



# 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 permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

# AN OVERVIEW OF WIRELESS SECURITY ISSUES

Kevin Tyrrell

GSEC Version 1.4b

## ABSTRACT

Wireless networking technology is quickly changing the way networked computers communicate. The convenience offered by the ability to connect to networks using mobile computing devices has also introduced many security issues that do not exist in the wired world. The security measures we have relied on in the past to secure our networks are now obsolete with this new technology.

This paper introduces the 802.11 standard and the security issues surrounding it. How to discover and access Wireless LANs (WLANs) is discussed and a checklist that can be used in securing them is presented. Finally, security enhancements to the 802.11 standard such as VPNs, centralized authentication and dynamic key distribution are discussed.

WLANs are indeed very useful, but the encryption and authentication methods specified in the 802.11 standard are flawed, leading to serious security issues. Applying the recommendations in the WLAN security checklist and deploying security enhancements such as VPNs, centralized authentication and dynamic key distribution to the WLAN architecture will help you overcome many of the flaws in the 802.11 standard.

## 802.11 BACKGROUND

The 802.11 standard is a group of specifications for WLANs created by the Institute of Electrical and Electronics Engineers Inc. (IEEE). The first WLAN standard was adopted in 1997. This standard defined the Media Access Control (MAC) and Physical (PHY) layers for a wireless LAN.

### *Media Access Control Layer (MAC)*

The Media Access Control Layer provides three services:

- Reliable data delivery from the physical wireless media to the upper layers of the OSI reference model.
- A controlled access method from the upper layers to the wireless media. This method is called Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA). CSMA/CA is similar to the collision detection access method used in 802.3 Ethernet LANs.
- The authentication services and the Wireless Equivalent Privacy (WEP), which is the encryption service for data transmitted on the WLAN.

### *Physical Layer (PHY)*

The physical layer is the interface between the MAC and the wireless media where frames are transmitted and received. The physical layer also provides three functions:

- An interface to exchange frames with the upper MAC layer for transmission and reception of data.

- Signal carrier and spread spectrum modulation to transmit data frames over the media.
- A carrier sense indication back to the MAC to verify activity on the media.

802.11 provides two different physical definitions: Frequency Hopping Spread Spectrum (FHSS), and Direct Sequence Spread Spectrum (DSSS). Both support 1 and 2 Mbps data rates. The 802.11b extension defines 5.5 Mbps and 11 Mbps data rates, in addition to the original 1 and 2 Mbps rates.

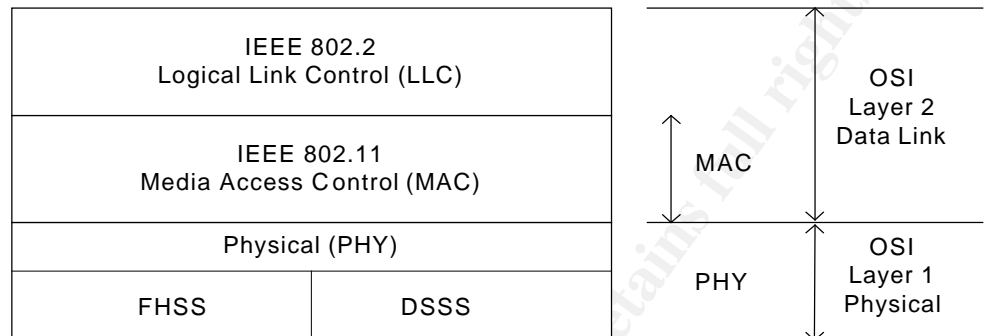


Figure 1. IEEE 802.11 Standards and the OSI Reference Model

802.11 networks operate in one of two modes, ad-hoc, also known as Independent Basic Service Set (IBSS) and infrastructure mode, which is also known as Basic Service Set (BSS).

#### *Ad-hoc Mode*

In ad-hoc mode, stations communicate directly with each other. An ad-hoc network is formed “on the fly”, when mobile devices within proximity of each other have a need to communicate and no pre-existing network infrastructure is in place near their location. An ad-hoc has no connection to the “outside world”.

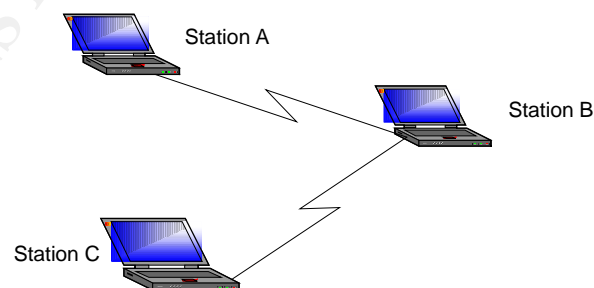


Figure 2. An Ad-hoc Network

### *Infrastructure Mode*

In infrastructure mode, the stations communicate only with a central access point. The access point acts as an Ethernet bridge between the wireless media and wired network the access point is connected to.

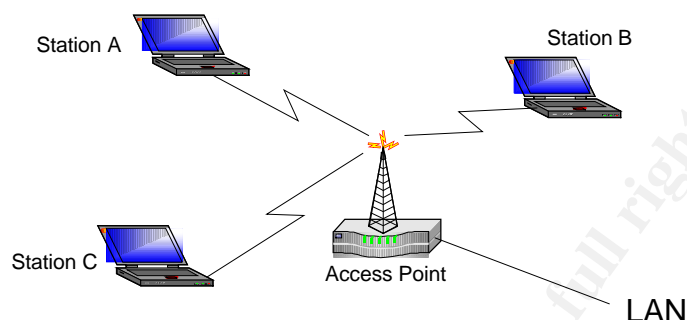


Figure 3. An Infrastructure Network

### *WEP (Wireless Equivalent Privacy)*

“WEP is an algorithm that’s used to protect wireless communications from eavesdropping and modification. A secondary function of WEP is to prevent unauthorized access to a wireless network. It relies on a secret key that is shared between a wireless station and an access point. The secret key is used to encrypt packets before they are transmitted and an integrity check is used to ensure the packets are not modified in transit. The 802.11 standard does not state how the shared key is established. In practice, most installations use a key that is shared between all stations and access points.” [3]

WEP uses the RC4 encryption algorithm. “RC4 is a stream cipher designed by (Ron) Rivest for RSA Data Security (now RSA Security). It is a variable key-size stream cipher with byte-oriented operations. The algorithm is based on the use of a random permutation. Analysis shows that the period of the cipher is overwhelmingly likely to be greater than 10<sup>100</sup>. Independent analysts have scrutinized the algorithm and it is considered secure.” [1]

### *Authentication and Association*

Before the wireless clients and access points can communicate they must establish an association. Once the association is established the two can exchange data. In infrastructure mode the client associates with the access point. The association process is a two-step process involving three states:

- Unauthenticated and Unassociated
- Authenticated and Unassociated
- Authenticated and Associated

The two parties exchange messages called authentication management frames while transitioning between the states.

All access points transmit a beacon management frame at fixed intervals. When attempting to associate with an access point and become a member of a BSS, a client listens for beacon frames from the access point. Some clients may also send out a probe management frame. This frame is used to find an access point with a specific Service Set Identifier (SSID).

After the client has found an access point, it is in the first state. It must now authenticate with the access point to move to the second state. There are three types of authentication – open system, shared key and MAC address based access control lists (ACLs).

#### *Open System Authentication*

Open system authentication is the default authentication protocol for 802.11. Open system authentication authenticates anyone who requests authentication. Essentially, it provides a NULL authentication process. The authentication management frames used by this protocol are sent in clear text even when WEP is enabled.

#### *Shared Key Authentication*

Shared key authentication uses a standard challenge/response mechanism along with a shared secret key to provide authentication. The client attempting to authenticate sends an authentication request management frame to the access point indicating it wishes to use shared key authentication. The access point responds by sending an authentication management frame containing 128 octets of challenge text to the client. The challenge text is generated by the WEP pseudo-random number generator using a shared secret and a random initialization vector (IV).

When the client receives the management frame from the access point it copies the contents of the challenge text into a new management frame. This new management frame is then encrypted with WEP using the shared secret and a new IV selected by the client. The encrypted management frame is then sent to the access point. The access point decrypts the received frame, and verifies the text matches what it sent in the first message. If the text matches, then the authentication is considered successful.

If the authentication is successful the process is repeated with the access point acting as the initiator. This second authentication assures mutual authentication.

After successful authentication, the client moves into the second state, authenticated and unassociated. Moving from the second state to the third and final state, authenticated and associated, involves the client sending an association frame and the access point responding with an association response frame.

After following the process described in the previous paragraph, the client becomes a peer on the wireless network, and can transmit data frames on the network. [6]

#### *Access Control Lists*

The third method of authentication relies on access control lists based on the MAC address of the client. Access points can limit which clients can access the network by using a list of authorized MAC addresses. If a client's MAC address is in the list then the client is allowed access to the network. If the MAC address is not listed the client is denied access. This method is the least secure of all because it is easy to spoof the

MAC address of a NIC. Maintaining the list of authorized MAC addresses can be time consuming and is also prone to error.

## WIRELESS SECURITY ISSUES

Any WLAN client within the service area of an access point can access data being transmitted to or from the access point. Radio waves are not stopped by obstructions such as walls, ceilings or floors, thus the transmitted data may reach unintended recipients even outside the building where the access point is installed. Without stringent security measures in place, installing a WLAN can be equivalent to placing Ethernet ports on the outside of your building, accessible to anyone interested in plugging into your network.

Stream ciphers such as WEP operate by expanding a relatively short key into an infinite pseudo-random key stream. This key stream is XORed with the plaintext of the data by the sender to generate the ciphertext. The recipient has a copy of the same key and uses it to generate an identical key stream. XORing this key stream with the ciphertext results in the original plaintext.

This mode of operation makes stream ciphers vulnerable to several attacks. If an attacker flips a bit in the ciphertext, then upon decryption, the corresponding bit in the plaintext will be flipped. Also, if an eavesdropper intercepts two ciphertexts encrypted with the same key stream, it is possible to obtain the XOR of the two plaintexts. Knowledge of this XOR can enable statistical attacks to recover the plaintexts. The statistical attacks become increasingly practical, as more ciphertexts that use the same key stream are known. Once one of the plaintexts becomes known, it is trivial to recover all of the others. [3]

To defend against the first type of attack an integrity check field is included in the packet. An initialization vector (IV) is used to avoid encrypting multiple ciphertexts with the same key stream. However both of these defenses have been poorly implemented.

The integrity check field is a CRC-32 checksum, and is part of the encrypted portion of the packet. The CRC-32 checksum is linear, which means that it is possible to obtain the bit difference of two CRCs based on the bit difference of the message used to compute them. What this means is if you change bit  $n$  in the message you can determine which bits in the CRC must be changed to produce a correct checksum for the modified message. Because changed bits carry through after the RC4 decryption, this allows the attacker to change arbitrary bits in the ciphertext and adjust the checksum so that the resulting message appears valid.

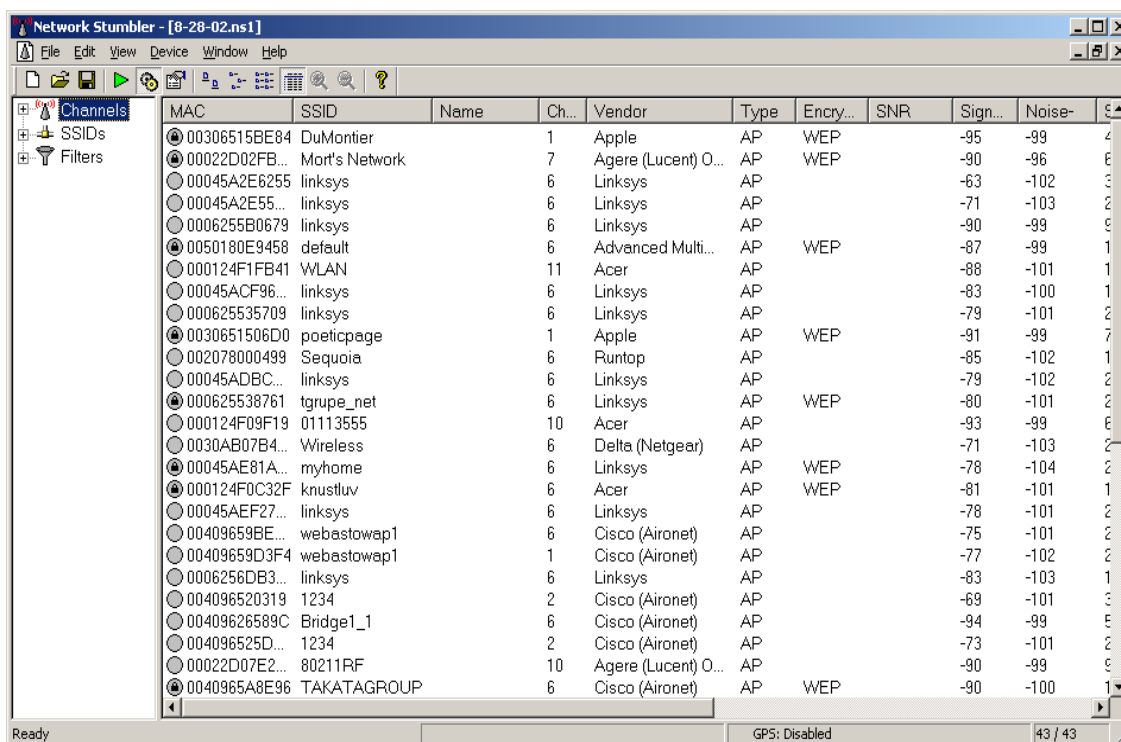
The initialization vector in WEP is a 24-bit field, which is sent in the cleartext portion of the message. This small number of initialization vectors assures the eventual reuse of the same key stream. A busy access point transmitting 1,500 byte packets at 11Mbps will exhaust the IV space in

$$1,500 * 8 / (11 * 10^6) * 2^{24} \text{ seconds}$$

or about 5 hours. This means in a little over 5 hours an attacker can collect at least two ciphertexts that have been encrypted with the same key stream and perform statistical attacks to recover the plaintext.

## WLAN DISCOVERY

Finding 802.11 WLANs is relatively easy. All that's needed is a wireless network interface card (NIC) running in promiscuous mode and some WLAN scanning software. There are a number of WLAN scanners available for different operating systems, the most popular ones for the Windows platform being NetStumbler and Aerosol. NetStumbler works with wireless NICs based on the Hermes chipset, Aerosol works with wireless NICs that use the PRISM2 chipset.



The screenshot shows the NetStumbler application window with the title bar 'Network Stumbler - [8-28-02.ns1]'. The interface includes a menu bar (File, Edit, View, Device, Window, Help) and a toolbar. On the left, there are expandable sections for 'Channels', 'SSIDs', and 'Filters'. The main area displays a table of discovered wireless networks. The table has columns for MAC, SSID, Name, Ch... (Channel), Vendor, Type, Encry... (Encryption), SNR, Sign... (Signal), Noise..., and a status column. The status column contains icons: a signal strength indicator (three bars) and a lock icon. The status bar at the bottom shows 'Ready', 'GPS: Disabled', and '43 / 43'.

MAC	SSID	Name	Ch...	Vendor	Type	Encry...	SNR	Sign...	Noise...	Status
00306515BE84	DuMontier		1	Apple	AP	WEP	-95	-99	4	Signal strength 3 bars, Lock
00022D02FB...	Mort's Network		7	Agere (Lucent) O...	AP	WEP	-90	-96	6	Signal strength 3 bars, Lock
00045A2E6255	linksys		6	Linksys	AP		-63	-102	3	Signal strength 3 bars, Lock
00045A2E55...	linksys		6	Linksys	AP		-71	-103	2	Signal strength 3 bars, Lock
0006255B0679	linksys		6	Linksys	AP		-90	-99	9	Signal strength 3 bars, Lock
0050180E9458	default		6	Advanced Multi...	AP	WEP	-87	-99	1	Signal strength 3 bars, Lock
000124F1FB41	WLAN		11	Acer	AP		-88	-101	1	Signal strength 3 bars, Lock
00045ACF96...	linksys		6	Linksys	AP		-83	-100	1	Signal strength 3 bars, Lock
000625535709	linksys		6	Linksys	AP		-79	-101	2	Signal strength 3 bars, Lock
0030651506D0	poeticpage		1	Apple	AP	WEP	-91	-99	7	Signal strength 3 bars, Lock
002078000499	Sequoia		6	Runtop	AP		-85	-102	1	Signal strength 3 bars, Lock
00045ADBC...	linksys		6	Linksys	AP		-79	-102	2	Signal strength 3 bars, Lock
000625538761	tgrupe_net		6	Linksys	AP	WEP	-80	-101	2	Signal strength 3 bars, Lock
000124F09F19	01113555		10	Acer	AP		-93	-99	6	Signal strength 3 bars, Lock
0030AB07B4...	Wireless		6	Delta (Netgear)	AP		-71	-103	2	Signal strength 3 bars, Lock
00045AE81A...	myhome		6	Linksys	AP	WEP	-78	-104	2	Signal strength 3 bars, Lock
000124F0C32F	knustuv		6	Acer	AP	WEP	-81	-101	1	Signal strength 3 bars, Lock
00045AEF27...	linksys		6	Linksys	AP		-78	-101	2	Signal strength 3 bars, Lock
00409659BE...	webastowap1		6	Cisco (Aironet)	AP		-75	-101	2	Signal strength 3 bars, Lock
00409659D3F4	webastowap1		1	Cisco (Aironet)	AP		-77	-102	2	Signal strength 3 bars, Lock
0006256DB3...	linksys		6	Linksys	AP		-83	-103	1	Signal strength 3 bars, Lock
004096520319	1234		2	Cisco (Aironet)	AP		-69	-101	3	Signal strength 3 bars, Lock
00409626589C	Bridge1_1		6	Cisco (Aironet)	AP		-94	-99	5	Signal strength 3 bars, Lock
004096525D...	1234		2	Cisco (Aironet)	AP		-73	-101	2	Signal strength 3 bars, Lock
00022D07E2...	80211RF		10	Agere (Lucent) O...	AP		-90	-99	9	Signal strength 3 bars, Lock
0040965A8E96	TAKATAGROUP		6	Cisco (Aironet)	AP	WEP	-90	-100	1	Signal strength 3 bars, Lock

Figure 4. The NetStumbler Capture Screen

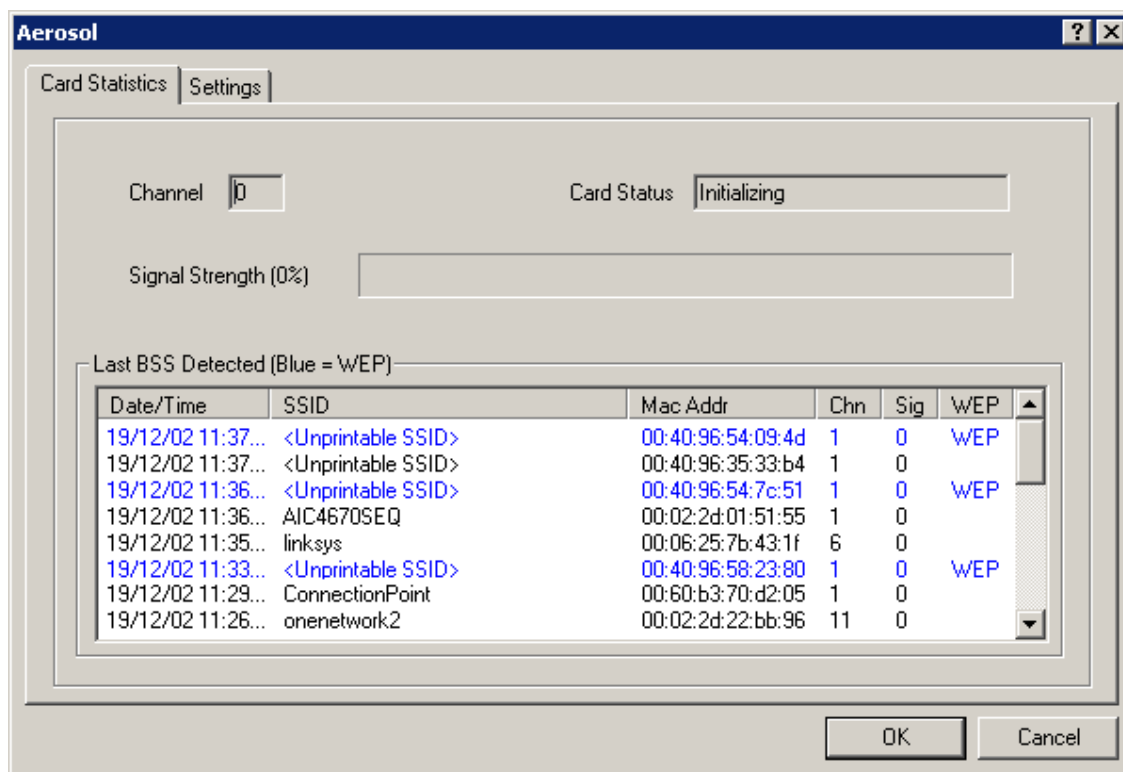


Figure 5. Aerosol In Action

To locate each other, wireless clients and access points send out broadcasts and beacons. Access point beacons are sent out at regular intervals, they are signals that enable the wireless client to find the access point and configure the appropriate communications settings. The beacon announces the SSID and the channel the access point is using.

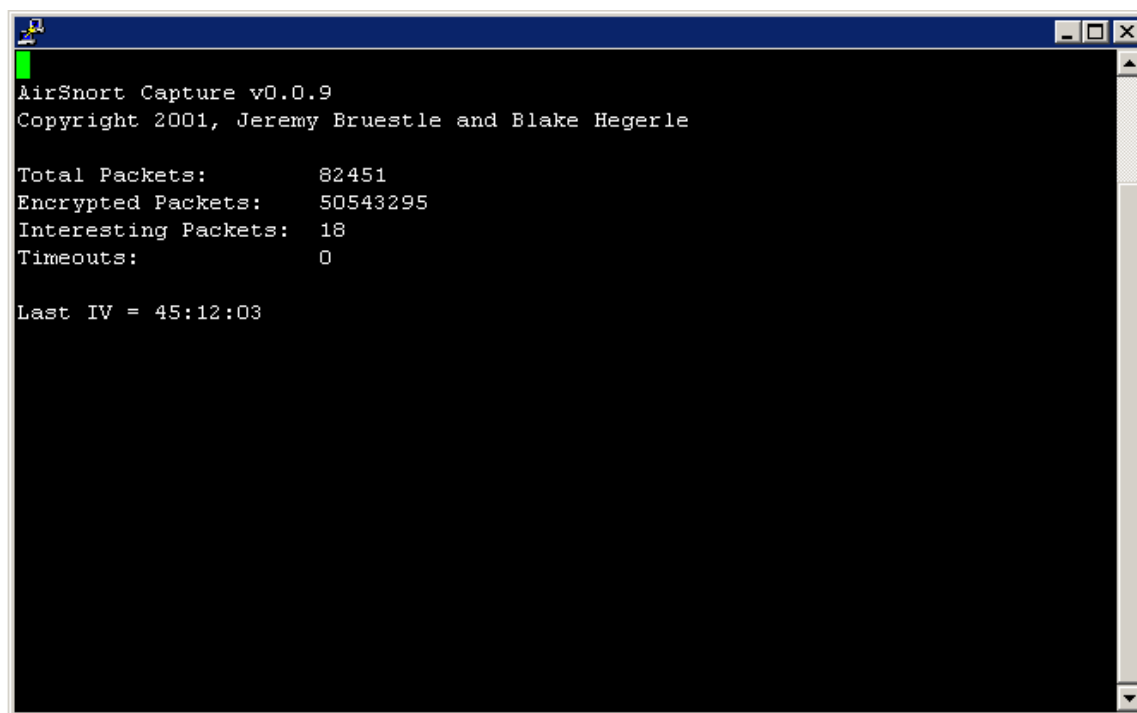
This type of system makes finding and connecting to WLANs convenient, but it is a major security weakness. On some access points the beacon announcement can be turned off. However this doesn't stop most WLAN scanners like NetStumbler and Aerosol from finding WLANs, these types of scanners cycle through all possible channels, sending out a continuous stream of broadcast packets. A nearby access point will respond to the broadcast packets on the channel it is configured to use, making itself known to the scanner, even if beacons are disabled. This active probing feature of NetStumbler and Aerosol also makes it easy for an alert administrator to detect when they are being used to probe his network.

## GAINING ACCESS TO WLANS

### Cracking WEP Keys

Many WEP attack tools have become available since the release of white papers such as "Using the Fluhrer, Mantin and Shamir Attack to Break WEP", by Adam Stubblefield, John Ioannidis and Avril D. Rubin. One of the most popular attack tools is AirSnort.

AirSnort is a Linux based tool that exploits the vulnerabilities discussed in the Stubblefield, Ioannidis and Rubin paper. It requires a wireless NIC based on the Prism2 chipset, capable of running in promiscuous mode and a WLAN scanner to find a target WLAN. AirSnort is comprised of two applications – capture and crack. Once the NIC is in promiscuous mode and an access point has been located, the capture application can be launched.



```
AirSnort Capture v0.0.9
Copyright 2001, Jeremy Bruestle and Blake Hegerle

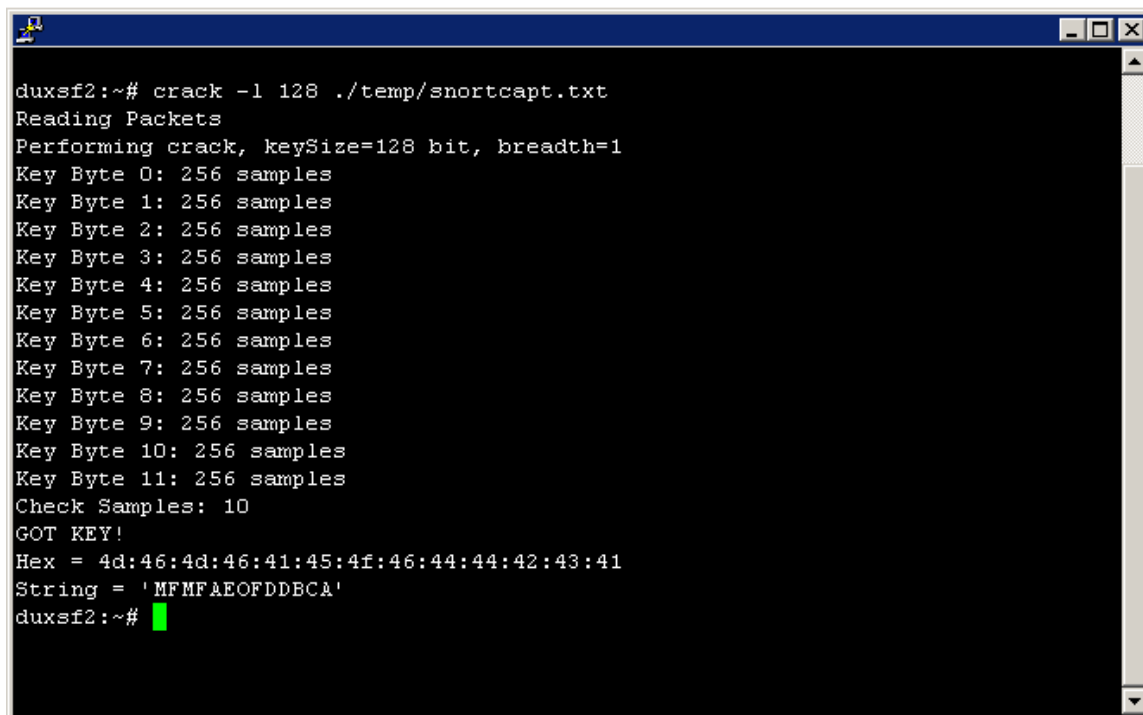
Total Packets:      82451
Encrypted Packets:  50543295
Interesting Packets: 18
Timeouts:           0

Last IV = 45:12:03
```

Figure 6. AirSnort Capture Utility

As the capture utility runs it displays the number of packets with weak keys it has captured and writes them to a file. These packets are called “interesting packets”. Once a large number of interesting packets have been captured, you can attempt to crack the WEP key by opening another console window and launching the crack application, leaving the capture application running. When enough interesting packets are captured, the WEP key will be returned.

© SANS Institute

A screenshot of a terminal window titled "AirSnort Crack Utility". The window has a blue title bar with standard Windows window controls. The terminal background is black with white text. The text shows a command prompt session where the user runs a crack command. The output lists 12 key bytes, each with 256 samples, followed by a check of 10 samples and the successful retrieval of a key. The key is displayed in both hexadecimal and string format. The prompt returns to the user.

```
duxsf2:~# crack -l 128 ./temp/snortcapt.txt
Reading Packets
Performing crack, keySize=128 bit, breadth=1
Key Byte 0: 256 samples
Key Byte 1: 256 samples
Key Byte 2: 256 samples
Key Byte 3: 256 samples
Key Byte 4: 256 samples
Key Byte 5: 256 samples
Key Byte 6: 256 samples
Key Byte 7: 256 samples
Key Byte 8: 256 samples
Key Byte 9: 256 samples
Key Byte 10: 256 samples
Key Byte 11: 256 samples
Check Samples: 10
GOT KEY!
Hex = 4d:46:4d:46:41:45:4f:46:44:44:42:43:41
String = 'MFMF&EOFDDBCA'
duxsf2:~#
```

Figure 7. AirSnort Crack Utility

## Sniffing WLAN Traffic

After the WEP key has been obtained, viewing the WLAN traffic requires the use of a sniffer that works with 802.11b network cards.

There are three requirements that must be met before you can view the traffic.

- You must know the operating channel. This can be obtained from scanning tools such as Aerosol or NetStumbler.
- The SSID must be known. This can also be obtained from scanning tools such as Aerosol or NetStumbler.
- The WLAN NIC must be operating in promiscuous mode.

Once the wireless NIC is properly configured the sniffer can be started. It should begin to record the wireless traffic. The Windows version of Ethereal works well with Prism2 chipset based NICs

## SECURING WIRELESS LANS

### Policies and Procedures

As part of an overall security policy, organizations should have a complete wireless network policy. "This wireless policy should, at a minimum, disallow the connection of non-IT supported access points into the network. On the procedures side, the IT department needs to conduct regular scans of its office space to check for rogue [access points]. This should include both physical searches and wireless scans." [4]

## **WLAN Security Checklist**

### **Don't Rely On WEP For Encryption**

WEP is insecure. It is not designed to provide a complete security solution for wireless networks, but only a level of privacy equivalent to wired LANS. In addition to WEP consider using an end-to-end encryption mechanism such as an IPSec VPN.

### **Segregate Wireless and Wired Networks**

Since WLANs are inherently insecure you should not allow WLAN traffic to coexist with wired LAN traffic in a trusted environment. Firewalls or screening routers should be placed between the networks and authentication between devices on the separate networks should be used.

### **Don't Use A Descriptive Name For The SSID Or The Access Point**

The SSID and the access point name are not encrypted in the header of 802.11 packets. WLAN scanners will detect these values and when you provide these descriptions you make it easier for an attacker to identify the source of the signal.

### **Hard Code The MAC Addresses That Can Connect To The Access Point**

Determine if the access point has the ability to maintain a list of the MAC addresses of the network cards allowed to connect to the access point. Using this feature provides some additional security. Attackers can still identify the access point and sniff the traffic, but they will not be able to connect to the network unless they spoof a MAC address on the list. There is administrative overhead in maintaining the list, which can be time consuming on a large network.

### **Change Encryption Keys Often**

To stop an attacker from compromising the WEP keys, they have to be changed every few minutes on a busy network, which is impractical. However, changing the keys periodically will make sure a compromised network does not stay compromised indefinitely.

### **Disable Beacon Packets**

Determine if the access point has the ability to disable beacon packets. The access point will then require the wireless NICs to use the same SSID as the access point before the access point will respond to traffic. Disabling this feature will prevent attackers from discovering access points using WLAN scanning tools that passively collect data instead of actively sending out broadcast packets.

### **Locate Access Points In A Central Location**

When architecting a wireless network make sure the access points are located in a central location within a building. This will help ensure the signals are not broadcast outside the building.

### **Change The Default Passwords And IP Addresses**

Almost all access points use a built in web server for administrative tasks. Anyone on a wireless or wired network who knows the IP address of the access point can connect to

the administration console by pointing a web browser at the IP address of the access point. The default IP address and authentication credentials can usually be found in installation and configuration instructions, which can be downloaded from the manufacturer's web site. The manufacturer of the access point can be identified with scanning tools such as NetStumbler by comparing the broadcast MAC address to listings published by the IEEE.

### Avoid Products That Use Weak WEP Keys

More and more vendors are providing products that do not use IVs that result in weak WEP keys. Some are also providing firmware upgrades to existing products that eliminate the use of weak keys. For these upgrades to be effective all wireless products must be upgraded, because the both clients and access points determine the IVs that are used.

### Do Not Use DHCP On WLANS

An attacker needs to obtain a valid IP address and subnet mask in order to access a network through a WLAN connection. If an access point is configured to use DHCP it will supply a valid address and subnet mask to any wireless device that successfully authenticates and associates with the access point. Using statically assigned IP addresses will not completely foil a determined attacker though. The attacker can passively sniff wireless traffic and get a good idea of what IP address ranges are in use, which narrows his search for an unused address. Not using DHCP will not completely eliminate the risk but it may be enough to deter a less experienced or determined attacker.

### Guard Against Unapproved Access Points

It's common in larger organizations to find users who have installed their own wireless networks to work "below the radar" of the IT staff. The networks may be used to collaborate and share information between teams or to get around firewalls to gain Internet access. The people setting up these networks rarely take security into consideration. The networks can easily be used by outsiders to gain access to your network.

## **802.11x Security Enhancements**

### *IPSec*

IPSec is a framework of open standards for ensuring secure private communications over IP networks. IPSec VPNs use the protocols defined in IPSec to ensure confidentiality, integrity and authenticity of data transmissions across public networks.

When an IPSec VPN is used in a WLAN environment, IPSec clients must be installed on each device connected to the wireless network. Users are required to establish an IPSec tunnel to route any traffic to the wired network. Filters need to be put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway. IPSec provides for confidentiality of the IP traffic through the use of the Triple

DES (3DES) encryption algorithm, which encrypts the data three times with up to three different keys.

### *EAP*

An alternative security approach introduced jointly to the IEEE by Cisco Systems, Microsoft and others uses the Extensible Authentication Protocol (EAP) to provide centralized authentication and dynamic key distribution. EAP lets wireless clients communicate through an access point with a RADIUS authentication server. Communication between the access point and the RADIUS server is via a secure channel. This eliminates "man-in-the-middle attacks" by rogue access points and RADIUS servers.

When EAP is implemented a wireless client that associates with an access point will not gain access to the network until the user performs a network logon. When the user enters his credentials the client and the RADIUS server perform a mutual authentication instead of one-way authentication, with the client authenticates by the supplied user name and password. The RADIUS server and client derive a client specific WEP key that will be used by the client only during the current logon session.

### *LEAP*

In November 2000, Cisco systems introduced LEAP authentication. This authentication algorithm is an extension of EAP, it provides both the mutual user-based authentication described above and centralized key management and distribution.

The additional key features of LEAP include:

- Secure key derivation

The original shared secret secure key derivation is used to construct responses to the mutual challenges. It undergoes irreversible one-way hashes that make password-replay attacks impossible. The hash values sent over the wire are useful for one-time use only at the start of the authentication process.

- Dynamic WEP keys

One of the biggest security exposures in WLANs is primarily due to static WEP and the tremendous administrative burden it imposes. With LEAP, session keys are unique to the users and are not shared among them. Also, with LEAP authentication, the broadcast WEP key is encrypted using the session key before being delivered to the end client. By having a session key unique to the user, and by tying it to the network logon required by EAP, the solution also eliminates vulnerabilities due to stolen or lost client cards or devices.

- Reauthentication policies

LEAP also allows administrators to set policies for reauthentication at the back-end RADIUS server. This forces users to reauthenticate more often and get new session keys. This can minimize attacks where traffic is injected during the session.

- Initialization Vector changes

LEAP changes the Initialization Vector on a per-packet basis so that attackers can find no predetermined sequence to exploit. This makes it difficult to create table-based attacks based on the knowledge of the IVs seen on the wireless network.

© SANS Institute 2003, Author retains full rights.

## REFERENCES

- [1] RSA Security. "What is RC4?." N/A  
URL: <http://www.rsasecurity.com/rsalabs/faq/3-6-3.html> (December 17, 2002).
- [2] Arbaugh, William, Narendar Shankar and Justin Wan. "Your 802.11 Wireless Network Has No Clothes." March 30, 2001.  
URL: <http://www.cs.umd.edu/~waa/wireless.pdf> (December 17, 2002).
- [3] Borisov, Nikita, Ian Goldberg and David Wagner. "Security of the WEP Algorithm." N/A  
URL: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html> (December 17, 2002).
- [4] Convery, Sea and Darrin Miller. "Wireless LAN Security in Depth." July 16, 2002.  
URL: [http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl\\_wp.htm](http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm) (December 17, 2002).
- [5] Mishra, Arunesh and William Arbugh. "An Initial Security Analysis of the IEEE 802.1X Standard." February 06, 2002.  
URL: <http://www.cs.umd.edu/~waa/1x.pdf> (December 17, 2002).
- [6] Thodupunuri, Sampath. "A Security Analysis of the Wireless Networks." N/A.  
URL: <http://islab.oregonstate.edu/koc/ece478/proj/2002RP/T.pdf> (December 17, 2002).
- [7] Stubblefield, Adam, John Ioannidis and Avril D. Rubin. "Using the Fluhrer, Mantin and Shamir Attack to Break WEP." August 02, 2001.  
URL: [http://www.cs.rice.edu/~astubble/wep/wep\\_attack.pdf](http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf) (December 17, 2002).
- [8] Cisco Systems Inc. "Cisco Aironet Wireless LAN Security Overview." August 09, 2002.  
URL: [http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w\\_ov.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm) (December 17, 2002).
- [9] Cisco Systems Inc. "Product Bulletin No. 1515 - Cisco Wireless LAN Security Bulletin." August 22, 2002.  
URL: [http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm) (December 17, 2002).
- [10] Sutton, Michael. "Hacking the Invisible Network." July 10, 2002.  
URL: <https://ialert.iddefense.com/idcontent/2002/papers/Wireless.pdf> (December 17, 2002).