

Nov 2008

WARDRIVING

Pune

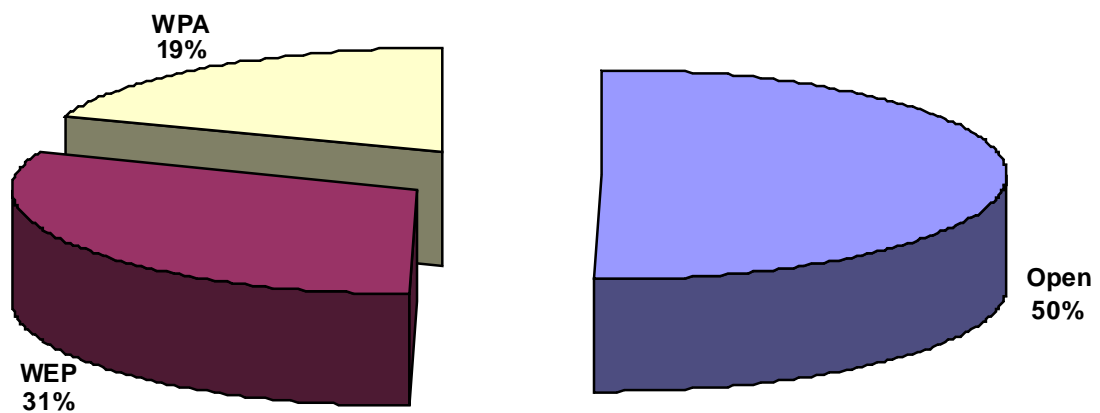


Club**HACK**



KEY FINDINGS

50 % of Pune's wireless networks is insecure and DO NOT require any skill to break into. This kind of networks can be misused by a terrorist, a kid next door, a competitor or anyone.



31% of the wireless networks need very little skill to break into. All it takes is little knowledge and around 15 minutes on hand to create havoc.

To our relief atleast **19%** of Pune's public who use wireless are safe. They use good methods of security that would require higher skills and time on hand to break into.

Introduction

The ease of using a Wireless network is spreading like wild fire and everyone is making their home or office wireless. Looking at the growing concern and lack of knowledge on wireless security, ClubHack decided to take a stock of situation of wireless security in Pune - one of the major IT cities in India.

To take this survey, ClubHack took help from Pune Police and conducted a Wardriving on 10th November 2008. This Wardriving aims at analysis of wireless network security in Pune city at common places like IT parks, residential areas, market areas, hotels, airport etc.

ClubHack would like to thank Pune Police for their cooperation and assigning an officer to accompany the wardrive.

What is Wardriving?

Wardriving is driving around a city searching for the existence of Wireless Networks (802.11). It's locating and logging wireless access points while in motion. Often, this task is automated using dedicated wardriving software and a GPS Device.

As per Wikipedia: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or PDA.

Process

On 10th November 2008, ClubHack created a setup in a car which included laptops & GPS enabled devices for the exercise. The car was driven in all the popular areas which included IT parks, multiplexes, residential areas, markets, busy streets etc. While the car was driving at a normal speed, the GPS and wireless enabled devices sensed the availability of wireless signals on the road. These signals were then recorded with details like MAC address of the access point, name of the network, security used, longitude and latitude of the location where the signal of a particular network was highest.

Terminologies

- SSID – Name of the wireless network.
- Access Point – Wireless equipment used to transmit signal. Alternatively it is also termed as wireless router, wireless device or AP.
- Ad-Hoc – Laptop to laptop connection over wireless is generally called as ad-hoc or peer-to-peer connection.
- Encryption – Security methodology used to secure the communication. Commonly used for wireless are as follows
 - Open: Not secured network where anyone can simply connect without any password
 - WEP: WEP is a security measure which is not very strong and was cracked long time back. Dedicated efforts of nearly 15minutes can help someone crack the WEP password.
 - WPA: WPA and its variants (WPA/WPA2) are considered to be fare security which takes a lot of time, efforts and knowledge to break into.

Interesting observations

ClubHack found some very nicely crafted SSID's in Pune. To name a few

```
<body bgcolor= #000000>
W!re1e$$
Hard Killer
!!Virus!!
Ç ±ÛSSID
StartYourVPN
NoVPN
Hackers Area (do not mess)
not_giving_ssid
```

There was an SSID which clearly tells that it's an AP in the office of system/IT manager but there was no security on it.

An ad-hoc network was found in the name of a big multinational company

An encrypted ad-hoc network was found. User seems to be a smart person.

Near a big company in IT security, a lot of hidden SSID were found

Few Open networks were found with hidden SSID, who are they trying to fool?

Wireless security myth

SSID Broadcast

There is a common myth in industry that hiding SSID increases security. ClubHack would like to inform that hiding SSID will not add much to the security but in case of a corporate user, hiding SSID will facilitate other kind of attack.

No harm in connecting to Open networks

Connecting to Open SSID is equally dangerous and can expose the user to attacks like passive sniffing, MITM, SurfJacking, ARP poisoning, local file access, remote exploits on client machines and a lot more.

Hotspot must be Open only

Keeping hotspot with Open security can lead to above mentioned attacks on the users connected. Captive portal webpage which asks for username and password can only restrict connectivity to Internet but without a username and password many of the above mentioned attacks can be launched.

“Free Internet Access” or “Free public wifi” will connect to internet for free

“Free Internet Access” or “Free public wifi” are known as Viral SSID and it does spread from one computer to another if a user tries to connect to it. They are ad-hoc connections and DONOT give you a free internet access

Recommendation

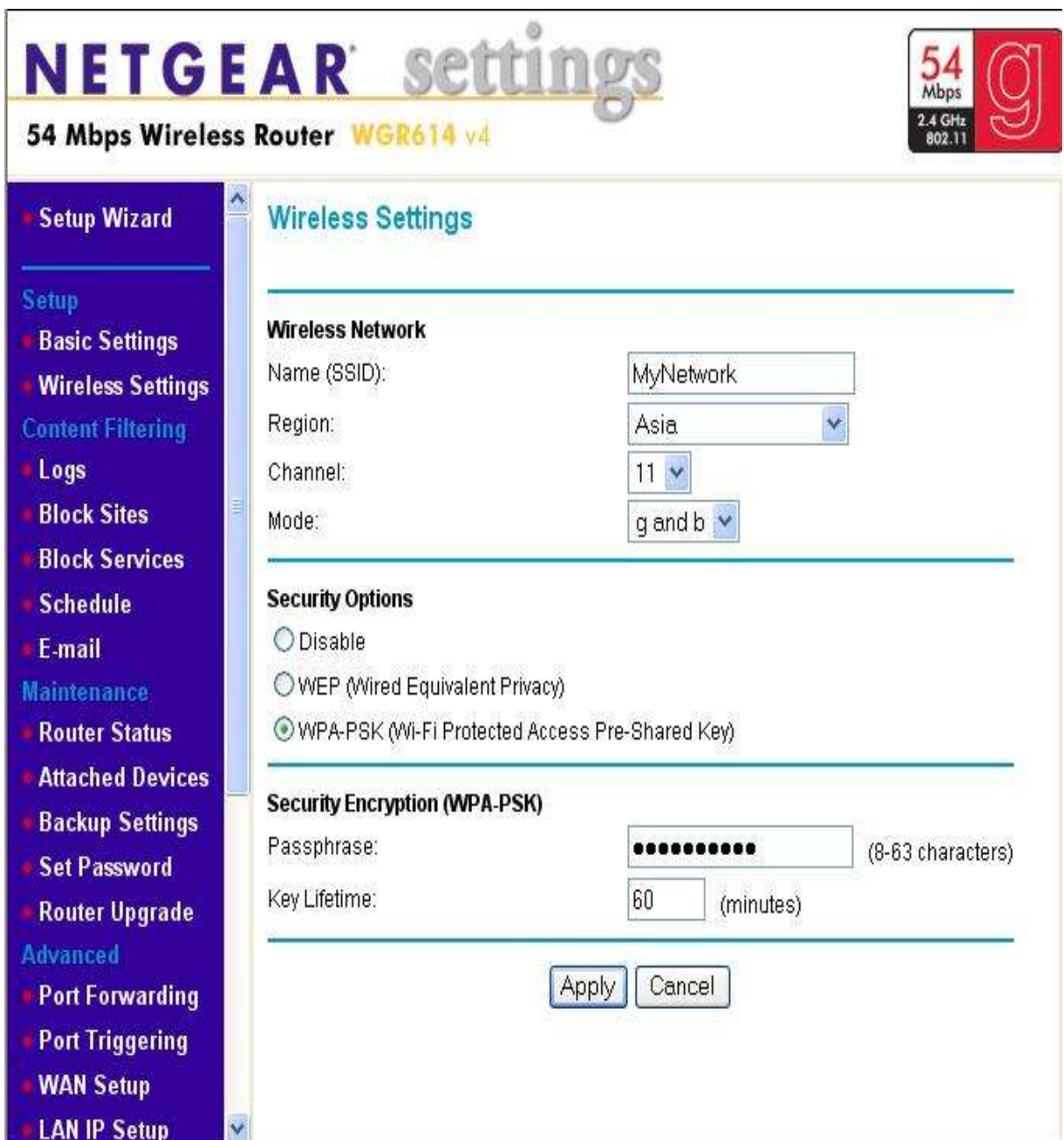
ClubHack and Pune Police recommends smart configuration of access points to secure the home/corporate wifi. Though these steps will not give 100% security but surely increase the security level and make breaking into the networks very difficult

With immediate effect users should move their devices to WPA or WPA2 security level
Steps to achieve WPA

- Open the configuration of your wi-fi device
- Go to wireless setting
- Under security option, select any one (whichever available)
 - WPA
 - WPA - PSK
 - WPA - Personal
 - WPA - AES
 - WPA2 - Personal
 - WPA2 - PSK
- Set a complex password
- Change the login password of the wireless router.
- Change the SSID to something classy
- Don't disable SSID broadcast
- Done

Please refer to the following sample screenshots of few common access points for quick reference.





NETGEAR settings

54 Mbps Wireless Router WGR614 v4

54 Mbps
2.4 GHz
802.11

Setup Wizard

Setup

- Basic Settings
- Wireless Settings

Content Filtering

- Logs
- Block Sites
- Block Services
- Schedule
- E-mail

Maintenance

- Router Status
- Attached Devices
- Backup Settings
- Set Password
- Router Upgrade

Advanced

- Port Forwarding
- Port Triggering
- WAN Setup
- LAN IP Setup

Wireless Settings

Wireless Network

Name (SSID): MyNetwork

Region: Asia

Channel: 11

Mode: g and b

Security Options

Disable

WEP (Wired Equivalent Privacy)

WPA-PSK (Wi-Fi Protected Access Pre-Shared Key)

Security Encryption (WPA-PSK)

Passphrase: (8-63 characters)

Key Lifetime: 60 (minutes)

Apply Cancel

Additionally to be secure on wireless networks keep in mind

- Keep away from Open networks
- Even if you use VPN, make sure your VPN encrypts all your internet traffic too and not only the internal traffic
- Never connect to “Free Internet Access” or “Free public wifi”
- Create a DHCP pool on your wireless router of a limit which you know will be sufficient for you
- Add reservations in DHCP pool to safeguard your IP allocation
- If possible add MAC address filtering, although it will not make you super secure but still will add one more pain point for attacker

About ClubHack

ClubHack is an initiative to bring security awareness in common people who use computers and Internet in their daily life. It's a member driven open community to make cyber security a common sense. The phenomenal growth of the Internet economy has led to a sharp increase in computer crimes and hacking incidents. ClubHack aims at making technology users aware of the risks associated with cyber transactions as well as the security measures. As our motto says **“Making Security a Common Sense”**

ClubHack also organizes India's own International hacker's convention every year in the month of December.

Disclaimer

- Wardriving is a passive activity which does not includes connecting to any network.
- Wardriving is a not an illegal activity
- Detail results of Wardriving will be submitted to Pune Police and will NOT be shared with anyone else
- The complete exercise was done to review the security status of the city and is absolutely educational only

Acknowledgements

ClubHack would like to thank Pune Police for their kind support.

Credits

Dr. Satyapal Singh, Commisioner of Police, Pune
Mr. Rajendra Singh, Adnl CP, Pune Police
Mr. Rajendra Dahale, DCP Cybercrime cell, Pune Police
Dr. Sanjay Tungar, Pune Police officer on the wardrive
Rohit Srivastwa, Founder ClubHack, War Driver (The scanning part)
Jamaal Raazi, Member ClubHack, War Driver (The driving part)
Tejas Bahulkar, for the photo of Shaniwar wada on the cover page :)