

# Review of Present IEEE 802.11 “Wi-Fi” Security Issues and of Other Possible Vulnerabilities

G. A. Mendez, Liyanage C De Silva, Amal Punchihewa; Institute of Information Sciences & Technology, Massey University, Palmerston North, New Zealand.  
and Stan Swan; Electronics, Massey University, Wellington, New Zealand

**Abstract**—This paper presents various IEEE 802.11x wireless security issues, and discusses flawed Wireless Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) in particular Pre-shared key (PSK). Types of attacks like active, passive and man-in-the-middle attacks will also be discussed. Finally describes attacks that are yet to be widely deployed against users of wireless using already known Remote Procedure Call (RPC) attacks.

**Index Terms**—802.11, Attack, Security Issues, Virus, Worm

## I. INTRODUCTION

THE computer use of wireless has dramatically increased over the years. In the 4<sup>th</sup> quarter of 2004 the worldwide Wireless Local Area Network (WLAN) market grew 10 percent sequentially and 30 percent year-over-year [1].

Total worldwide sales of home and small-office wireless LAN products in 2003 topped \$1.3 billion (about 60 percent of the market), while enterprise wireless sales came in at less than \$900 million [1].

With the ever expanding number of wireless users, the number of backdoors to networks is increasing. This is illustrated by the more or less constant percentage of people who are not configuring wireless devices appropriately. The Wireless Geographic Logging Engine WiGLE reports a worldwide value for encryption usage is approximately 34% [2].

This paper discusses the various security protocols implemented in the standard wireless networks, in particular Small Office Home Office (SOHO) and not enterprise solutions. There will be a brief overview of the different types of attacks and then talk about attacks that are set to rapidly spread in turn with the expansion of wireless numbers.

## II. SECURITY PROTOCOLS

There are several security protocols that can be enabled on wireless clients and Access Points (AP), and these are illustrated in Fig. 1. These protocols on their own do not allow a realistic amount of security. Maximizing security can be done by having several tiers or levels of security, doing so will make it harder if not impossible to

compromise the wireless network. This is due to the fact that it increases the amount of work required for the hacker to compromise the network.

Unless the attacker is specifically attacking that network it is often easier to move onto the next and most likely unsecured network.

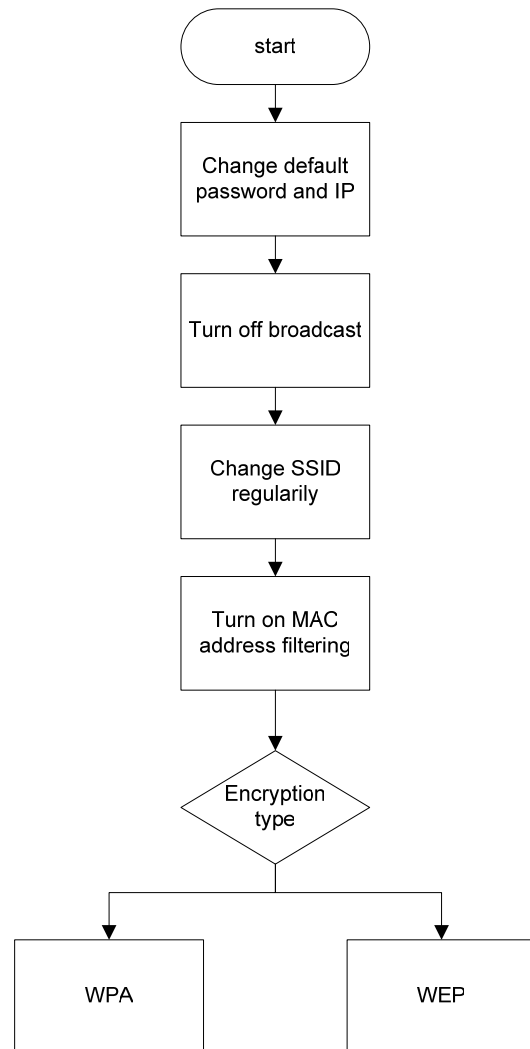


Figure 1 Tiers/levels of wireless security

### A. Service Set Identifier (SSID) Broadcast

SSID broadcast is a function of wireless AP. Its function is to broadcast its name information so that a wireless client can discover it using the appropriate client management software or Window XP wireless connection software. Turning this off can prevent most amateur hackers from locating your access point using wireless sniffing tools like

Net Stumbler (wireless mapping tool). However reasonably knowledgeable hackers can use sniffer tools like Kismet (wireless mapping tool for Linux) which requires the hackers' wireless adaptor to run in promiscuous mode. This mode searches for 802.11x (a / b or g) traffic and obtains the SSID from the packet information. The disabling of SSID broadcast can therefore be circumvented by hackers. In addition the use of company names or locations for SSID names may be bad practice, as it could allow a hacker to pinpoint the physical location of a wireless LAN.

**B. MAC (Media Access Control) Address Filtering**

The MAC Address filtering function on AP's allow access to only those wireless clients with the authorized MAC Addresses. The approach is used to deny access to the wireless network if the MAC address of an authenticating client doesn't match with the list of authorized MAC addresses. This makes it harder for a hacker to access your network with a random MAC Address.

Network addresses can easily be captured from legitimate wireless traffic using packet monitoring tools such as Ethereal. Once the address information is gathered (MAC Address information is transmitted with each wireless packet) it can easily be spoofed by manually inputting another MAC address in the network settings shown in Fig. 2

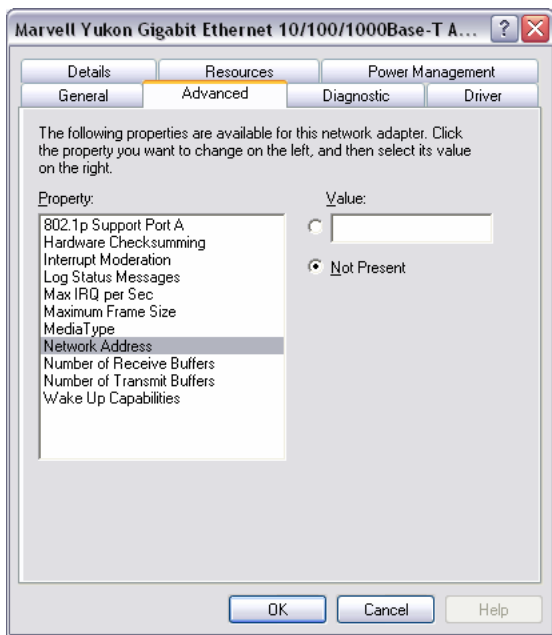


Figure 2 Spoofing a MAC Address

Thus the filtering can be circumvented because by using a captured address the AP will allow the attacker the spoofed network address to authenticate with the network.

**C. Wired Equivalent Privacy (WEP)**

WEP was ratified in September 1999 and was a method to improve security on wireless networks (802.11). WEP was created to provide the same amount of confidentiality of traditional wired networking, and hence the name.

Due to the wireless medium, the packets are susceptible to eavesdropping. In addition several serious weaknesses were identified [3]. In 2001 a discovery was made by Fluhrer, Mantin and Shamir: for all possible keys, the

statistics for the first few bytes of output keystream are strongly non-random, leaking information about the key. If the long-term key and nonce (a randomly chosen value, different from previous choices, inserted in a message to protect against replays) are simply concatenated to generate the RC4 key, this long-term key can be discovered by analysing large number of messages encrypted with this key. This and related effects were then used to break the WEP encryption, at both 64 and 128 bit levels.

This fact in addition to tools like Aircsnarf, WEPCrack or AirCrack is used in conjunction with software like Void11. Void11 uses tools "deauth" and "auth". Deauth floods the wireless network with deauthentication packets and spoofed Basic Service Set ID's (BSSID). This causes stations to drop their network connection. Auth floods the AP's with authentication packets and random addresses. This will enable the cracking tools to gather enough packets to usually crack the WEP key in 5-15 minutes [4].

**D. Wi-Fi Protected Access (WPA)**

WPA was introduced in 2003 to deal with the serious security issues of WEP. WPA is superior to WEP in Wi-Fi security for SOHO users. Two modes are available: Pre-Shared Key and RADIUS (Remote Authentication Dial-In User Service).

Pre-Shared Key gives you a choice of two encryption methods: TKIP (Temporal Key Integrity Protocol), which utilizes a stronger encryption method, and AES (Advanced Encryption System).

The only susceptible WPA scheme is TKIP [5] with a short password (a password of less than 20 characters is susceptible to being cracked), this can technically speaking be extended to WPA2 using TKIP. "[6] The weakness of the WPA scheme is the calculated MIC value that is used in the validation messages 2-4 of the four-way handshake. The use of programs like coWPATty targets the final EAPoL message. Because both the MIC value (not the key) and the EAPoL message are passed as plaintext, an attacker can focus on the MIC hash value. The challenge is tied to the fact that an attacker must first convert the dictionary word to a PMK, using the correct algorithm with an accurate SSID value. Then the resulting value is plugged into another equation that also requires the MAC addresses and Nonce values of the supplicant and authenticator. The result of this calculation is the PTK, from which the attacker can strip the MIC Key. With this MIC Key, the attacker then performs the same HMAC\_MD5 hash on the captured EAPoL message to see whether the selected password produces the same MIC as the captured MIC."

To execute a successful attack on a random network, an attacker must have a large dictionary file, a powerful computer, and a little luck in order to obtain the password. [6]

**E. Other Methods**

There are other methods for securing networks, including Virtual Private Networks (VPN) and proprietary solutions, but this paper mainly investigates home user solutions as they are the majority of users at the present. Most enterprise

solutions require that a server additional hardware be setup for these services in addition to the wireless hardware.

### III. ATTACK TYPES

#### A. Passive Attacks

A passive attack Fig.3 is one where an individual with the necessary hardware (a simple device like a palmtop or laptop with a wireless adaptor) and software (AirSnort or Ethereal) can 'listen in' or packet sniff wireless network traffic. This is further made easier by the fact that all 802.11 traffic is conducted over unlicensed public frequencies 2.4GHz Industrial Scientific Medical (ISM) band, meaning that it is harder to protect the network as anyone can use these frequencies.

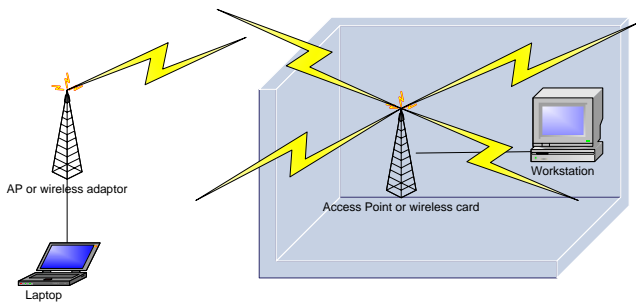


Figure 3 Passive attacks

Passive attacks are very difficult to detect as there is no way to prevent or know when a passive attack is taking place. A single person can drive around picking up signals leaking from networks, and can in certain situations where the signal is strong enough, be parked down the street or even further [7] from the company and be able to access the network. Most passive attacks are harmless, and not illegal unless accessing networks, actively attempting to crack encryption, jamming or analysing wireless traffic with intent to cause harm.

Passive attacks are usually conducted using programs like Kismet or Ethereal and using hardware that is able to work in promiscuous mode. This requires a card that uses the Prism 2 or Prism 2.5 chipset.

#### B. Active Attacks

Once enough information is obtained during a passive attack, an active attack can begin Fig. 4 These attacks can start with the cracking of encryption, spoofing of MAC addresses and are the same as wired attacks, unauthorised access to sensitive data, theft and damage for files due to viruses inserted into the network etc. In addition spam can be easily distributed using simple windows commands like netsend.

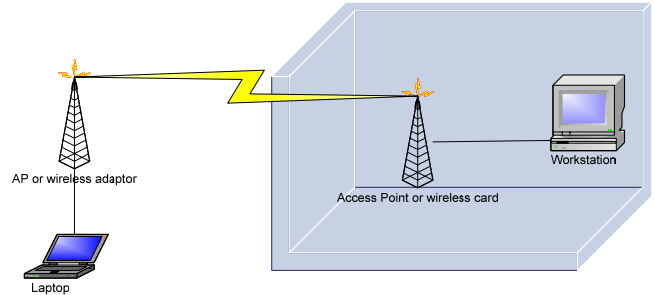


Figure 4 Active Attack

In particular Denial of Service attacks [8] are of particular importance as, if done in the MAC layer of the 802.11 protocol it does not matter if the network is open or has WEP enabled. The three main DoS attacks are: Probe Request Flood (PRF), Authentication Request Flood (ARF) and Association Request Flood (ASRF)

These are flooding attacks, and work due to repeated, massive injection of frames; each frame has its own fake MAC address (MAC spoofing), randomly generated, in order to simulate the presence of a large number of stations sending requests to the AP.

When the AP responds to fake frames sent by the attacker station, it gets no ACK frames back, so it starts a retransmission cycle for every single frame received, therefore a lot of buffer space is used up in order to store response frames waiting to be transmitted again. Therefore in this manner a simple flood of requests for an attacker can cause the exhaustion of all internal buffers of the AP, this will effectively prevent any genuine traffic from being processed. This results in a complete denial of service.

“As the attacks act at a low level with respect to any authentication mechanisms, their effect cannot be mitigated by the introduction of WEP or other security protocols; indeed, in some cases, introduction of WEP resulted in a heavier load on the AP, increasing its vulnerability to the attacks”.

The reason for this is that with WEP enabled, the AP needs even more resources to handle the encrypted communications, therefore reducing the internal buffer and decreasing the time and packets required to cause a DoS.

#### C. Man-in-the-middle Attacks / Evil Twin

Attackers interfere with a connection to a legitimate network by sending a stronger signal from a base station close to the wireless client, turning the fake access point into a so-called evil twin shown in Fig. 5.

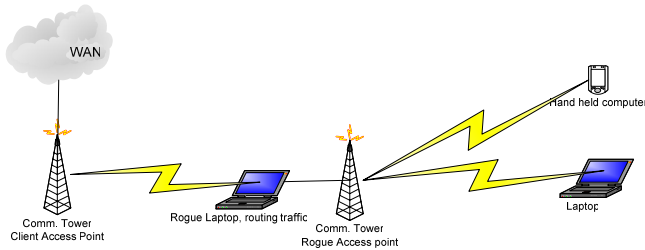


Figure 5 Man-in-the-middle attacks

Once an unknowing user has connected to an evil twin, a hacker can intercept transmitted data. Users are invited to log into the evil twin with bogus log-in prompts and can be lured into passing sensitive data such as user names and passwords. There is no need to crack encryption or gather packet information if you can get the user to enter user and password information.

In addition this type of attack can be used to get users to unknowingly install viruses, worms and keyloggers (software that records keyboard strokes on an infiltrated machine) so antivirus software doesn't protect it. It doesn't recognise the signatures. This was done recently at an IT conference [9]. Indicative of the serious nature and susceptibility of an attack like this is of Spencer Parker, a director of technical solutions at AirDefense, whose computer was infected by the attack. This illustrates the serious need to educate users. As the article shows, experts in the field of wireless security have succumbed to these attacks, meaning that if attacks were conducted against average users the intrusions would probably never be detected until too late and/or a greater percentage of the civilian population would be misled and their data security compromised.

#### IV. DISCUSSION

A slowly increasing type of active attack is taking hold. The use of worms to attack wireless users. The attacker waits till a patch comes out then using that knowledge attacks computers that haven't yet installed the patches (interim period). The simpler method makes it easier than finding a security hole (means you don't have to be a expert hacker or find one of the ever decreasing numbers of weaknesses, you just have to know what the weakness is by look on the internet on what the weakness is and then initiate attacks using that weakness with the knowledge that there is an interim period when computers aren't patched.

"A virus [10], for example, is a program that embeds itself within another program. It executes when that program executes, typically causing some mischief, like deleting data, altering a display, or scrolling a message. Just as human viruses need a cell to reproduce, computer viruses need a host program. They cannot spread from one computer to another on their own; usually, they get into a computer when a naive user runs an infected program, often by opening an infected e-mail attachment. Viruses can often be detected by observing changes in the files stored on the machine."

"Worms [10], unlike viruses, are specifically designed to propagate through a network, usually the Internet, replicating themselves at each machine before jumping to

new ones. No human action is needed for a worm to get from one computer to another. In most cases, the frenetic activity and communication the worm causes is itself the point: a worm like Sapphire creates so much network traffic so quickly that it overwhelms routers and other network nodes, in what is called a denial-of-service attack." As Fig 6. shows a worm can spread at an enormous rate.

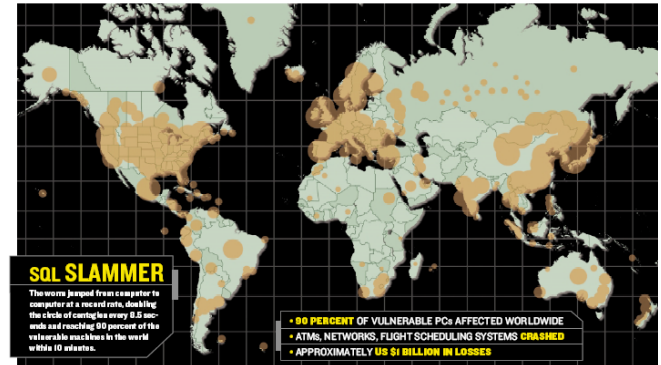


Figure 6 Danger of Worms [Courtesy IEEE Spectrum] [10]

"Today, so-called blended threats [11], such as Blaster and Sobig.F, are increasingly sophisticated. Blended threats combine the characteristics of viruses, worms, Trojan horses, and malicious code with desktop, server, and gateway vulnerabilities to carry out an attack. These threats are difficult to prevent because they are designed to elude the security products commonly deployed across today's enterprises. Recent blended threats have also included MyDoom, Netsky, and Sasser."

Blended are different to worms and viruses in the speed in which they spread. The Slammer worm in 2003 infected computers worldwide in only 10 minutes as illustrated in Fig. 6 showing spread of infected areas. Blended attacks use multiple paths to infect computers. They efficiently propagate by exploiting known security holes and vulnerabilities. It is this behavior which makes it possible to use wireless to attack users who think they are protected behind hardware firewalls.

"In 2003, Symantec documented 2,636 new vulnerabilities, an average of seven per day. Of these new vulnerabilities, 80 percent were remotely exploitable, and 70 percent were easily exploitable." In the first six months of 2004 Symantec documented 1,237 new vulnerabilities, 70 percent of which were easily exploitable.

Moreover, the period of time between the announcement of a vulnerability and the release of an associated exploit continues to shrink, making it increasingly likely that we will see a so-called "zero-day" threat. A zero-day blended threat could target a vulnerability before that vulnerability is announced and a patch made available."

A RPC attack works (in this case the blaster worm) in this manner; the attacker scans for a vulnerable computer. Once one has been found, it sends a buffer overflow to the victims' computer. The buffer overflow caused by unchecked parameter in a DCOM function then causes the victims computer to request the program from attacker (this can be a file on the attackers machine on a file put on the internet). The computer is infected.

Then it possible of obtaining usernames and passwords from the key logging software and then using say for example Microsoft Remote Desktop tool to gain access to

all the user data and/or network shares on a server. VPN's are at risk, as once a computer is compromised all the details and usernames and passwords can be used to access any previously secured resources through VPN.

As a popular key logging software site states [12] "You can attach keylogger to any other program and send it by e-mail to install on the remote PC in the stealth mode. Then it will send keystrokes, screenshots and websites visited to you by e-mail or FTP. You don't have to worry about the firewall alerts - now our keylogger can be invisible for the firewall program. Our keylogger supports remote installation, update and removal - no physical access required!". The use of wireless attacks can circumvent corporate firewalls and antivirus systems. This compromised computer can as with any serious hacking attempt, can then be used to launch an attack on other machines without being able to track down the culprit.

Recently in New Zealand media [13], attention was given to a recent spate of banking details and passwords being stolen from users using internet cafés though key logging software being installed on the machines they were using. While this was in itself a shocking threat, the new very probable future attacks of RPC attacks can easily steal users passwords and sensitive data through wireless connections for peoples homes and workplaces.

The main fact for this is due to a majority of banks in New Zealand only using one level/tier of security, as opposed to international banks using two levels or tiers of authentication. That is a password and username in addition to a unique password that is sent to the users registered cell phone whenever a banking session is started by the user.

## V. CONCLUSION

While blended attacks have yet to take off, given time they could be set to be the new bane of computer users (specifically ones with wireless hardware in the network). They would be infected at anytime anywhere without knowledge that key logging software has been installed on a client machine till credit card information, private information and company secrets are stolen.

While internet banking can be secured easily by using a two level/tier authentication, wireless user data and company secrets can still be stolen by these attacks. The regular updating of Microsoft software, use of proper firewalls and antivirus tools can and will greatly minimize risk to attacks such as these. In addition use of anti-keylogging software is recommended.

[14] "Anti-keylogger™'s protection spyware will not be able to record and steal your sensitive information, passwords, logins, PINs (Personal Identification Numbers)." Microsoft should incorporate this software into their operating systems to reduce logging.

The computer industry is also to blame for security issues. The reason for this is that they sell wireless products that don't force users to choose new passwords (using easy to setup wizards and so on) and change default weak settings. People still use default SSID's, and leave the default password or easy to crack passwords (words in dictionary). By doing so an attacker can attack the AP's known weaknesses of the particular make and model. It

should be companies' moral obligation to force users to change the factory settings before the network will work

Another method that can be implemented is turning off AP's when not in use i.e. the AP is on during working hours from Monday through Friday from 8a.m to 5 p.m. An easy modification of available AP functions could be used as show in the Fig. 7 below. Either a software solution or the use of a simple cheap time switch could be used to restrict running hours of the AP.

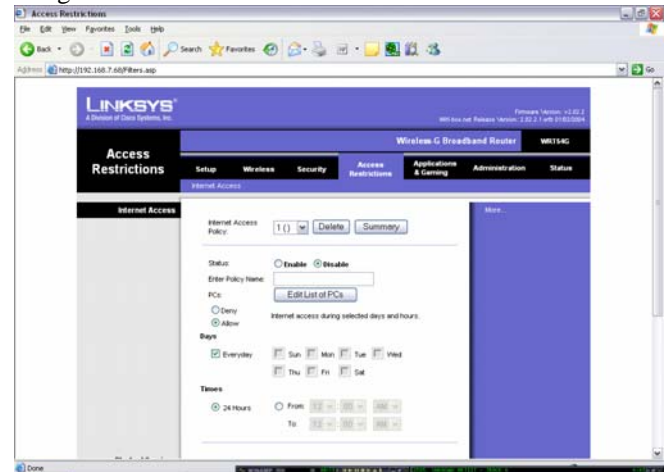


Figure 7 Enforcing Access Restrictions

While WPA2 and other standards like 802.16 WiMAX have just recently been released, it is still yet to be seen how long they will remain secure before a weakness is found and they are cracked.

The most important point may be not to trust wireless now till it is more secure, and if there is valuable information on a network that has to be protected, don't use wireless.

## REFERENCES

- [1] Synergy Research Group, February 15 2005, WLAN Equipment Sales Grow 30% in 2004 [Press release], <http://www.srgresearch.com/store/2-15-05.htm> Visited : May 15th 2005
- [2] March 30 2005, Wireless Geographic Logging Engine, <http://www.wigle.net/gps/gps/GPSDB/stats/> Visited : May 18th 2005
- [3] N. Borisov, I. Goldberg, and D. Wagner, Intercepting Mobile Communications: The Insecurity of 802.11
- [4] H Cheung, March 31 2005, "The Feds can own your WLAN too" <http://www.tomsnetworking.com/Sections-article111.php> Visited : May 11th 2005
- [5] R. Moskowitz, November 4 2003, Weakness in Passphrase Choice in WPA Interface, <http://wifinetnews.com/archives/002452.html> Visited : May 1st 2005
- [6] S. Fogie, March 11 2005, Cracking Wi-Fi Protected Access (WPA), part 2, <http://www.informit.com/articles/article.asp?p=370636> Visited : May 1st 2005
- [7] S. Swan, Massey University, May 2004, USB adaptors & DIY antenna = "Poor Man's WiFi"?, <http://www.usbwifi.orcon.net.nz/> Visited: may 28<sup>th</sup> 2005
- [8] G. Me & F Ferreri, 2004, New Vulnerabilities to Dos Attacks in 802.11 Networks, [http://www.wi-fitechnology.com/Wi-Fi\\_Reports\\_and\\_Papers/Dos-attacks/defining\\_DoS\\_attacks.html](http://www.wi-fitechnology.com/Wi-Fi_Reports_and_Papers/Dos-attacks/defining_DoS_attacks.html) Visited : May 16th 2005
- [9] D. Hett, 25 April 2005, Hackers attack IT conference, <http://news.zdnet.co.uk/0,39020330,39195956,00.htm> Visited : May 18th 2005
- [10] J. Riordan, A. Wespi., D. Zamboni., "How to Hook Worms" *IEEE Spectrum*, Volume 42, Issue 5, May 2005 Page(s):32 - 36.
- [11] Symantec Enterprise Solutions, September 21 2004, Wireless Security: An Update, <http://enterprisesecurity.symantec.com/article.cfm?articleid=4708&EID=0#INTRO> Visited : May 18th 2005

- [12] Blazing Tools Software, <http://www.blazingtools.com/bpk.html>  
Visited : May 18th 2005
- [13] One news, March 29 2005, Internet banking security questioned,  
[http://tvnz.co.nz/view/news\\_national\\_story\\_skin/481755%3fformat=html](http://tvnz.co.nz/view/news_national_story_skin/481755%3fformat=html) Visited: May 18<sup>th</sup> 2005
- [14] Anti-Keylogger, <http://www.anti-keyloggers.com/> Visited : May 24th 2005