control list; their vulnerabilities and tools available to exploit these vulnerabilities. Knowing how these mechanism and protocols works, including its weakness and vulnerabilities can be very helpful for planning, designing, implementing and/or hardening a much secure wireless network, effectively minimizing the impact of a attack.

2. Basic Wireless Lan Concepts

The IEEE 802.11 is a family of standards, each one defining and specifying parts of the standard. Some of these standards are:

Physical and Max data rate specification

802.11b, using the 2.4 GHz radio spectrum and 11 Mbps max data rate.
802.11a, using the 5 GHz radio spectrum and 54 Mbps max data rate.
802.11g, using the 2.4 GHz radio spectrum and 54 Mbps max data rate.

Security

802.11i Wireless Robust Security Network. This standard defines the 802.11 wireless network security protocols.

QoS (Quality of Service)

802.11e Quality of Service in 802.11 wireless networks. This standard defines the QoS for traffic prioritization to give delay sensitive application such as multimedia and voice communication priority.

The 802.11 wireless networks operate in two basic modes: infrastructure and ad-hoc.

Infrastructure mode is the most common operation mode in which we could find wireless networks. In this operation mode, each wireless client connects directly

© SANS Institute 2005 Author retains full rights.

to a central device called Access Point; there is no direct connection between others wireless clients. An Access Point acts as a wireless hub that connects the wired network with the wireless clients and handles the connections between them. This device is also the main responsible for handling the clients' authentication, authorization and link-level data security, such as access control and enabling data traffic encryption.

Ad-hoc mode is the less common operation mode but is important as infrastructure mode. In this operation mode, each wireless client connects directly with each other. There is no central device managing the connections, meaning that each wireless client talks to each other freely. The main advantage of this operation mode is that it permits a rapid deployment of a temporal network where no infrastructures exist, e.g. in a case of natural disaster emergency. Flexible and easy to use, security in this type of network is harder to implement because there is no central device that could authenticate and authorized the wireless clients. Each node must maintain its proper authentication list.

To acknowledge the wireless clients for the presence of near surrounding wireless networks, the wireless networks periodically generates a beacon signal (generally around 100ms between each one). In infrastructure mode, the Access Point generates this signal; in ad-hoc mode, one random station assumes the responsibility. A beacon is a small broadcast data packet that reports the characteristics of the wireless network, with information such as supported data rate (max data rate), capabilities (encryption on or off), Access Point MAC address, SSID (wireless network name), etc.

The SSID (Service Set Identification) serves to identify a particular wireless network. A client that wants to join a wireless network must set the same SSID as the one in that particular Access Point. Without it, the wireless client will not be able to select and join a wireless network. Some vendors are taking this as a security measure, hiding the SSID from the beacon. Hiding the SSID cannot be considered as a security measure because it will not make the wireless network invisible and can be easily defeated using wireless network analyzers. Most wireless network analyzers are capable of obtaining the hidden SSID by passively sniffing it from any probe signal containing the SSID.

Even if you turn off the SSID broadcasting, the beacon signal cannot. An Access Point, with the SSID hidden, generates the beacon with the SSID field in blank, making it visible to anyone with a wireless network analyzer tool, e.g. Kismet Wireless[1].

[1] URL: http://www.kismetwireless.net/

© SANS Institute 2005 Author retains full rights.

3. IEEE 802.11 Security

Due to the RF signal nature of the wireless network, it is very difficult to control which computers or devices are receiving the wireless network signal. Therefore, the wireless relies on software link-level protection, specifically implementing cryptography to protect from eavesdropping and other network attacks. The original 802.11 standard only offers WEP to secure the wireless network.

3.1. Access Control List

The access control list is the simplest security measure we can find in a wireless network. The protection offered by this mechanism mainly consists of filtering out unknown users and requires a list of authorized client's MAC addresses to be loaded in the Access Point. Only those registered MAC addresses will be able to communicate with the Access Point, and will drop any communication that come from others not registered MAC addresses.

As the name of this mechanism implies, it just offers access control to the network behind the access point, no any other protection are offered, meaning that it will not protect each wireless client nor the wireless network traffic confidentiality or integrity. Therefore, any wireless network protected with only this mechanism is very vulnerable and open to any network attack.

In addition, this security mechanism can be easily defeated, making it ineffective as a access control measure; it turns out that is relative easy to change the MAC address on practically any wireless network interface temporarily (at least in Windows and UNIX/Linux OS). Changing the MAC address to impersonate another user or device is called MAC spoofing. In UNIX/Linux OS, we only need to execute one command to do MAC spoofing[2]:

ifconfig **eth0** hw ether **00:01:02:03:04:05**

Where:

eth0 is the network interface we want to modify.
00:01:02:03:04:05 is the MAC address we want to specify with numbers in hex number format.

In Windows environment, we need the help of tools designed specially for this intention. There are at least two tools available for MAC spoofing:

[2] The network interface must be down before executing this command.

© SANS Institute 2005 Author retains full rights.

a. SMAC[3], from KLC Consulting, and
b. MAC Makeup[4] (freeware), from H&C Works

Both have easy to use graphical interface, are compatible with Windows 2000 and XP, does not require installing any driver and are nearly compatible with any network interface card, including wireless.

With the help of wireless analyzers utilities, anyone can obtain by its own a list of registered MAC addresses, allowing anyone to use this information to penetrate in a not well-protected wireless network. Wireless analyzers are very powerful utilities that can passively monitor or sniff wireless network traffic, gathering important information about the wireless network.

3.2. WEP (Wired Equivalent Privacy)

Initially, WEP (Wired Equivalent Privacy) was the only link-level security option defined in the 802.11 standard. Its main purpose was the protection of the confidentiality and integrity of the wireless network traffic. WEP was designed to provide comparable confidentiality to a traditional wired network, hence the name.[5]

To meet the security proposed, WEP uses encryption to protect the data. WEP uses the RC4 stream cipher with a 64 or 128 bits key to provide data packet encryption. In addition, WEP can be used as a access control method, because once WEP is active, the Access Point will just establish communication with nodes that have the same shared secret key, rejecting the others.

In a WEP-protected wireless network, every member of this wireless network, the wireless clients, must share the same secret key with the Access Point. This secret key can be a password or a character sequence generated by a wireless configuration program using a passphrase. It is not relevant how the secret key is introduce, especially true when using cards from several manufacturers, the most important thing is that every member of the wireless network must have the same WEP secret key.

We have mentioned that WEP uses a 64 or 128 bits key to encrypt the data, but actually, the effective key is smaller, because part of the WEP key is transmitted in clear text along with the data packet. The WEP key, the key used to encrypt the data packet, is a concatenation of two values, a dynamic value called Initialization Vector (IV) and the static part of the key, the shared secret key. The Initialization Vector (IV) is a dynamic 24-bit value chosen randomly by the transmitter wireless network interface to give the WEP key liveness, giving more

[3] URL: http://www.klcconsulting.net/smac/
[4] URL: http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp
[5] Wikipedia, "Wired Equivalent Privacy"

© SANS Institute 2005 Author retains full rights.

than 16 millions possible keys. Liveness is required in WEP key because each message must be encrypted with a different key. The length of the shared secret key depends of the WEP key size chosen. When a 64 bit key is used, the shared secret key is 40 bits long (5 ASCII character) and for a 128 bit key, the shared secret key is 104 bits long (13 ASCII character). To synchronize the WEP key, the transmitter with the receiver, the IV value is transmitted in clear text along with data packet, therefore revealing 24 bits of the 64 or 128 bits key.

In a WEP-protected wireless network, a data packet that gets into the link-level is encrypted before sending it off the air. The data packet encryption is performed as follow:

First, the wireless network interface randomly chooses an IV value and concatenated with the shared secret key to form the WEP Key (IV + secret key). The 802.11 standard does not define how the wireless network interface must be chosen. Therefore, the way the wireless network interface chooses the IV value depends on the manufacturer.

When the WEP Key is ready, this key is passed to the RC4 stream cipher to produce a pseudo-random string with the data packet length. The actual encryption occurs when the wireless network interface performs a logical XOR operation between the data package with the pseudo-random string. To complete the WEP-protected data packet, the link-level headers, IV value and the encrypted data packet are packed together and then transmitted to the recipient.

The steps for encrypting messages are also the same steps for decrypting a WEP-protected data packet. When the recipient decrypts a WEP-protected data packet, it first reads the IV value and then follows the same steps of the encryption process. A particular WEP key (the same IV and shared secret key) will always produce the same pseudo-random string, making it possible to regenerate the same pseudo-random string.
Finally, the data is decrypted by performing a second logical XOR operation between the encrypted data packet with pseudo-random string, canceling the effect of the first logical XOR operation.

© SANS Institute 2005 Author retains full rights.

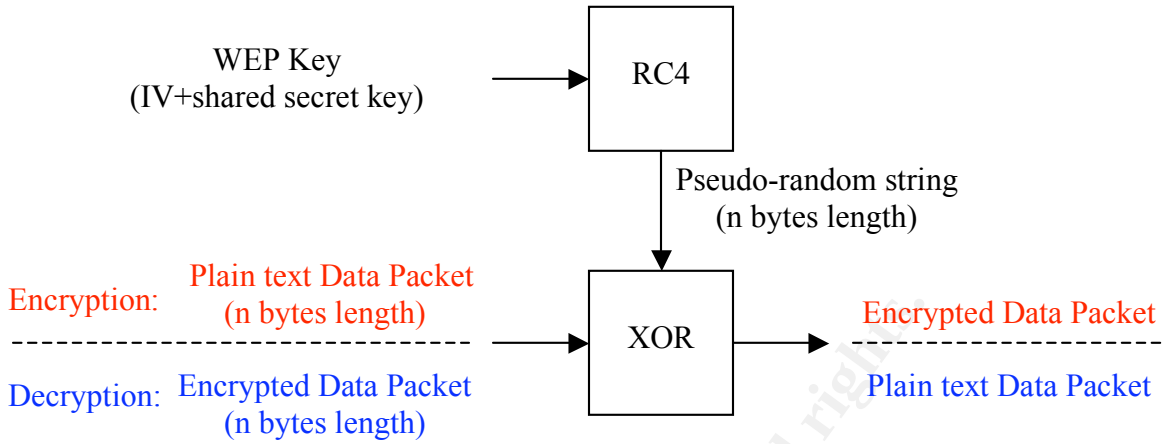

Figure 1. WEP Encryption/Decryption Process. (Black) Common steps, (Red) Encryption Process, (Blue) Decryption Process.

When the WEP was designed, it was considered sufficiently secure, until a research find out a weakness that was inherent in the WEP mechanism. From that time ever, several tools have been developed for cracking successfully the WEP shared secret key, turning it insecure.

3.2.1 WEP Key recovery

The WEP protocol contains a critical cryptographic weakness that allows an attacker to possible recover the shared secret key. This weakness consists of exploiting the fact that certain IV value produces weak WEP keys. When a weak WEP key is used to encrypt, the first bytes of the pseudo-random string may contain some correlation with the WEP key. Each weak key may leak one byte of the shared secret key with a 5%[6] certainty probability. Because the certainty level is not high, the attacker must capture large amounts of raw WEP-protected data packets, approximately from 5 Million to 10 Million packets[7], to elevate the probabilities for successfully crack the shared secret key. This weakness was publish by Fluhrer, Mantin,and Shamir, in "Weaknesses in the Key Scheduling Algorithm in RC4".

Several tools for WEP cracking have already been around for a while. Some of the first tools that exploit the FMS weakness are Airsnort[8] and Wepcrack[9]. There are also others tools that have more capabilities, including optimizations for requiring less weak WEP-protected data packets and brute-force attacks. Some

[6] Airsnort, URL: http://airsnort.shmoo.com/faq.html
[7] Airsnort, URL: http://airsnort.shmoo.com/
[8] Airsnort download, URL: http://sourceforge.net/projects/airsnort
[9] Wepcrack, URL: http://wepcrack.sourceforge.net/

© SANS Institute 2005 Author retains full rights.

of the tools are: Airjack, dwepcrack, Aircrack. Generally, this tools works on a UNIX/Linux platform, but some tools are already ported to Windows OS.

Attackers, using any of this WEP cracking tools, have a good chance to obtain the shared secret key by passively capturing large amount of wireless network traffic. Once the attacker successfully obtains the shared secret key, the wireless network is totally defenseless.

3.2.2 IV collision

Another way for an attacker to break into a wireless network without knowing the shared secret key is by also capturing passively a large amount of data packets, but this time is looking for IV collision. An IV collision occurs when two or more data packets are encrypted with the same IV value, therefore the same WEP key. When an IV collision is detected, the attacker can perform a logic XOR with the two encrypted data packet to take off the encryption. The result is the XOR of the two data packets. With enough time, and use of analytic and statistics methods the attacker could be able to recover the contents of the two packets. The data packet contents recovery effort and time required decreases when more packets encrypted with exactly the same WEP key are captured and used for the recovery. Note that if this attack is successfully accomplished, the pseudo-random string recovery for a particular WEP key is straightforward. An attacker could then keep all the pseudo-random strings in a record, using it for decryption, packets forging, and access to the network

Some wireless interface card vendors, aware of the WEP key vulnerability, offer an update for their wireless cards to address the weak key vulnerability by avoid using weak IVs for encryption. Avoiding some IVs reduces the number of WEP keys making the IV collision weakness worse.

3.2.3 Dynamic WEP

Before an attacker can actually access to a WEP protected network, he needs to capture a large quantity of data packets to crack the shared secret key. If the wireless network could change the shared secret key every time before the attacker could get enough data packets to crack the secret key, it will make it much harder to crack the secret key. Therefore, a way to prevent a possible secret key recovery without making any other vulnerability worse is by changing the shared secret key frequently. Using the current WEP mechanism could be very troublesome because it does not include any automatic key rotation system that could support this solution.

A solution to achieve this goal is using the 802.1x protocol to provide automatic key delivery and periodic rekeying. The 802.1x protocol handles the user

© SANS Institute 2005 Author retains full rights.

authentication and authorization process. The authentication server generates the WEP key when a user is authenticated and authorized.

3.3. WPA (Wi-Fi Protected Access)

WPA is a solution released by the Wi Fi Alliance while a definitive security protocol is standardized. This security protocol is based on 802.11i, the next 802.11 wireless network security protocol standard. WPA consists of three main components: TKIP, 802.1x, and MIC. Each component was designed and implemented to address specifics 802.11 weakness.

Important security improvements were implemented, such as key hierarchy that protects and practically nullifies the exposure WPA main key from attacks and implementing 802.1x protocol for access control to the network. Using key hierarchy means that WPA does not directly use the main key to encrypt, instead the main key (Pairwise Master Key) is used to generate other temporal keys such as session keys, group keys, etc; and recursively the session key is used to generate the per-packet encryption key. The IV is also expanded from 24 bits to 48 bits long and assigning it another role as a sequence counter for avoiding replay attacks. Improvement in packet integrity protection is made by implementing a specially designed cryptographically protected hashing function instead of using the CRC32 linear function.

3.3.1 TKIP (Temporal Key Integrity Protocol)

This protocol is the direct replacement of WEP and it addresses most critical vulnerability. Within its designed goal was to maintain compatibility with existing 802.11 hardware so they could be upgraded via software. One of the most important enhancement from WEP is that each packet is guaranteed to use a completely different key by generating it by a per-packet key mixing function instead of a concatenation of the IV and the shared secret key.

Most of the cryptographics functions are hard-coded in the wireless network interface hardware; therefore, it cannot be upgraded by software. Because of these limitations, the WPA protocol reuses some of the WEP protocol hard coded functions to ensure compatibility and performance. Functions like the RC4 stream cipher output function are hard coded in the wireless network interface and cannot be changed. To solve this problem, TKIP reuse the RC4 stream cipher, but it changes the way of using the shared secret key. Instead of using the shared secret key directly to the cipher, it is used only as a seed for generating others keys. This approach minimizes the exposure of the shared secret key to any attack. The first key generated is the session key. This key is used as a seed for generating the per packet key.

© SANS Institute 2005 Author retains full rights.

How does TKIP work?

Each packet's key is generated by a per-packet key mixing function. The per-packet key is generated by hashing the senders MAC address, the IV, and the session key. To lower the processing power required to generate each per-packet key, the per-packet key mixing function is divided in two phases:

Phase 1: This first phase is the most processor intensive task, but this value is calculated once for each session. The senders MAC address, temporal session key, and the highest 32 bits of the initialization vector are hashed together. The result from this phase remains intact until a session key change occur or each time the IV upper 32 bits change.

Phase 2: This phase is calculated for each packet received. The lowest 16 bits and the result of the phase 1 are hashed together. The result of this phase is the 104 bits per-packet key.

After the phase 2, the encryption process is very similar has WEP process, the differences are: The WEP 24-bit IV field is replaced by the WPA lower 16 bits IV with a dummy byte inserted in the middle and the WEP key is replaced by the per-packet key. The encryption/decryption process is then executed as the same as WEP.

Using TKIP, encryption key is an effective full 128-bit dynamic key instead of just 24-bit dynamic with 40 or 104 bit static key, effectively improving the wireless network security.

3.3.2 MIC (Message Integrity Code)

MIC is a keyed hashing function that protects the data packet integrity. This is an 8-byte value, which is calculated across the entire unencrypted raw data packet before being encrypted and transmitted. The main purpose is to detect any kind of bad intentioned packet modification.

The hashing function used by MIC is a new hashing function specially designed for low processing power devices, such as the hardware in the wireless network interface. Because of this processing power limitation, the protection provided is equivalent to a 20-bit key, which is considered by the current cryptographic standard as a low protection. To compensate for this low protection, WPA resorts to countermeasures to protect the wireless network from data packets modification attack.

When the wireless network detects an altered data packet, it will trigger the countermeasures, which are the following:

© SANS Institute 2005 Author retains full rights.

a) The wireless link of the compromised devices are disabled for 60 seconds, and
b) Every compromised device is forced to request new session keys.

The potential danger of the MIC countermeasures is that it can be used for launching a denied of service attack to the wireless network by forging invalid data packets, making the Access Point enforce the countermeasures continuously.

3.3.3 802.1x Port based Network Access Control

802.1x is a protocol designed to protect a network from the user link point, such as a port of a switch in a wired network, or the access point in a wireless network. We have also seen this protocol implemented in the dynamic WEP.

This protocol divides the network devices into three types:

a) Supplicant is the network client that wants to connect to the network.
b) Authenticator is the link point where the supplicants physically connect to the network. Commonly this device is a network switch or an access point that links the client with the network. In the client authentication process, the main role of this device is requesting and relaying authentication messages between the supplicant and the authentication server.
c) Authentication server is where a client is validated. It could be any authentication server, but commonly a RADIUS server is used.

In an 802.1x-enabled network, any client that wants to initiate a network session must first authenticate before it can actually be able to be connected to the network. An 802.1x switch or access point will only permit EAP (Extensible Authentication Protocol) authentication messages; blocking any other network traffic until the user or computer completes successfully the authentication process.

WPA and 802.11i standard protocol implements this 802.1x protocol to improve the access control security to the wireless network. In addition, this protocol is responsible of generating and delivering the WPA session keys to the supplicant once successfully authenticated.

3.3.4 WPA-PSK (WPA Pre-Shared Key)

WPA offers a special mode where there is no 802.1x authentication infrastructure, permitting the use of a pass phrase as a pre-shared key.

© SANS Institute 2005 Author retains full rights.

Every station may have its own pre-shared key tied to its MAC address, but most of the manufacturers implement only one pre-shared key for the whole wireless network. The configuration of this mode is very similar like WEP, in which a user only needs to introduce a passphrase.

A weakness has already been found on this WPA operation mode. If the pre-shared key is configured with a weak pass phrase, an attacker can capture the authentication messages and then made an offline recovery of the passphrase. Users using WPA-PSK are encouraged to use complex and long passphrase to prevent the passphrase to be cracked.

4. 802.11i

As we mention earlier, WPA is a subset of the new security standard 802.11i (a.k.a. WPA2), meaning that 802.11i includes all WPA capabilities features and more security features. The main difference between 802.11i and WPA is the ability of 802.11i to use state-of-the-art AES (Advanced Encryption Standard) to encrypt the data packets. The AES algorithm is the encryption standard used by U.S government agency[10]. The downside of using AES encryption is that WEP-only capable wireless network interface cannot be software upgraded to support AES. A wireless network that wants to use the 802.11i standard full capabilities may require the replacement of the wireless network devices.

4.1. AES-CCMP (Advanced Encryption Standard – Counter mode CBC MAC Protocol)

The 802.11i standard can use the AES (Advanced Encryption Standard) block cipher to encrypt the data packets, which replaces the WEP's RC4 stream cipher. The AES encryption algorithm is a block cipher, which encrypts the data in blocks of fixed length. For 802.11i, the block size as well as the per-packet key size is 128-bit.

Block ciphers have several mode of operation for splitting data into the fixed size blocks for encrypting and protecting the data. The mode of operation selected by 802.11i is CCMP (Counter mode with Cipher Block Chaining Message Authentication Code). This mode of operation offers counter mode for protecting privacy while Cipher Block Chaining Message Authenticaction Code is used for protecting the data integrity.

In counter mode, each fixed size data block is not encrypted directly instead, a arbitrary value is encrypted and then combined with a logical XOR with a data block. For each successive data block, the arbitrary value is increment by one. The Cipher Block Chaining Message Authentication Code creates a MIC

[10] Wikipedia, "Advanced Encryption Standard"

© SANS Institute 2005 Author retains full rights.

(Message Integrity Code) to protect the data integrity. To generate the MIC each encrypted data block is performed a logical XOR with the result of the previous MIC. The result is then encrypted with AES. The process repeats until all the blocks for a message are processed. In this way, the data of all the blocks are combined in a single 128-bit block.

5. Wireless Networks Tools

In this section, you will find some useful tools for auditing your wireless network. Some of these tools are already mentioned in the body of this document.

5.1. MAC spoofing

Tool	Author	Website
SMAC	KLC, Consulting Inc.	http://www.klcconsulting.net/smac/
MAC Makeup	H & C Works	http://www.gorlani.com/publicprj/macmakeup/macmakeup.asp

5.2. Wireless Analysers

Tool	Author	Website
Kismet Wireless	Kismet Wireless	http://www.kismetwireless.net/
Airtraf	Peter K. Lee	http://airtraf.sourceforge.net/
Netstumbler	Netstumbler	http://www.netstumbler.com

5.3. WEP Cracking Tools

Tool	Author	Website
dwepcrack	dachb0den labs	http://www.dachb0den.com/projects/dwepcrack.html
Airsnort	Airsnort	http://airsnort.shmoo.com/
WEPAttack	Dominik Blunk, Alain Girardet	http://wepattack.sourceforge.net/
WEPCrack	Anton T. Rager	http://wepcrack.sourceforge.net/

© SANS Institute 2005 Author retains full rights.

6. Conclusions

In this document, we described the 802.11 Wireless Network security protocols and mechanism that we can find in nearly any 802.11 device. Not all the security features advertised in the retail boxes of the 802.11 devices are effective; some are very easy to by-passed. Features such like SSID hiding and MAC access control list can be used for limit the resources to attacker, but cannot be trusted as security measure.

The WEP protocol, which was originally designed to protect the 802.11 wireless networks, has several important weaknesses that cannot provide us a trusted security level. Many vendors offer software upgrade to WPA in their 802.11 products line.

Current and future wireless network users are encouraged to use or upgrade their wireless network to the latest security standard released. Currently the IEEE 802.11i is the most recent security standard released that we could use to protect our wireless network; giving us many security improvements, avoiding almost all of the vulnerabilities from the previous security standards. If we could not use the 802.11i standard in our wireless network, other security measures should be taken such as VPN, IPSec, etc.

As we can see, these security protocols and mechanism are getting more and more complex, so getting an idea of what they will do and not do is a good start to protect our Wireless Network.

7. References

Wikipedia: "Wired Equivalent Privacy" September 12, 2004.
URL: http://en.wikipedia.org/wiki/WEP (September 30, 2004)

Everard, Ben; Gorochow, Tom; Stoneman, Graham; Warne, Marc
"Wireless Network Security Issues"
URL: http://www.dcs.warwick.ac.uk/~nikos/cs406/Wirelessw.pdf (September 15, 2004)

Symbol, "Why 'Not Broadcasting the SSID' is not a Form of Security",
March 25, 2003.
URL: http://www.symbol.com/products/wireless/broadcasting_ssid_.html
(September 15, 2004)

Geier, Jim, "802.11 Beacons Revealed", October 31, 2002.
URL: http://www.wi-fiplanet.com/tutorials/article.php/1492071 (August 7, 2004)

© SANS Institute 2005 Author retains full rights.

Trapeze Network, “Enterprise Wireless LAN Security”.
URL:
http://www.trapezenetworks.com/technology/whitepapers/WLANsecurity2.asp
(September 16, 2004)

Geier, Jim, “802.1X Offers Authentication and Key Management”, May 7, 2002.
URL: http://www.wi-fiplanet.com/tutorials/article.php/1041171 (August 7, 2004)

Kismet Wireless Home Page
URL: http://www.kismetwireless.net/ (October 10, 2004)

Aircrack Home Page
URL: http://www.cr0.net:8040/code/network/aircrack (October 10, 2004)

Hulton, David, “Practical Exploitation of RC4 Weaknesses in WEP Environments”, February 22, 2002.
URL: http://www.dachb0den.com/projects/bsd-airtools/wepexp.txt (October 10, 2004)

Anderson, Eric, Wireless Networking, “FreeBSD Handbook”.
URL: http://www.signal42.com/freebsd/network-wireless.html (September 25, 2004)

Wireless LAN Security & Wardriving (802.11).
URL: http://www.wardrive.net/wardriving/tools/ (October 10, 2004)

Linux-Wireless.com
URL: http://www.linux-sec.net/Wireless/Sniffers/ (October 10, 2004)

AirSnort Homepage.
URL: http://airsnort.shmoo.com/ (October 19, 2004)

Pollino, David, Schiffman, Mike, “802.11: Use, Misuse and the Need for a Robust Security Toolkit”, May 2002.
URL: http://www.cansecwest.com/core02/Cansec.pdf (September 25, 2004)

The Unofficial 802.11 Security Web Page, August 12, 2004.
http://www.drizzle.com/~aboba/IEEE/ (October 10, 2004)

Weplab
http://weplab.sourceforge.net/ (October 10, 2004)

(In)Security of the WEP algorithm
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (October 10, 2004)

© SANS Institute 2005 Author retains full rights.

Walker, Jesse R., “Unsafe at any key size; An analysis of the WEP encapsulation”, Oct 27, 2000.
URL: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (August 20, 2004)

Griffith, Eric, “802.11i Security Specification Finalized”, June 25, 2004.
URL: http://www.wi-fiplanet.com/news/article.php/3373441 (October 10, 2004)

Wikipedia, “Advanced Encryption Standard”, October 15, 2004.
URL: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard (October 22, 2004)

Wikipedia, “Block cipher modes of operation”, October 19, 2004.
URL: http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation (October 22, 2003)

© SANS Institute 2005, Author retains full rights.

Last Updated: September 3rd, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced