PV018 – term project
WiFi security survey in Brno

Marek Kumpošt

My term project deals with WiFi security (the use of WEP encryption) and provides comparison between the results from measurement being performed a year ago when I was working on my master's thesis. I'll also provide the results from 2003 that I've been given while cooperating with security specialists from Autocont. The aim of this project is to determine whether the situation in the field of WiFi security aspects and (mainly) the use of WEP (Wired Equivalent Privacy) becomes better over these three years or stays on the same level.

Few words about the equipment used for detecting 2,4 GHz WiFi signal:

I used my laptop equipped with Intel(R) PRO/Wireless 2200BG Network interface controller which supports up to 54 Mb/s transfer speed.

Software used for monitoring was NetStumbler 0.4.0 – a tool for Windows that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. This software is primarily used for WLAN administrators to get them the ability for verifying their wireless networks from the coverage point of view. NetStumbler can also be used for finding WiFi signal and for capturing some basic information about detected signal. That is the mode of operation that we were using while moving around Brno and trying to find various WLANs. The information that NetStumbel can acquire is:

- SSID (Service Set Identifier) information about Access Point (AP)
- AP MAC address
- Channel which is used for data transfer (1-11)
- Transmition speed
- AP or in general NIC (network interface controller) vendor
- Type of detected network (AP or P2P)
- Encryption state (no encryption or WEP enabled)
- Some information about signal and noise level
- Time information when the network was detected
- GPS information if the respective device is connected

Information for the purposes of this term project was mainly the state of WEP encryption and SSID settings. I will also mention the AP vs. P2P rate and manufacturers of detected APs.

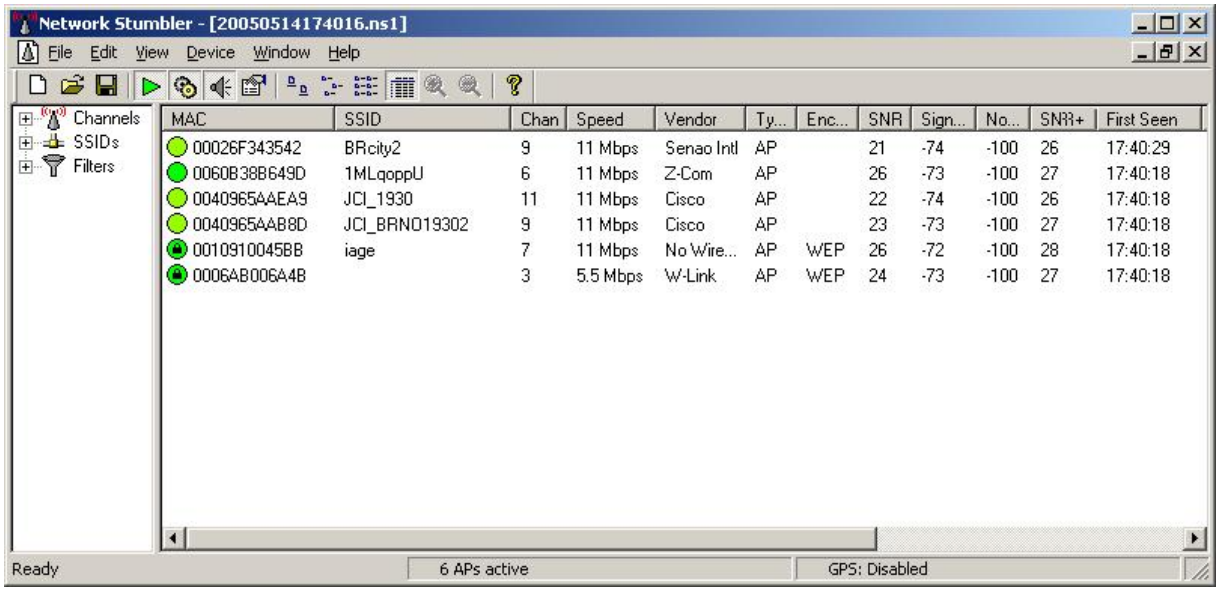


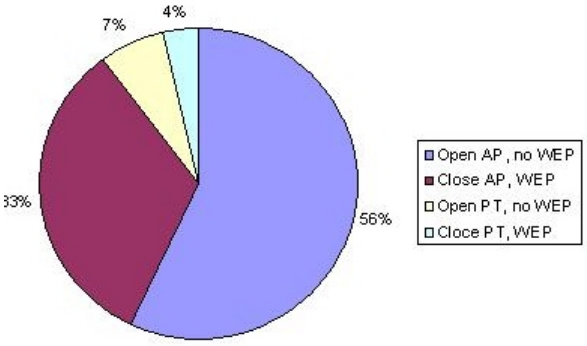
Figure 1: NetStumbler main window

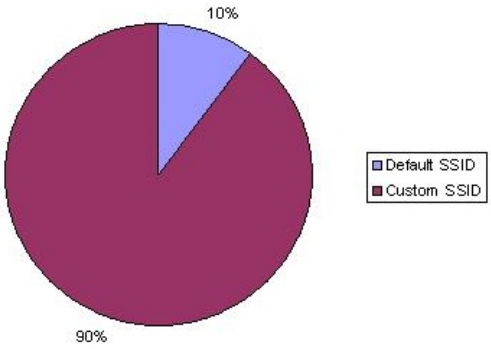
The first measurement that I was participating on was in May 2004 and has been done in cooperation with security specialists from Autocont. We were equipped with two notebooks one special directional antenna and GPS receiver (so that we had the information about the exact location). This information was afterwards used for marking detected WLANs into the map (but this will not be included in this report).

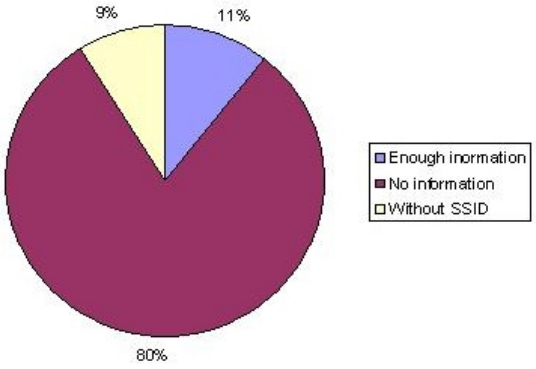
Second measurement was done in May 2005 and I did it alone. I used my laptop and public transfer to move around the town.

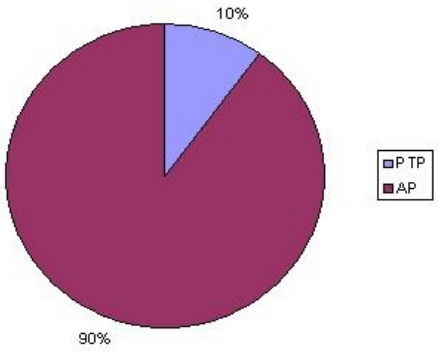
Weather conditions, which may have negative impact on wireless signal broadcasting, were in both cases quite good (no rain, snow :-) or fog).

Data from May 2003 (**137** WLANs have been detected, no information about the experiment duration):

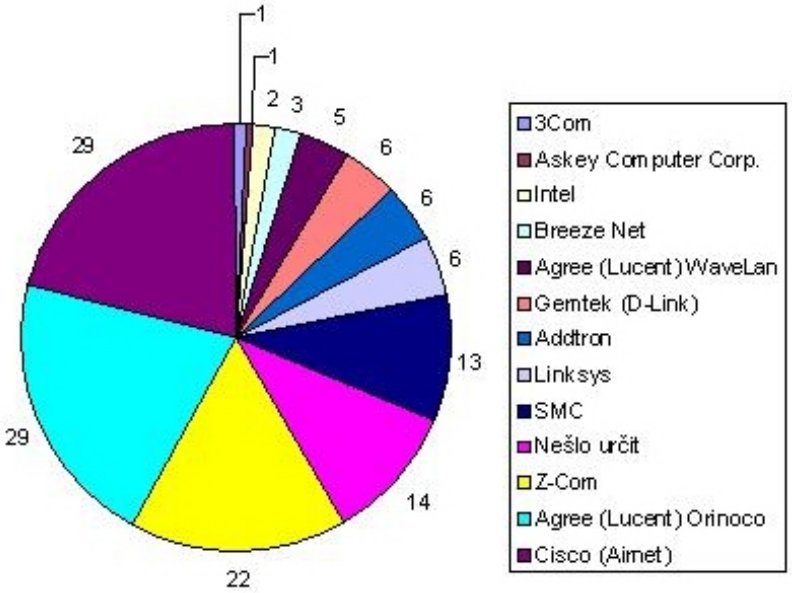




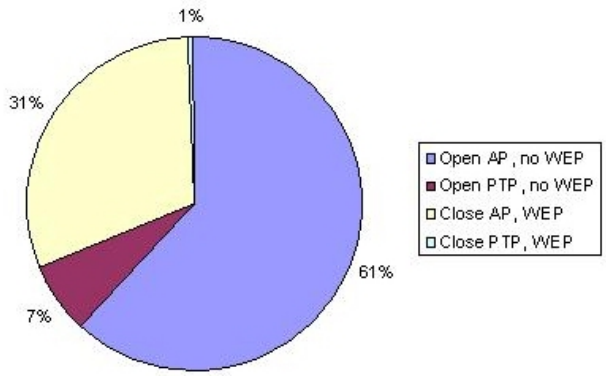


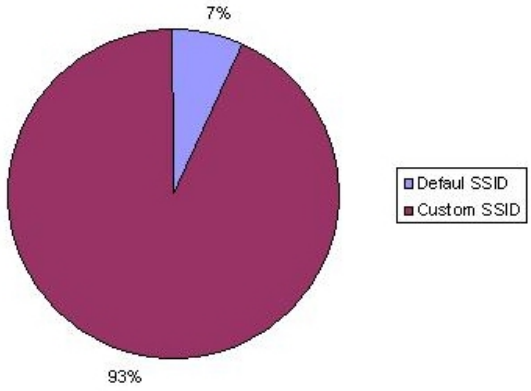


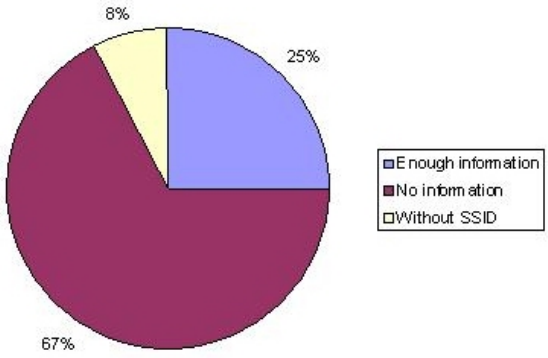
Amount of information in SSID about the owner of WiFi Access Point.

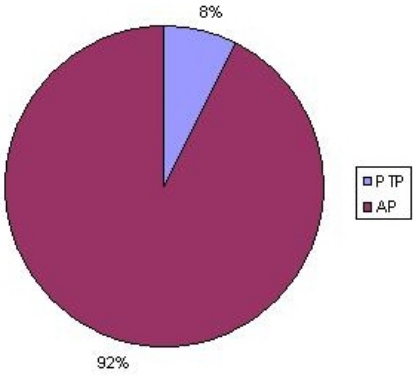


Data from May 2004 (**146** WLANs have been detected within 2 hours 30 minutes):

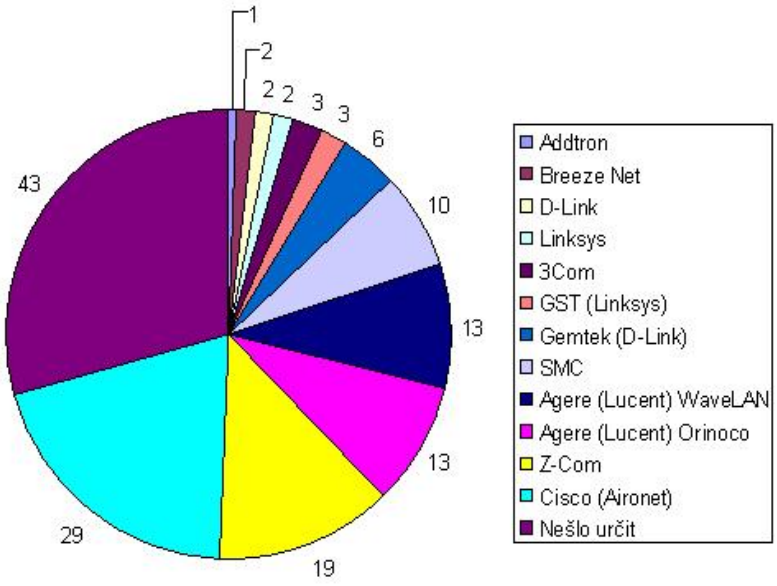




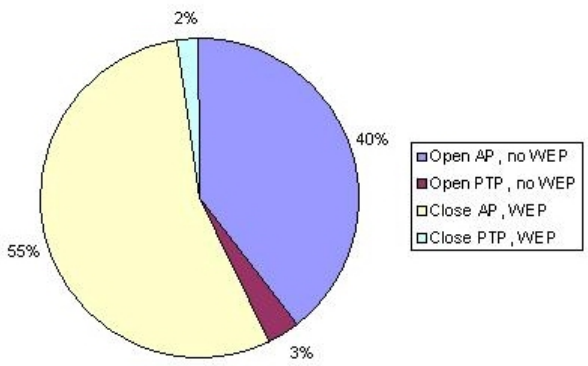


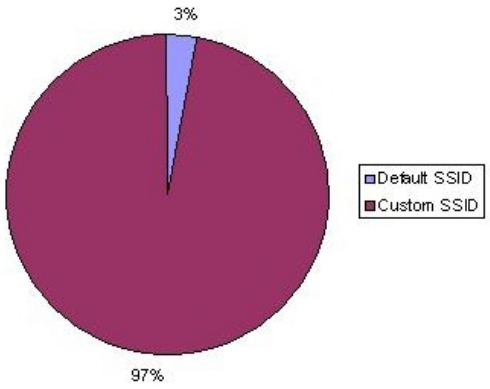


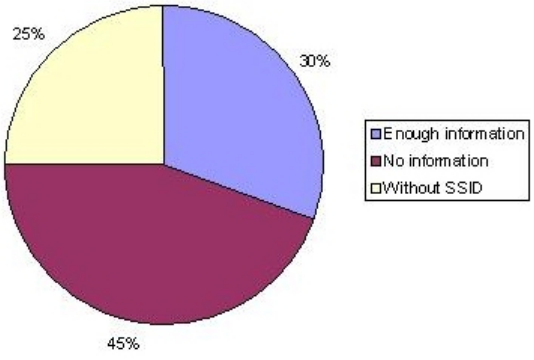
Amount of information in SSID about the owner of WiFi Access Point.

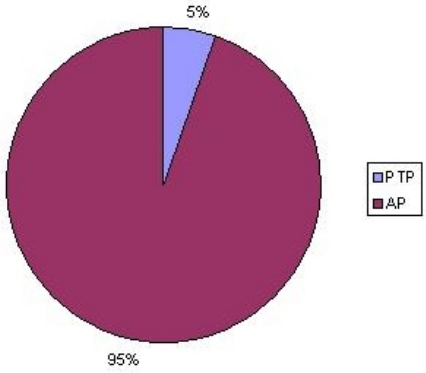


Data from May 2005 (**220** WLANs have been detected within 2 hours 30 minutes):

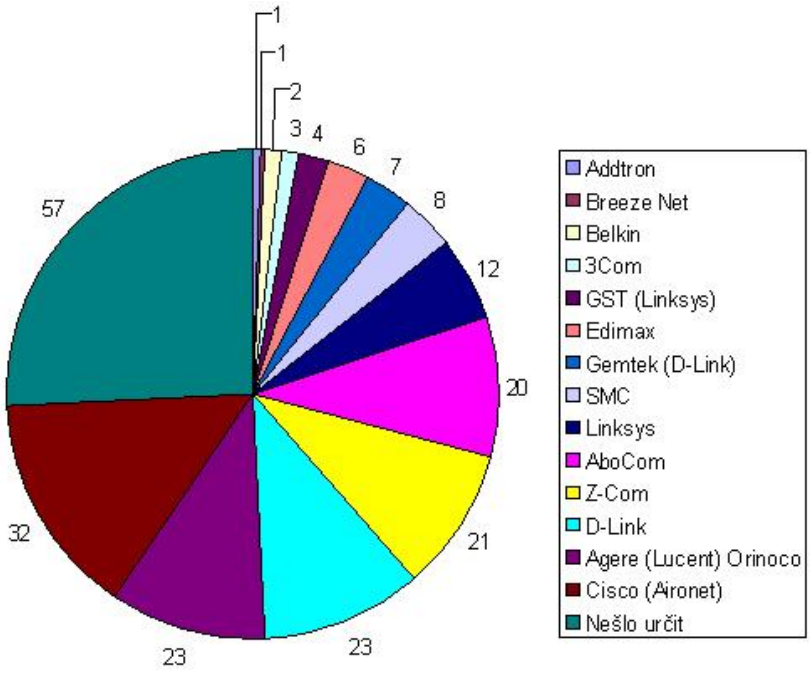








Amount of information in SSID about the owner of WiFi Access Point.



Here I would like to conclude the results and summarize some of them in a table.

The very first observation which should be detected while going through the result is the high increase of use of Wi-Fi networks over the last year. In May 2004, 147 wireless devices have been detected within 2 hours and 30 minutes. In May 2005, 220 devices have been detected within the same period of time. This means 50% increase.

Now, let's turn our attention to some security aspects which are the main item of interest in this project.

	May 2003	**May 2004**	**May 2005**
Open AP, no WEP	56 %	61 %	40 %
Open PTP, no WEP	7 %	7 %	3 %
Close AP, WEP	33 %	31 %	**55 %**
Close PTP, WEP	4 %	1 %	2 %

Tab 1.: The use of WEP encryption

	May 2003	**May 2004**	**May 2005**
Default SSID	10 %	7 %	3 %
Custom SSID	90 %	93 %	97 %
Enough information	11 %	25 %	30 %
No information	80 %	67 %	45 %
Without SSID	9 %	8 %	25 %

Tab 2.: SSID setup and the amount of information in SSID

Table 1 shows the state of use of WEP encryption which makes Wi-Fi communication more secure (we are now not considering the weaknesses of this encryption scheme). The use of this mechanism increased rapidly with respect to the level of use in last two years.

The first part of table 2 shows SSID setup in detected networks. The results show that customization of this setting is increasing. On the other hand the amount of information in SSID (second part of table 2), which should be used to detect the owner (and therefore possible purpose) of the network is also increasing. The attacker is able to successfully predict the purpose of detected network. The best recommendation is to turn off so called SSID broadcast to disable the attacker from exploiting this information.

So finally, the use of WEP encryption is increasing but is still at quite low level. Maybe the new standard (802.11i/WPA2) will make the use of encryption more common...