Final assignment Hackers Hut: Warbiking the TU/e

Bas Kloet (461462), Christian Luijten (496505),
Bram Senders (511873), Paul van Tilburg (459098)

September 24, 2004

For the final assignment of the course Hackers Hut at Eindhoven University of Technology, we chose to do some wardriving on the university's campus.

Since wireless technology is becoming increasingly popular, it is being used by people who don't realise the added security threats.

The places where technology hits first are — among others — universities. Many people are confronted with technologies they aren't used to. In this situation, errors can be made in the configuration and usage of wireless network technology, making them vulnerable to attacks.

Our goal is to make an inventory of wireless networks at the campus and to check if they are configured correctly to work with the central security system already used in the Auditorium and on various other places.

We installed the software package Kismet[1] on a laptop with a wireless network card and a GPS[2] receiver. Then we packed the laptop in a backpack and jumped on our bikes.

We started at the EHoog building and the route we followed is, globally, Hoofdgebouw, Auditorium, via the Limbopad to Vertigo, Matrix, Helix, TNO Chemistry buildings, a tour around the skating dome, Twinning Center, Multimedia Paviljoen, Traverse, Laplace, WHoog, W-Hal, Hoofdgebouw, ELaag, EEg and back to the EHoog building. This route is displayed — along with the networks found — in Figure 1.

[1] See `http://www.kismetwireless.net/`
[2] Global Positioning System

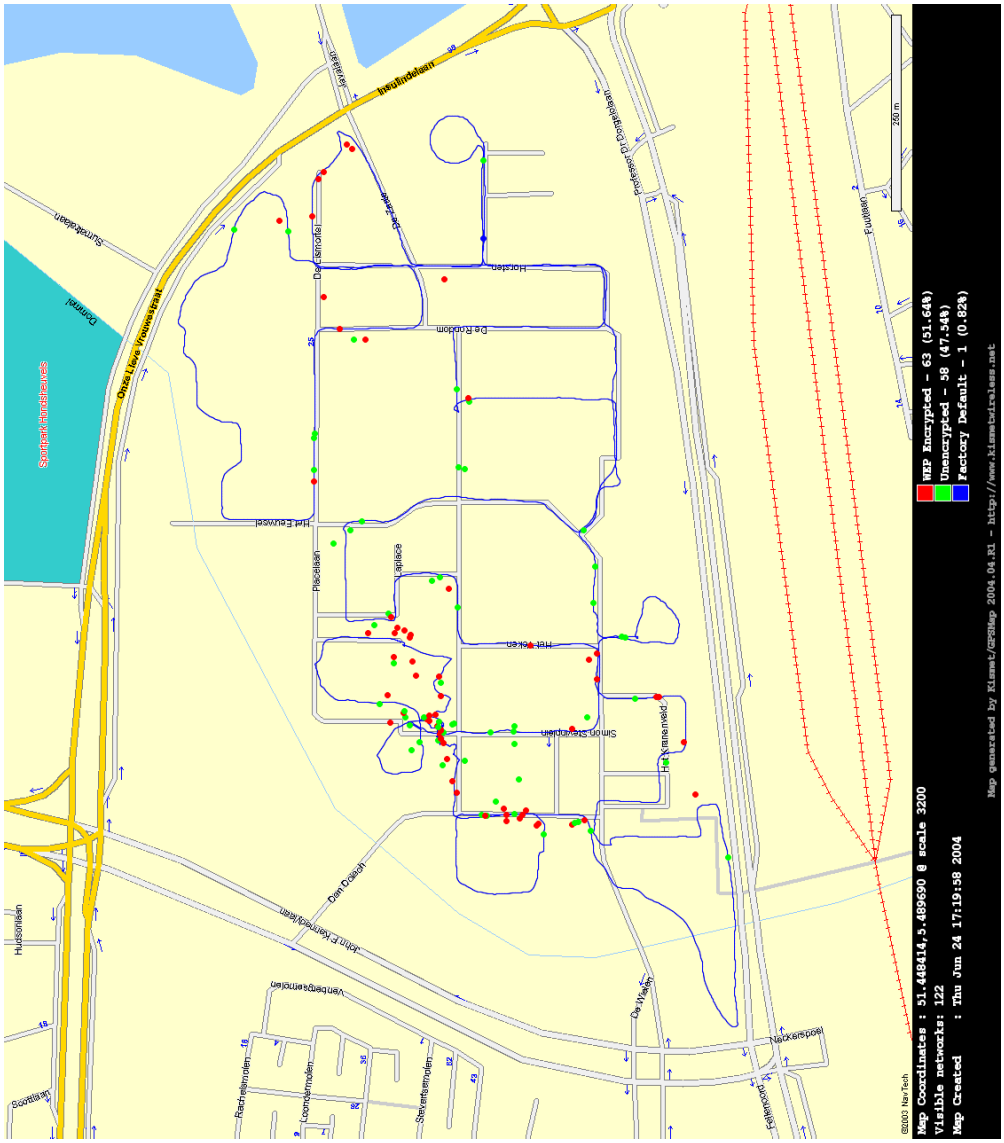

Figure 1: Warbiking route

Information Kismet gathers

Every moment Kismet receives a packet from an unknown network, it stores information about that packet. If it is a packet of an already known network, the known information may be extended.

Kismet stores information like the SSID[3] and hardware address, network type (ad-hoc, infrastructure, probe), used network standard (802.11a/b/g), network speed, whether the packet is encrypted or not, the time and date, if a GPS receiver is available and also the exact coordinates where the reception took place. Using these coordinates a map of the area can be made.

Results

During this ride on 24 june 2004, we found 116 active wireless network interfaces. Of these interfaces, 33 use the SSID 'tue' and are of type 'infrastructure'. Part of these are the access points the TU/e ICTServices installed in the Auditorium and on various other places earlier this year. They can be recognized by their Info-field which starts with 'ap-', followed by the abbreviation of the building and the floor number, then another dash and a unique number. There are 32 of these access points and they all use PEAP[4] for encryption and authentication. PEAP authenticates wireless LAN clients using an encrypted SSL/TLS tunnel between the client and the authentication server. No other data is routed by the access point before the client is authenticated.

We received 34 more packets which were in fact probes (type 'probe') of other wireless network cards trying to find a network.

After filtering out these, 49 networks still remain. We went back to some of them to do some extra testing. A very peculiar name that drew our attention was the 'labtuin'. It is a 54MBit access point, uses no WEP[5] and should be an easy target. However, when we came there, it was total radio silence, we could not find it anymore. Probably the users were all on holiday and the device was turned off.

So we looked for another open network. One of these networks has the SSID 'EESI3B', and is located in the Laplace building. We sat down in the grass in front of the EHoog building and started scanning.

DHCP requests for a private network came in, so we decided to go a little bit inside. We set the MAC address of our network card to 00:00:00:00:DE:AD:BE:EF to avoid being detected with a TU/e-registered MAC address and did a DHCP request. The DHCP server returned some 192.168.2.0/24 address with which

[3] Service Set IDentifier

[4] Protected Extensible Authentication Protocol, developed by Cisco, Microsoft and RSA Security

[5] Wireless Equivalent Privacy, encryption method often used on wireless networks

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-06-28 15:10 CEST
Interesting ports on 192.168.2.1:
(The 1652 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
1723/tcp open  pptp
3306/tcp open  mysql
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 144.921 days (since Wed Feb  4 16:05:08 2004)

Nmap run completed -- 1 IP address (1 host up) scanned in 27.328 seconds
```

Figure 2: Output of `nmap -O -sS 192.168.2.1`

we could reach a webserver at 192.168.2.1 which we found using nmap[6] (See Figure 2).

It was very slow, but had some links about inventory on the main page. Sadly, these were links to TU/e network addresses which we couldn't reach because we got a local address without a working route to the outside.

Other open services were SMTP[7], which can for instance be used to send out spam anonymously.

Conclusion

We can conclude that getting into the network seems very easy at first sight, but if one really tries to get in there actually are some obstacles. The networks that we detected that were open, were also not very heavily used at that moment. To be able to get inside these networks however, more traffic is needed.

Attached are some images we could generate out of Kismet's gathered data: All detected networks along with their signal strength (Figure 4), all unencrypted (at least not encrypted by WEP) networks projected on a map of the campus (Figure 5), and an interpolated view of the wireless coverage (Figure 6). Delivered seperately is the output of Kismet.

An example of the information provided by Kismet is given in Figure 3. The

[6] See `http://www.insecure.org/nmap/`
[7] Simple Mail Transfer Protocol

Amount	Type	Comment
33	TU/e access points	Assumed safe
34	Probes	Not of use
49	Other networks	Interesting
53	No WEP	
8	No WEP, infrastructure	Networks *22*, 60, 61, 81, *86*, 89, 103, 111

Table 1: Summary of detected networks

```
Network 1: "tue" BSSID: "00:0D:28:DD:60:5C"
  Type     : infrastructure
  Carrier  : 802.11g
  Info     : "ap-hg4-2"
  Channel  : 06
  WEP      : "Yes"
  Maxrate  : 11.0
  LLC      : 2696
  Data     : 41
  Crypt    : 31
  Weak     : 0
  Dupe IV  : 0
  Total    : 2737
  First    : "Thu Jun 24 14:11:36 2004"
  Last     : "Thu Jun 24 14:54:58 2004"
  Min Loc: Lat 51.446243 Lon 5.483728 Alt 201.300003 Spd 0.057539
  Max Loc: Lat 51.449974 Lon 5.488378 Alt 472.890015 Spd 9.919726
```

Figure 3: Example output of Kismet

first line shows the SSID and the hardware (MAC) address of the network interface. There is an Info field, which can in case of the official base stations be used to locate them ('ap-hg4-3' is an access point in the main building, floor 4, number 3). The WEP field is "Yes" which indicates that WEP is used for encryption.

In total, *116* networks have been found, which are tabulated in Table 1. The numbers of the two networks that got extra examination are emphasized, more information about these can be found in the attached Kismet output.

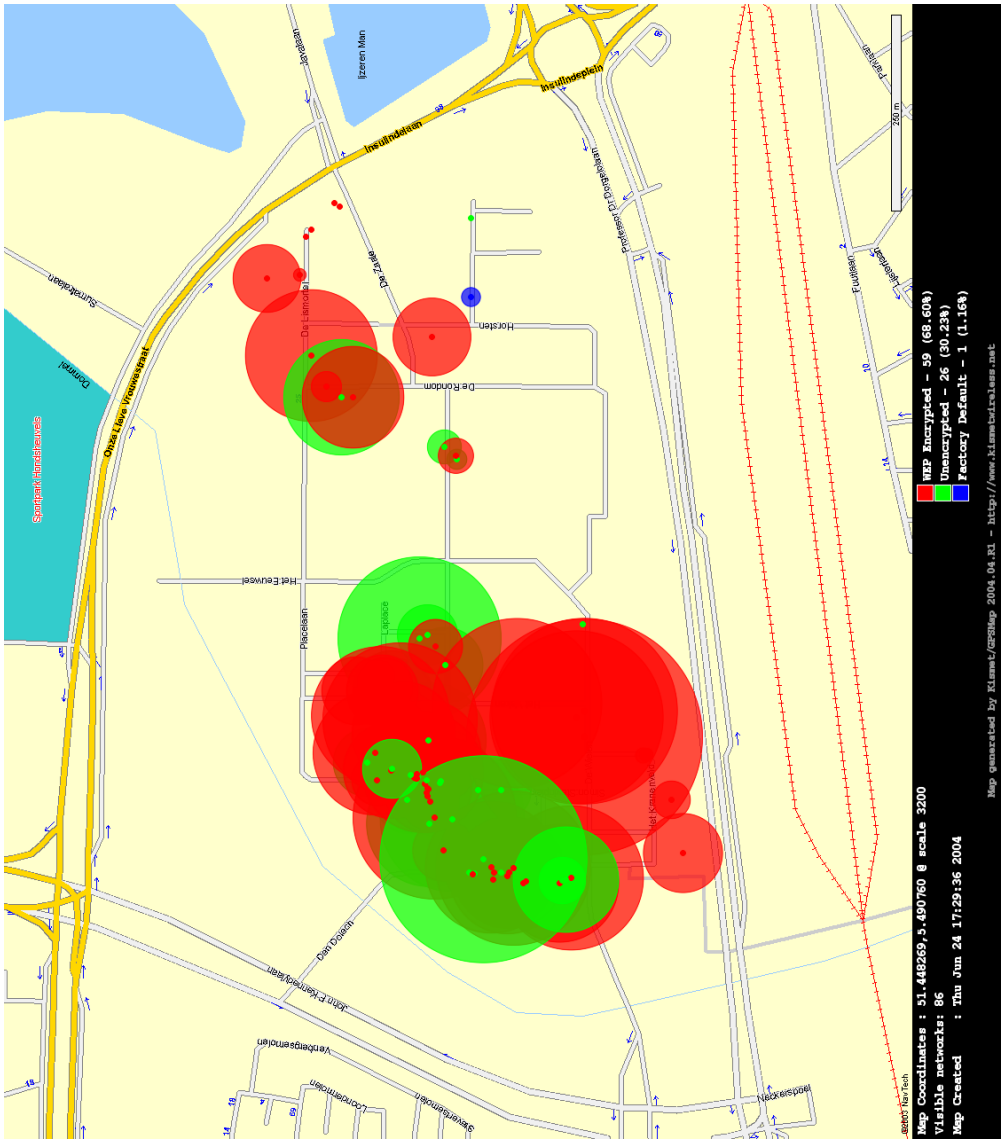

Figure 4: Detected networks

Figure 5: Unencrypted networks, projected over campus image

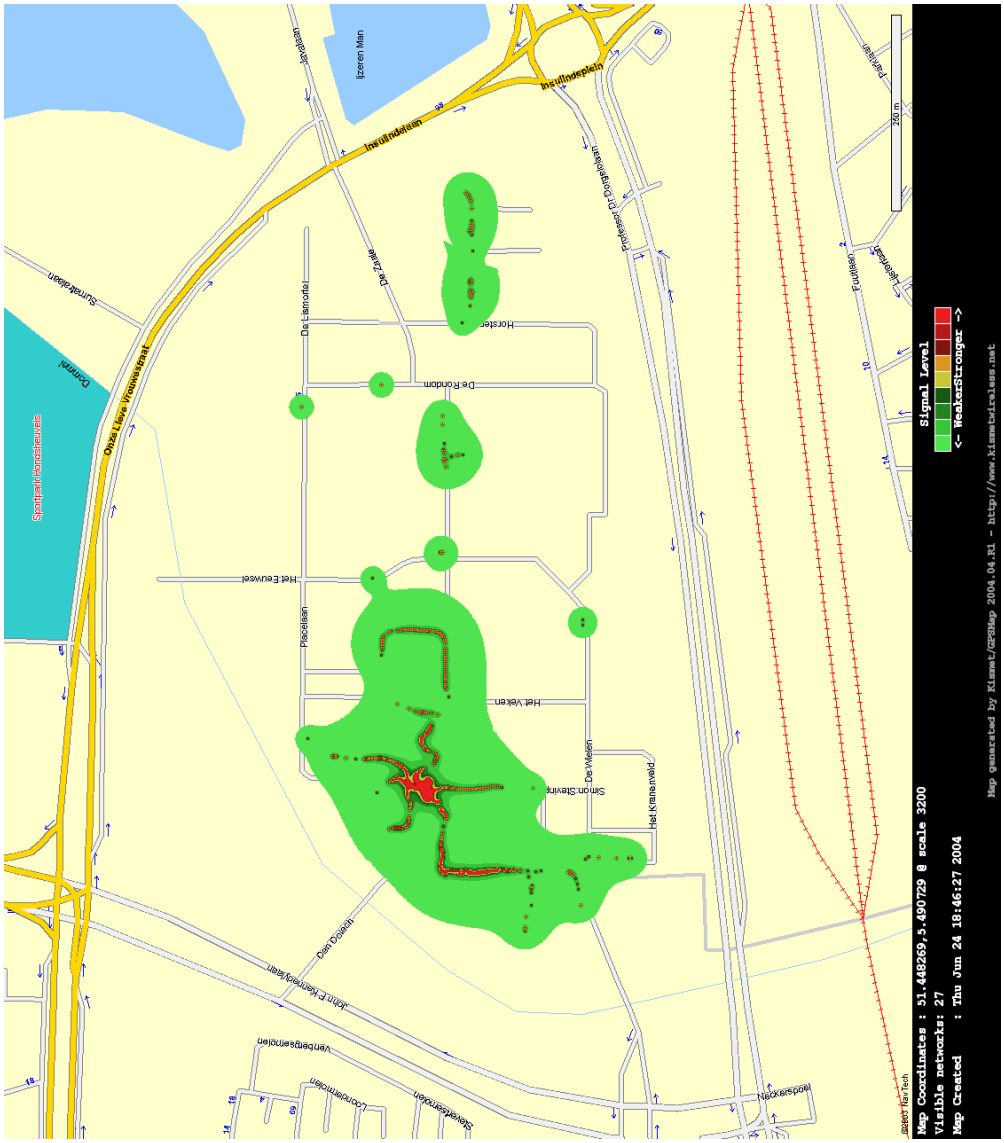

Figure 6: Interpolated coverage