Global Information Assurance Certification Paper

Well treat your Wi-Fi Network Security

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1
Research on Topics
in Information Security

Submitted by : Thang LE BA , December 07, 2004
Location : SANS Conference - LONDON June, 2004.

ABSTRACT

WI-FI (**W**ireless **F**idelity) is getting more and more popular, and in the meantime the costs of implementing WI-FI have dropped. We use it at home and also at work. But security concerns are not the same.

How can we secure confidential or private data? How can we ensure their integrity?

This document has dual purposes : point out the inherent risks when setting up a (**WLAN**s) (**W**ireless **L**ocal **A**rea **N**etwork) and provide the technical means commonly used, highlighting their effectiveness and also weakness. An overview of enhanced technology available at the present time or in the close future will be considered.

Table of Contents

List of Figures

INTRODUCTION

A WLAN is a local area wireless network, using the radio waves and communicating via the 2.4 GHz or 5 GHz band.

The initial 802.11 specification is available in different rates and frequency modulation.

IEEE (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers) is a worldwide association of technical professional, with an extensive range of activities.
Their members deliver specifications and standards to ensure the interoperability of software and hardware on different machines from different vendors.

The IEEE 802.11a (1999) using the 5 GHz frequency band, operate at a theoretical rate of 54 Mbps but the range from 50 m to 300 m, depends more on the obstacles.

The IEEE 802.11b (1999) use 2.4 GHz frequency band with a theoretical data rate of 11 Mbps and a range from 50 m to 300 m.

The IEEE 802.11g (2004) operate at a theoretical rate of 54 Mbps, with a range from 50 m to 300 m, use the same frequency as 802.11b.

The new IEEE 802.11 (2004) “Super G” operate at a theoretical rate of 108 Mbps, may not work with all equipment.

The 802.11 standard includes encryption, **WEP** (**W**ired **E**quivalent **P**rivacy) to secure data sent. But despite this, data can be intercepted by nearby users. The reason is that most of WI-FI access points users leave the default built-in settings as if security is not a personal decision.

In fact, it is. It depends on the type and value of data and environment. Enterprise network require a higher level of security than a home user.
Knowing the risk of an attack by hackers, network administrators must use the appropriate tools to defeat every attempt of intrusion. This supposes that they are aware of the techniques and mechanisms used by snoopers.

DIFFERENT TYPES OF ATTACKS

There are two types of attacks : **passive** and **active**

War driving

War driving is a **passive** way of attacking : driving a car and using laptop equipped with WI-FI **NIC** (**N**etwork **I**nterface **C**ard) to locate and map all access points (**A.P**) by drawing distinctive signs on the buildings or pavements.

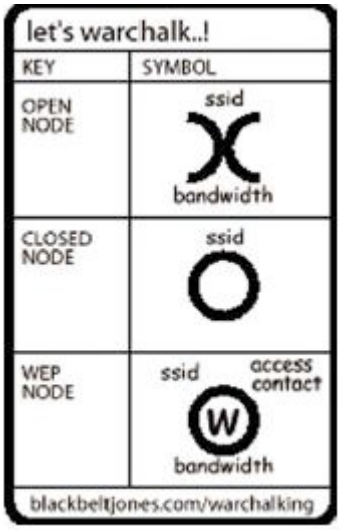


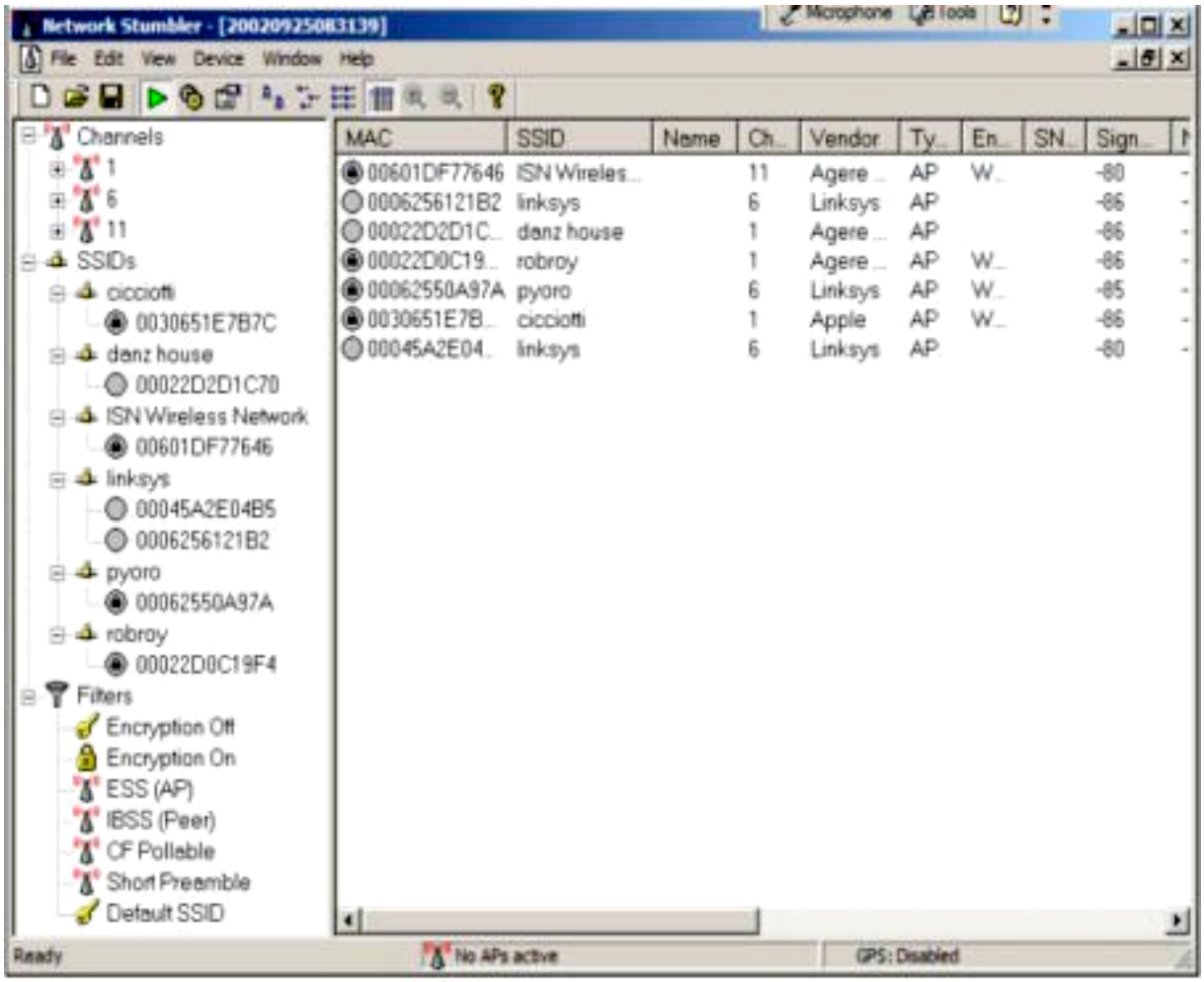
Figure B-1: Warchalking

LINKSYS wireless-G broadband router guide

An A.P indicates its presence by broadcasting its **SSID** (**S**ervice **S**et **I**dentifier) which is your network name and therefore can be detected, using tools as Netstumbler (Windows) or CISMET (Linux). These tools monitor the signal strength and can tell if a network is unencrypted.
Connected to it the war driver can now search for information as passwords or credit card numbers sent out to the internet.

The following Netstumbler tool session displays information such as the SSID (some are the default, which are not recommended), the channels used, the type of encryption implemented…

All these information provide a clue to the hacker and make his job easier.



Discovering Wireless LANs Using Netstumbler
http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html

How to protect against ?

Type an IP address into your browser such as 192.168.0.1
and check through your router configuration utility that :

SSID is not broadcasting (should be in disabled status) but SSID can be guessed if default is used).

Password must not be the default and must be changed.

Wireless communications must be encrypted using WEP encryption but it can be bypassed by AIRSNORT software tool.

Access to the router is restricted using and specifying your own **MAC** (**M**edia **A**ccess **C**ontrol) address.

Shared files must be protected by a password.

Those steps can help you protect your network against hackers, putting them off smuggling into your computer because they will spend much more time to do it.

After gathering enough information from the passive attack, the hacker can launch an active one against the network.

DOS (**D**enial **O**f **S**ervice) is an **active** attack . A mischievous person, by setting up and generating a high power signal to produce **RF** (**R**adio **F**requency) interference, or sending more traffic to a network than data buffers can support, so to overflow them, users or organisations are deprived of the services of a resource they would normally expect to have.

It is a security breach and does not result in the theft of information but the temporary loss of network connectivity or services such as e-mail, deprive concerned organisations a lot of time and money.

A known DOS attack based on an overflow of data buffers is sending e-mail with 256 character file name attachments.

ARP poisoning

ARP is part of Denial of Service, with the aim of providing a fake MAC address and causing a massive attack to quickly overload the network.

ARP (**A**ddress **R**esolution **P**rotocol) , also part of TCP/IP protocol plays a preponderant role in retrieving or picking up the MAC address and setting up a correlation table which contents logical and physical addresses .

Because fake MAC address will never be found in this table, persistent ARP << ARP who has>> requests can fill up the correlation table in next to no time at every update and lead to many misfunctions such as having your network disconnected.

How to protect against ?

Keep systems patched and configured properly.

Deny invalid source IP addresses (spoofed source IP) which are not assigned to your site and only allow packets to be sent with valid ones by filtering at routers and firewalls.
Spoofed source IP is used to make tracing and stopping DOS attack difficult.

Man in the middle attack

Someone nearby can connect to your wireless network and use Windows and collect data from your shared files or documents.

A Hacker monitors frame transmissions, and learns about the IP address, SSID of the network, and now he is able to program a rogue radio **NIC** (**N**etwork **I**nterface **C**ard) to mime a legitimate one and that way, steals your session.

He can intercept legitimate keys exchanged during the **SSL** (**S**ecure **S**ockets **L**ayer) handshake, substitute his own and alter messages sent between two parties without letting them know. He acts as the man in the middle, receiving and sending "packets" on their behalf.

In cryptography, this kind of attack is one of the main weaknesses of public key which uses two keys : one key is kept private and the other is made public.
The message is encrypted with the addressee's public key, the addressee can use the private key to decrypt it.
If a successful attack on a certification authority occurred, public key would be vulnerable to impersonation, it means that the compromised public key can be bound to another user.

How to protect against ?

Set up static ARP address for the gateway.

(SSL) Authentication at both sides of a connection is advisable.

Certificates on the server must be validated by users.

Basic security process

How to secure ?

There are standard 802.11 built-in internal solutions on any WI-FI equipments and two operating mode : infrastructure and ad-hoc.

Infrastructure : when connected to an A.P (**A**ccess **P**oint) or router.

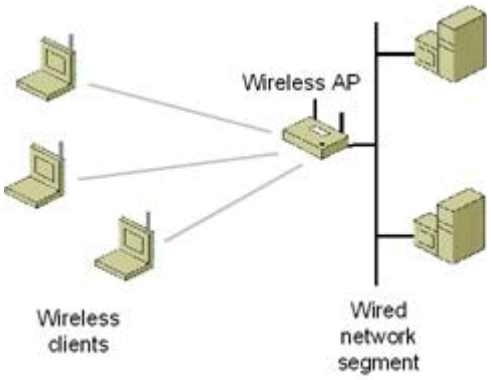


Figure 1 Infrastructure mode wireless network

Ad-hoc : creation of a network between several workstations.

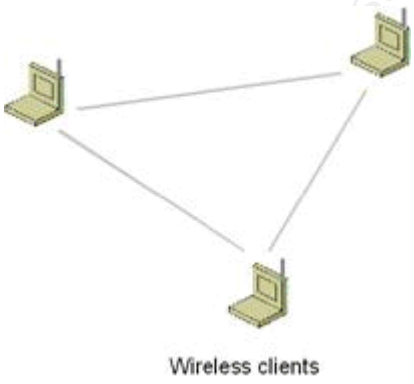


Figure 2 Ad hoc mode wireless network

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

Change factory default settings

Some of them need to be changed such as：

Do not broadcast your SSID

Change Router password

Disable wireless web access to minimize the risk to have someone else altering the configuration and settings of your WI-FI router from a remote or wireless network.

Reduce the range of the signal

The first thing to do when setting up a wireless local area network , is to think of the appropriate places for all A.P according to the area to be covered. If the range of the signal is beyond your need, reduce it to fit, orienting antennas. It will minimize the signal leakage and avoid snoopers keeping an eye on your wireless **LAN** (**L**ocal **A**rea **N**etwork).

Use Firewall

Install or configure and activate your personal Firewall to filter the incoming and outgoing traffic of data and restrict the number of open ports.
Enable firewall features in router configuration such as the ability to block anonymous Internet requests.

Use static IP addresses

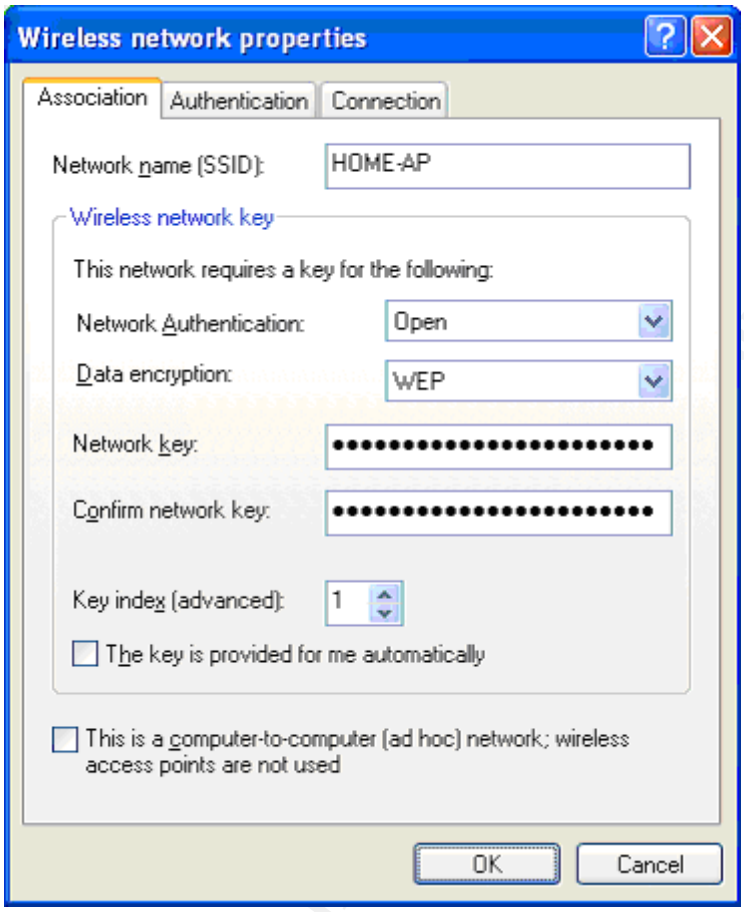
Enable **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) to allow automatic IP addresses to be generated to your different devices. As a default option, it is a common way if you don't want to be bothered with. But be aware that in this case, anyone with a proper SSID by implementing DHCP can obtain an IP address automatically and access to network services.
So turn off DHCP and use a static IP address instead, which is a number assigned to a computer to be its permanent address on the network.

WEP (**W**ired **E**quivalent **P**rivacy) **Encryption**

A word or phrase with any random keyboard characters is used to generate the RC4 encryption of the WEP key.

RC4 uses a symmetric encryption key where the same key is used to encrypt and decrypt the message.

The more long and random the key, the safer your security network is. But ensure you change the key regularly to avoid some malicious users deciphering it.
Both the sender and the receiver must use the same encryption key.



Example properties of an infrastructure mode wireless network using WEP for Windows XP with SP2

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

The weak point :

The reason why WEP is vulnerable is due to the fact that WEP is based on a static shared key and that key remains unchanged until human intervention takes place, WEP is not advisable for enterprise use. Even with longer encryption key, WEP does not offer adequate integrity protection.
.

More advanced encryption methods exist.

Advanced security process

WPA (**W**I-FI **P**rotected **A**ccess) **Encryption**

Level of data protection and access control to Wireless LAN are increased with WPA encryption compounded of authentication through the 802.1X standard and **EAP** (**E**xtensible **A**uthentication **P**rotocol) and dynamic key exchange which uses TKIP.

TKIP (**T**empora**l** **K**ey **I**ntegrity **P**rotocol) **Encryption**

TKIP is an enhancement of WEP, providing stronger security encryption key which combines a temporal key with the MAC address of your machine plus the 16 octet initialization vector.
Combined with the base key which is created every time a wireless station is associated to an access point (A.P) a sequence of 48 bit serial number is added and incremented to the key allowing the key to be changed and making it unique when a packet using TKIP is sent.

AES (**A**dvanced **E**ncryption **S**tandard)

AES is a symmetric cipher algorithm which has replaced **DES** (**D**ata **E**ncryption **S**tandard) and approved by the **NIST** (**N**ational **I**nstitute of **S**tandards and **T**echnology)

The strength of the encryption key, depends on its size 128-bit keys, 192 , 256 .Thus it will take quite a long time and a tremendous amount of processing to crack AES protected data , as shown below :

- 3.4×10^{38} possible 128-bit keys
- 6.2×10^{57} possible 192-bit keys
- 1.1×10^{77} possible 256-bit keys

802.11I (June 2004)

is the new security standard for Wireless networks. WI-FI Alliance has chosen the name of WPA2 for this standard. WPA2 uses AES and is backward compatible with WPA. Both have fresh encryption, unique and no key reuse.

The main concern of WI-FI Alliance, which is an international association, is to certify wireless products having met full interoperability requirements, based on IEEE 802.11 specification.

Utilize VPN (Virtual Private Network)

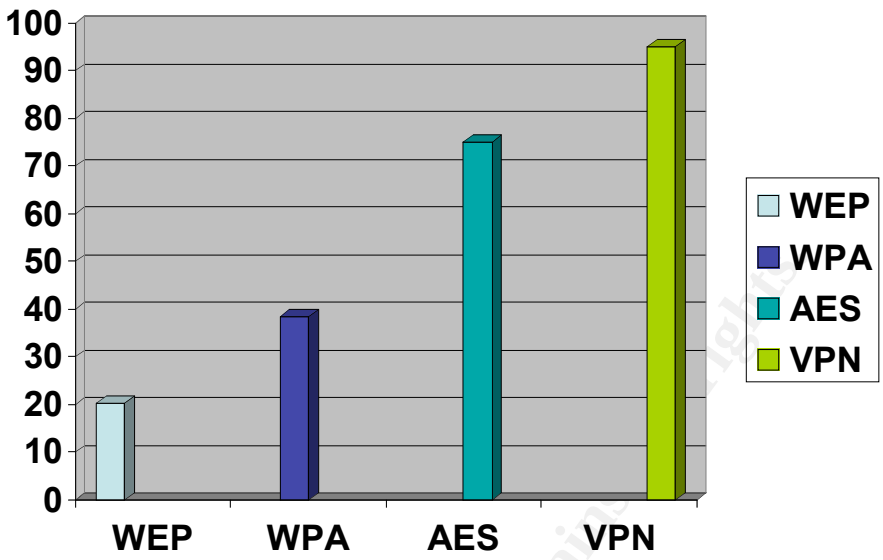
The aim is using encryption and security mechanisms to ensure that only authorized users can access the network and thus prevent data from being intercepted.

Because data remain encrypted all the way long, end to end tunnel, VPN is recommended for WI-FI networks.

Install Radius (Remote Authentication Dial-In User Service) server

When **EAP** (Extensible Authentication Protocol) protocol is used in WI-FI networks, identity of the user is requested and sent to Radius server for authentication. In a way, it is based on a mutual authentication, it means that both parts prove their identity which helps ensuring that the A.P is the genuine one.

EAP support multiple authentication methods such as **TLS** (Transport Layer Security) or **TTLS** (Tunneled Transport Layer Security).



Wireless LAN
Increasing protection in relation to the encryption method used

COMING SOON

The awaited **802.11E** standard will be finalized by WI-FI Alliance by the end of this year. It will improve the throughput and bandwidth management, first and foremost, **V**oice **O**ver **W**ireless **IP** (**VoWIP**) and video transmissions.

Summary

Most of people install WI-FI at home without thinking about security, because they attach very little importance to it, or simply due to their lack of knowledge.
By definition, “Well treat”, is : “consider in a specific way or provide treatment for”. In the same way, assuming WI-FI is a patient, the more you know about, the more you can take care of and cure. This is what this paper intends to do, by listing all the main threats and techniques used to prevent attacks.
But the best way to be safe is to protect first. It is essential as far as WI-FI is concerned. Even if you do not deal with financial data, private data it is worth keeping away from prying eyes , because you can never predict whether their intentions are harmful or not.

As WI-FI technology becomes widespread and commonly used, it is highly recommended to keep up to date on new security process and specifications. You can link to the following references or use any search on “WI-FI” word on the web. Some are references and trusted sources such as www.wi-fi.org (WI-FI Alliance) or www.sans.org (The SANS institute).

Don’t forget to update the firmware and drivers to enable new features and benefit from new fix known issues.

In conclusion, key words are: **keep yourself informed**, **protect** and **enjoy** WI-FI

Technical terms used

AES (**A**dvanced **E**ncryption **S**tandard)
A.P (**A**ccess **P**oint)
ARP (**A**ddress **R**esolution **P**rotocol)
DES (**D**ata **E**ncryption **S**tandard)
DHCP (**D**ynamic **H**ost **C**onfiguration **P**rotocol)
DOS (**D**enial **O**f **S**ervice)
EAP (**E**xtensible **A**uthentication **P**rotocol)
I.E.E.E (**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers)
IP (**I**nternet **P**rotocol)
LAN (**L**ocal **A**rea **N**etwork)
MAC (**M**edia **A**ccess **C**ontrol)
NIC (**N**etwork **I**nterface **C**ard)
NIST (**N**ational **I**nstitute of **S**tandards and **T**echnology)
RADIUS (**R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice)
RF (**R**adio **F**requency)
SSID (**S**ervice **S**et **I**dentifier)
SSL (**S**ecure **S**ockets **L**ayer)
TCP/IP (**T**ransmission **C**ontrol **P**rotocol/**I**nternet **P**rotocol)
TKIP (**T**empora**l** **K**ey **I**ntegrity **P**rotocol)
TLS (**T**ransport **L**ayer **S**ecurity)
TTLS (**T**unneled **T**ransport **L**ayer **S**ecurity)
VoWIP (**V**oice **O**ver **W**ireless **IP**)
WEP (**W**ired **E**quivalent **P**rivacy)
VPN (**V**irtual **P**rivate **N**etwork)
Wi-Fi (**W**ireless **F**idelity)
WLAN (**W**ireless **L**ocal **A**rea **N**etwork)
WPA (**W**I-FI **P**rotected **A**ccess)

References

http://en.wikipedia.org/wiki/IEEE_802.11

http://www.wi-fi.org/OpenSection/secure.asp?TID=2#security_tech

http://www.sans.org/rr/whitepapers/awareness/1399.php

http://www.webpronews.com/it/security/wpn-2 by **Zackary Anderson** 2004-08-18

http://www.uptotech.com/sinformer/n/news4320.php

http://www.futura-sciences.com/sinformer/n/news4323.php

http://www.infosyssec.net/infosyssec/secdos1.htm (4)

http://www.wi-fiplanet.com/tutorials/article.php/1457211

http://www.windowsecurity.com/articles/Wireless_Attacks_Primer.html

http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wifisoho.mspx

http://www.informit.com/guides/content.asp?g=security&seqNum=64