# Analysing and Mapping Wireless Networks

Andrej Komarov (ITdefence Ltd/Russia)

Difficulty

● ○ ○

**Wireless technologies are getting into our daily lives more and more each day. For one it's a craze of convenience or the decision of the different technological problems, and for others – fighting the jumping-off place where real cyberfights are unwrapped.**

Hacking in the wireless sphere is more independent, original and wide, then, for example, web-hacking. You will understand why after reading this article. Imagine! We will go to the Kremlin, Red Square (Russia) and take a warchalking tour under the President's towers.

Everything, that is required for the beginning of the practical side is: notebook with Wi-fi card, some software for penetration tests, GPS module for navigation and, of course, a comfortable backpack. After perusal of this article you will learn to make maps of the AP's, to analyze the security level of wireless Networks and even to make jokes.

### My equipment

GPS-receiver GlobalSat BU-303 USB on SiRF StarIIe/LP chipset, providing high quality and speed of coordinates definition. As it possesses almost minimal *cold start* – 45 seconds.

The problem is that at startup, the device *does not know*, where it is on the planet. In order to orient itself it starts to scan a range of frequencies, to analyze signals and calculate your coordinates.

The notebook is an Alienware NP9860 – the ideal tool for wardriving, and ideal for its compactness.

## Wi-fi positioning and GPS

With the development of Wi-Fi (Wireless Fidelity) and the actively growing number of WLAN networks. Such decisions are very real and the widespread availability literally everywhere, from small offices to huge corporate sort networks.

It is not necessary to hide, today the safety of such networks (standard 802.11 x) leaves much to be desired.

### What you will learn...

- Wi -fi positioning,
- how to make a wardriver's map,
- common attacks in the wireless infrastructure.

### What you should know...

- Some knowledge on wireless technology,
- basic knowledge on network analyzing.

In the center of Moscow the wi-fi services are available at almost every corner, under the official public information for today in the capital it is over five-hundred public access points.

For simplification and the presentation of the work we shall use Wi-fi positioning which is a method of drawing AP's (Acess Points) on a special map that can be converted into one of the most popular graphic formats.

**Figure 1.** *Kreml*

We shall also use Netstambler (*netstumbler.com*) for our scanner. But you should remember that using this tool can be easily detected by Wireless IDS or special triangulation systems. First of all, there is special Easter egg in Netstumbler, hidden in LLC frames:

- 0.3.2 Flurble gronk bloopit, bnip Frundletrune,
- 0.3.2 All your 802.11b are belong to us,
- 0.3.3 *intentionally blank.*

Secondly, some of IDS systems, like Wireless Snort, have special preprocessors, which can detect Netstumbler in about one second. For more information about this there is a paper written titled *Analysis of WLAN discovery applications for Intrusion Detection* (Joshua Wright).

As the purpose of studying we have chosen Ohotniy Riad, there we will try to analyze the geo-distribution of wireless activity and to visually trace hotspots finding the distance between them.

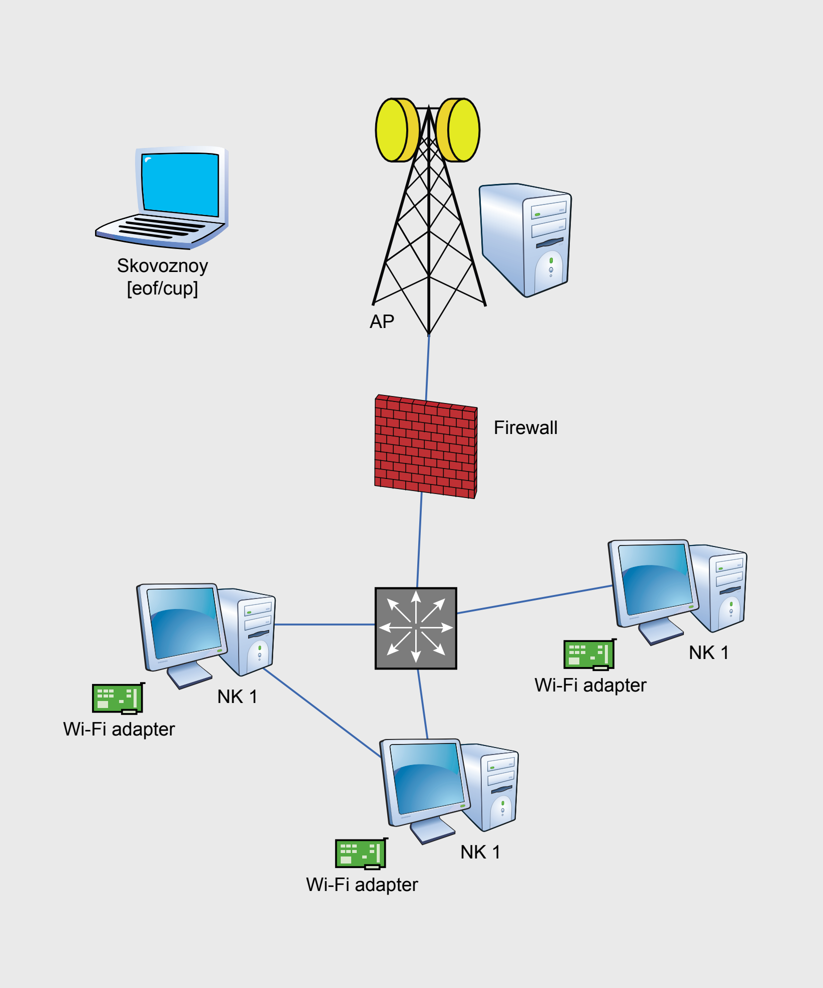


**Figure 2.** *Wiimap*

## Wi-fi hotspot's mapping software

Products that can be used for navigation and Wi-Fi mapping.

### Microsoft Mappoint Europe

Is a commercial cartographical product supporting integration with most of the GPS-devices and is absolutely compatible with Netstambler.

Compatibility occupies an important role, as the report after the scan cannot be imported to all mapping software that is suitable for GPS navigation. At worst special scripts may be required of you to transform broad gullies. A concrete example of this is MapSource MPS, for compatibility with which it is required to use *http://terenin.com/nets2mps.zip.*

In real time by using a wireless network and a computer and the mechanism of Microsoft Location Finder, which uses a database of known points of access for Wi-Fi to create the definition of coordinates of the user. (*http://wireless.gayamerican.org/microsoft-mappoint-wifi.html*)

### Microsoft Streets And Tips

Analogue of Microsoft AutoRoute. This software is ideal for automobile fans (including wardrivers) as it is geared to be visually convenient explaining where you are at any given moment.

There is also an option of voice support. For successfull importation of the scanner's report use StreetStumbler 2004 RC4.6 (*http://home.adelphia.net/~kg4ixs/ss2004*).

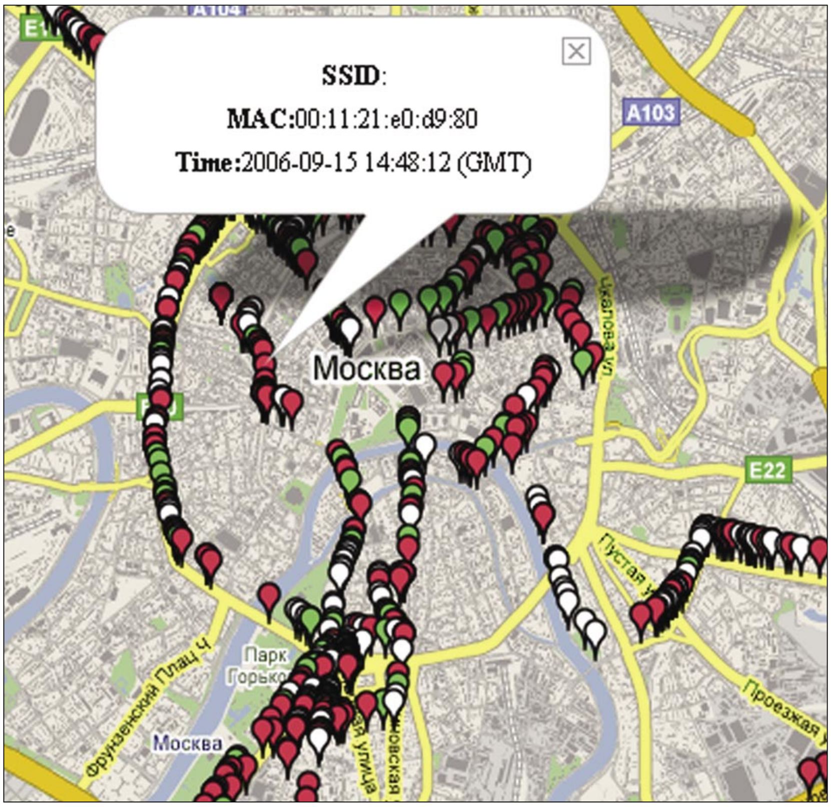
This program will transform received NS. The file and all of the information from it will be visually displayed on a `map`. (*http://www.microsoft.com/streets/ProductDetails.aspx?pid=001*)

## AVTOGIS

This tool is absolutely compatible with Netstambler, and is necessary to start the scanner together with Stumbverter and to connect the GPS-module. With it's help you can find the necessary street, house or any city object. (*http://www.kiberso.com/*)

Of course you will note, that all of the products are commercial, but there are absolutely free-of-charge realizations of such ideas. Wardrivers are self-educated people that have written a huge amount of scripts, allowing the conversion of NS reports into a suitable format. One of them is PHP Stumbler Parder v1.1 (*http://kb3ipd.com/phpStumblerParser/index.php*).

All received information will contain breadth, longitude, MAC address of the removed point, SSID, the information on the channel, and the type of authorization. Personally I prefer to use the *.kml* format.



SSID:
MAC:00:11:21:e0:d9:80
Time:2006-09-15 14:48:12 (GMT)

**Figure 3.** *map*

**Listing 1.** *A special script you can inject your report into the map*

```
GDownloadUrl ("WARDRIVING_REPORT.xml", function (data)
{

   var xml = GXml.parse (data);
   var markers = xml.documentElement.getElementsByTagName ("marker");
      for (var i = 0; i <markers.length; i ++) {
      var point = new GLatLng (parseFloat (markers [i] .getAttribute
                   ("lat")),
                parseFloat (markers [i] .getAttribute ("lng")));
      var marker = createMarker (point, ' <small> <B> SSID </B>: ' + markers
                   [i] .getAttribute ("ssid") + ' <br> <B> MAC: </B>
                   ' +markers [i] .getAttribute ("bssid") + ' <br> <B>
                   Time: </B> ' +markers [i] .getAttribute ("time_gmt") +
                   ' </small> ');
                map.addOverlay (marker);

                // map.addOverlay (new GMarker (point, icon));

}
```

This is what Google Earth service supports and you can use it for Wi-fi mapping. Swing Google Earth Desktop (*http://desktop.google.com/download/earth/GoogleEarth.exe*), *File>Open>*.

We import the report that we find on the Internet. Near us is a hotspot, therefore we have found ourselves on the map, having connected to it. But what to do, if it had not appeared, and there is only the GPS and the module? Well- let's take advantage of our favourite service and program GPS TrackMaker 13 (*http://www.ruslapland.ru/gps.htm*).

If you do not want to spend your own money for gprs for the purpose of pumping maps onto a laptop do all stuff at home. Load GE/GPS and load the maps from the Internet, surf the planned districts for warwalking.

The program will bring the received structures into memory (*temporary*) and the files will saved in *C: \Documents and Settings \ PCname \ApplicationData \Google \GoogleEarth*.

Because we are not connected to the Internet, you can start Google Earth and ignore all the inquiries about connecting to a network – preload the data from there – and on the screen and you will see the cached images in the advance prepared square. For more a more evident perception I recommend KNSGEM (*http://www.rjpi.com/knsgem.htm*).

This program will help *to paint* a habitual map over the present map of the warwalker – to illuminate the found points in various colors, and to paint over zones of a radio covering a certain area or to lead remote lines.

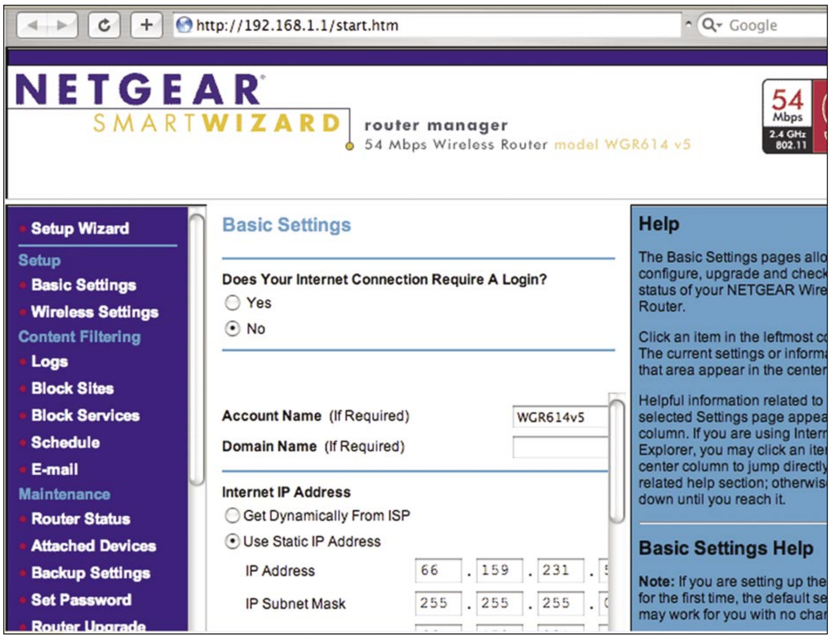
## How to make the wardriver's map accessible

First method on how to make the wardriver's map accessible for everyone on the Internet:

- Register at *http://www.google.com/apis/maps/signup.html*. We will define the size of the future `map`, and after that you will receive a unique ID and a JS code to insert on your host,
- Notice, Google API supports only XML, or modified KML. Therefore we need to use PHP Stumbler Parder v1.1 (*http://kb3ipd.com/phpStumblerParser/index.php*) which allows us to convert the report from NS in XML,
- With the help of a special script you can inject your report into the `map`: see Listing 1.

By the way, such markings can me done via PHP/SQL (*http://www.map-server.com/googlemaps/tutorial.html*) or with the help of special add-ons like GMapEZ (*http://bluweb.com/us/chouser/gmapez/start.html*). The second method if. If you prefer Kismet as wi-fi scanner, you can use gpsmap (with gmap patch *http://www.parknation.com/gmap/*) for mapping:

- Download the gpsmap-gmap-X.X.tgz file,
- Uncompress it by typing `tar zxf gpsmap-gmap-X.X.tgz` (Where X.X is the version number),
- Download the source code for kismet (*http://svn.kismetwireless.net/code/trunk kismet-devel*),
- Change to the kismet-source directory (*cd kismet-devel*),
- Patch the kismet source code (`patch -p0 < ../gpsmap-gmap-X.X/gpsmap-gmap-X.X.diff`),
- Run configure (`./configure`),
- Make gpsmap (`make gpsmap`),
- Copy gpsmap to its desired location (`cp gpsmap /usr/local/bin`),
- Change to the `gpsmap-gmap-X-X` directory (`cd ../gpsmap-gmap-X.x`),
- Copy the index.html file and the mapfiles folder to a webserver,
- After running gpsmap on a gps file copy the output *.js* file to the same folder as the `index.html` file and name it gpsdata.js,
- You also need to get a key for using google maps from google (*http://www.google.com/apis/maps/signup.html*). Insert this key into the top of the *index.html* file in the location of KEYHERE,
- Now hopefully you can see the page and wireless locations in your browser.



Basic Settings

Does Your Internet Connection Require A Login?
○ Yes
● No

Account Name (If Required) WGR614v5
Domain Name (If Required)

Internet IP Address
○ Get Dynamically From ISP
● Use Static IP Address
IP Address 66 . 159 . 231 . 5
IP Subnet Mask 255 . 255 . 255 . (

Help

The Basic Settings pages allo configure, upgrade and check status of your NETGEAR Wire Router.

Click an item in the leftmost co The current settings or inform that area appear in the center

Helpful information related to selected Settings page appea column. If you are using Intern Explorer, you may click an ite center column to jump directly related help section; otherwis down until you reach it.

Basic Settings Help

**Note:** If you are setting up the for the first time, the default se may work for you with no char

**Figure 4.** *Router*

In addition you can convert kismet or kiswin dump into html: *http://www.maco.sk/kismet2html/*

## Local wireless network security analyzation

When you have connected to an unsecured Wi-Fi AP, your IP will be automatically configured and changed based on what is given out by the network. Detect it with ipconfig and try to come through a browser on `x.x.x.1`. The problem is that there can be a special WEB-based control panel, in which there may be a table of rounting that can be configured.

Lame administrators install it with default factory password (admin, cisco, guest). Having gained access to it, you can edit the table of routing and everything that you only dream about. After that I advice you to parse backtracks through vulnerabilities. *Bypass Authefication* or config info watching (remember CISCO bug in `/level/99/show/config`).

```
perl hardware_auditor.pl -s 192.168.0.0
                         -e 192.168.0.100
LOADINC MAC ... ok
LOADING BUGS ... ok
LOADING CREDITS ... ok (default passes
                         db)
```

You can brute force firmware default passwords, or go through authorization as it helps to detect some buggy AP through standard bugs like `/cgi-bin/firmwarecfg` and `/cgi-bin/Intruders.cfg` (in Dlink models): see Listing 2.

As with the initial ip – you can analyse the received network environment for the presence of bugs. NMAP will help with that: for example, scan a range with the open port 139 in order to try a penetration with the `kaht2` eploit:

```
nmap-sT-p 139 x.x.x.0/24.
nmap_po_tochke.png
```

For convenience download NMAP with the GUI the interface – NMAP FE. Of course you can try to find shared resources and exploit the SMB shares it all depends on your mindset.

A famous group, The Hackers Choice (THC) has released a special utility THC-RUT, which people called *the Swiss army knife of wardriving*. It uses several methods to analyze every network: arp lookup, spoofed DHCP request, RARP, BOOTP, ICMP-ping, ICMP address mask request, OS fingerprinting, and fast host detection.

Using vulnerable services (lsass, etc.) not authorized for access, you can intrude into open spaces of a network and steal information, or backdoor computers or to simply spy on their activity. In networks having good channel we actually can place Ddos-boats. We can go further.

## Common attacks in the wireless infrastructure

*The network* `setka1` requires a network key. Type the key, and then click Connect.

### Network key

A network key helps to prevent unknown intruders from connecting to their network. With the help of WEP or WPA keys the admin can organize authentication but there are several methods for breaking these keys.

Standard WEP, is based on RC4 and the application is used very extensively – beginning with the *Hidden ROM* in XBOX, to furnishing the Private Keys in Windows products. Moreover it is used in the Wired Equivalent Privacy portion of `IEEE 802.11b/g`. It consists of the stream cipher RC4 for confidentiality, the CRC-32 checksum for integrity.

Standard 64-bit WEP uses a 40 bit key, which is concatenated to a 24-bit initialization vector (IV) to form the RC4 traffic key.

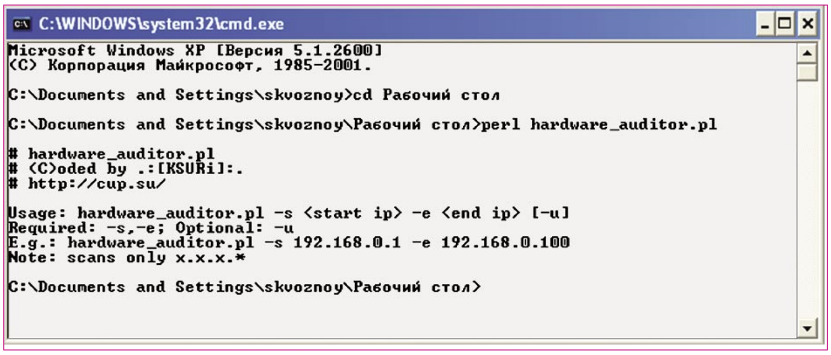
A 128-bit WEP key is almost always entered by users as a string of 26 Hexadecimal (Hex) characters (0-9 and A-F). Each character represents 4 bits of the key. `4 * 26 = 104 bits`; adding the 24-bit IV brings us what we call a `128-bit WEP key`. A 256-bit WEP system is available from some vendors, and as with the above-mentioned system, 24 bits of that is for the I.V., leaving 232 actual bits for protection. This is typically entered as 58 Hexadecimal characters. `(58 * 4 = 232 bits) + 24 I.V. bits = 256 bits` of WEP protection. Methods of cracking:

- Bruteforce,
- FMS attack,
- Korek attack.

The most popular tool for cracking is AIRCRACK – a set of utilities for auditing wireless networks, the tools include:

- Airodump – packet sniffer,
- Aireplay – frames injector,
- Aircrack – analyzator of recieved packets,
- Airdecap – the decoder of received packages WEP/WPA.

The quantity of sniffed packages depends on length of the WEP-key. The received packages will be dumped into IV file, and the analysis of which will be performed by Aircrack.



```
Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.

C:\Documents and Settings\skvoznoy>cd Рабочий стол

C:\Documents and Settings\skvoznoy\Рабочий стол>perl hardware_auditor.pl

# hardware_auditor.pl
# (C)oded by .:[KSURi]:.
# http://cup.su/

Usage: hardware_auditor.pl -s <start ip> -e <end ip> [-u]
Required: -s,-e; Optional: -u
E.g.: hardware_auditor.pl -s 192.168.0.1 -e 192.168.0.100
Note: scans only x.x.x.*

C:\Documents and Settings\skvoznoy\Рабочий стол>
```

**Figure 5.** *xek ksur*

For breaking a 64-bit key you will need to intercept up to 200,000 IV-packages, 128-th – up to one million. Sometimes one hour is required to crack the key, sometimes – less than ten minutes. By the way, according to the FBI who performs a lot of educational tests for penetration, use a traffic generation utility that will boost the process, and you can crack WEP in 3 mins, but remember that 802.11 standard allows us to create 152-bit WEP keys, against 64/128 bit, the procedure used for breaking it is similar, but longer. Start Airdump:

- We specify the wireless network adapter,
- Type of your network adapter: *Orinoco*/*Realtek*, *Aironet*/`Atheros`,
- Scanned channels. Unfortunately the precise channel to us is not known – we put 0 (scanning of all 14),
- We set a name of a dump-file of all intercepted packages – gemashaloma (hello poncheg `:D`),
- Definition of formed packages WEP IVs – we press `Y`.

The process has run, the program displays the AP's MAC-address, the MAC-address of the connected client, and the identifier of a network.

The speed of process depends on the speed of the traffic exchange between the AP and client. To raise it, as I told you, it is possible to boost a huge amount of traffic with the command: `ping-t-l 31337 IP _ wlan`.

Stop process with [*Ctrl*+*C*], and start processing the received IV's file in Aircrack:

```
aircrack.exe-b AP's_MAC-n 64/128-i 1
                         gemashaloma.ivs.
```

Flag `-b` means that we work with a AP's identificator `(-b bssid`: MAC address, Access Point), for more detail about other options in Aircrack you can learn from the program's manual or the help option.

After some expectation my mood has improved – *KEY Found*, in brackets the long-awaited password *trabzon* was seen. For a similar process it is possible to apply a new utility Weplab (*http://weplab.sourceforge.net/*) or chok-chok that was widely discussed on Netstambler's BBS. Realize that some kinds of attacks: bruteforce with dictionary phrases are using a static FMS attack and so on.

You have probably paid attention to the WPA-standard (Wi-Fi Protected Access) if you have some wardriving penetration testing skill. It was created as technologists of the world realized all of the vulnerabilities of the previous standard. It is more secure as it allows the request of the name and the password of the user, to check them with registration records in a database of a authorization server, and only then to make a decision on the admissionto the network. Advantages of WPA:

- Dynamic generation of keys,
- Precise distribution of the cryptographic sums by means of technology MIC (Message Integrity Check), that does not give in to false package introduction,
- Integrated enciphering under standard AES.

If in the column *Encyption* of your wireless scanner you notice the WPA label, don't worry. Processing of WPA cracking consists of the reception of IV packages of the connection, their analysis and decoding. As for a file-report it is required to use CAP, instead of IV. For this purpose in airodump there is the option on the last question *Only write WEP IVs (y/n)* is answered *is not present*. The procedure for IV package sniffing can be caused by deauthorization frames. Unfortunately Windows does not allow to the use of it, but you can use Perl script like `MAC_flood` for it. Alternatives are: void11 (Linux):

`void11_penetration-s CLIENT MAC-B ATTACKED MAC-D wlan0`. We shall pretend, that you managed to force the client's reconnections, sniffed the initialization vectors from the client to the AP and have have been intercepted and put into a file gema.cap. We shall feed that file to Aircrack: `aircrack.exe-p 4-a 2-w passes gema.cap` (passes – it's necessary to have special dictionary of passwords for bruteforce).

On the duration of the bruteforce procedure you will notice that it is much longer then WEP-cracking, sometimes it will be more then 2 hours. Also in W2K there are no mechanisms for WPA authorization (unlike XP) – therefore for our own convenience and for the convenience of Windows 2000/98/ME we will use WPA Assistant (*http://www.wirelesssecuritycorp.com/wsc/public/WPAAssistant.do*) a freeware programm, which will help you connect to networks with WPA-PSK.

**Listing 2.** *Usual router's configuration file*

```
# Copyright (c) 2002 Atheros Communications, Inc., All Rights Reserved
# DO NOT EDIT -- This configuration file is automatically generated
magic Ar52xxAP
fwc: 34
login admin
DHCPServer
Eth_Acl
nameaddr
domainsuffix
IP_Addr 10.0.0.30
IP_Mask 255.0.0.0
Gateway_Addr 10.0.0.1
RADIUSaddr
RADIUSport 1812
RADIUSsecret
password IntrudersTest
passphrase
wlan1 passphrase AnewBadPassPhrase
# Several lines removed.
```

Sometimes the method of MAC spoofing is very usefull. The filter mode of MAC addresses provides a connection only from PC's entrusted in the special list. But in any case you are likely to detect an identifier of the network.

### SMAC

This utility isfor changing the MAC on a Windows 2000/XP. Enter the new Spoofed MAC address and click *Update MAC*. Sometimes it is impossible to enter the network with it, as the already authorizated real MAC-owner has connected to it. For this purpose there are fighting methods, like deassociation frames sending, moreover, you can make some good traffic generation in the network in order to boost for example the sniffing process. *www.klcconsulting.net/smac/*

### VOID11

This idea consists of disconnecting remote clients with special frames from the AP. Of course after this they will try to renew the connection and a lot of traffic will be generated. This sort of long attack can do much harm to the administrator or even break his business. As the network will absolutely be inaccessible for some time and on the monitors in the tray will be shown *Wireless Network unavailable*. Such situations are the result of DDOS attack on the wireless network that can be organized by frame injection.

### Another:

*MAC-flood* – fast sending of large quantities of generated MAC-addresses *http://home.jwu.edu/jwright/perl.htm*

Use: $perl *macfld.pl*-c 1000-u 10000 (c – number of packages, u – timeout). More on *http://www.wirelessdefence.org/Contents/Void11Main.htm.*

*FATA Jack* – sending of massive amounts of frames, that can freeze all network traffic and halt work. *http://www.wi-foo.com/soft/attack/fata_jack.c.*

## LEAP cracking

In corporate networks administrators will sometimes use hardware with a special type of authentication. For example, Lightweight EAP (LEAP) is a protocol, developed by CISCO Systems in order to prevent most types of attacks. It is very similar to bilateral Challenge Authentication Protocol (CHAP) but in any case there is an opportunity for bruteforce cracking. Another method of LEAP detection is Wireshark (former Ethereal) using – *REQUEST, EAP-CISCO Wireless* (*LEAP*) on the sniffed interface specified. Joshua Wright – famouse researcher in computer sphere created a special program ASLEAP (*http://asleap.sourceforge.net/*)which can intercept network packages at a repeated connection of the client and bruteforce the passwords. If you do not have such tools in your arsenal, use special script on PERL – anwrap (*http://www.securiteam.com/tools/6O00P2060I.html*), you need the Active Perl Library for it to be installed also. Anwrap:

```
perl anwrap.pl <users.txt> <passes.txt>
<log.txt>.
```

Analogue with use of a program from Van-Hauser:

```
THC-leap cracker:
./leap-cracker-f passes.txt-u users.txt
```

*Concerning ASLEAP*: it works in two modes, offline (search already sniffed packets) and real-time (capture of packages and the subsequent search). For it to work in real time the accessible network interface is required by you, to define which is possible to start the program with `-D` flag.

`./asleap-i` any-`w` gemababy (record in a file the pcap-report)-t 3 this will allow the process to begin the interception of packages using any accessible interface with a record in a pcap-file with a 3 seconds timeout.

`./asleap-r gemababy-W` passes (uses the files of AiroPeek NX or pcap-reports.

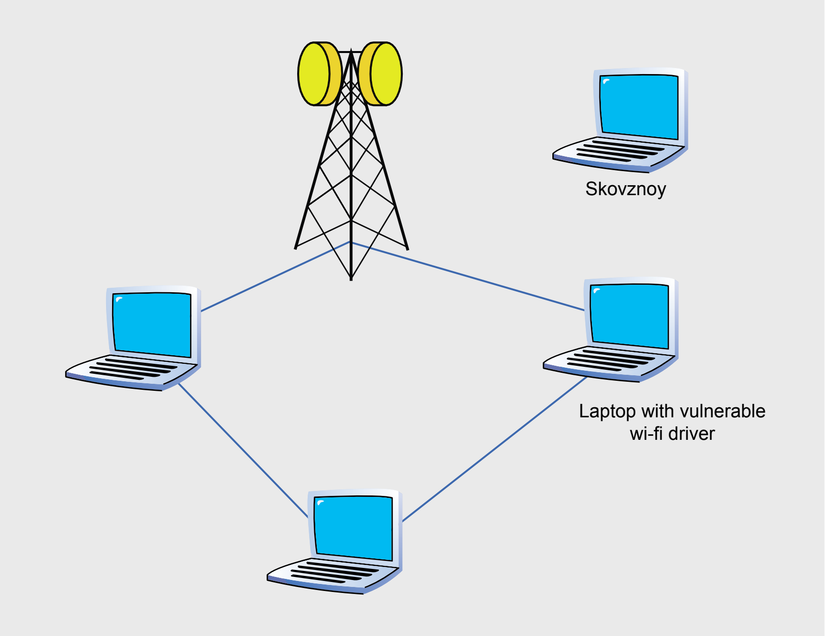


**Figure 6.** *Fuzzing*

The difference from *cable* hacking to Wi-Fi hacking is that Wi-Fi hacking gives a greater freedom of actions. First, the method of the wardriver's location detection is much more difficult, than if you use your usual cable connection. In fact for this purpose it is required to involve a whole Security group with notebooks on your searches (triangulation method). A signal to alarm them that there can be a sudden connection of the new device that has just come up on air. Skilled administrators will detect yours (new) MAC in logs.

On September, 3rd, 2006 Johny Cashe has described essentially a new attack – using the vulnerability of drivers it is possible to execute unauthorizated code. Some vulnerable products:

```
APPLE:MacOS X 10.4
INTEL:Intel PRO/Wireless 2200BG
INTEL:Intel PRO/Wireless 2915ABG
INTEL:Intel PRO/Wireless 2100
INTEL:Intel PRO/Wireless 3945ABG
(w22n50.sys, w22n51.sys, w29n50.sys,
w29n51.sys)
```

LORCON – a new utility which helps to search for mistakes in drivers for wireless technologies and the standard 802.11x

```
skvoz@cup # ./lorcon -c 1 -d 80 -t 00:
0C:6E:4F:A2:00,
```

where `-c` – number of channel (default 1), `-d` *listening port*, `-t` – MAC of buggy device.

```
Finding channel and signal strength ...
DONE!
Preparing shellcode ...
Sending attack ...
Waiting for response
..... Got shell!
```

It is very useful as you can organize stealth attacks. Nobody can detect you because the time period of stumbling in order to detect the wireless infrastructure is minimal. So you shouldn't be afraid of Wireless Triangulation Systems at all. ●