Tracking people using Bluetooth
Implications of enabling Bluetooth discoverable mode

Martin Pels, Jelmer Barhorst, Maarten Michels,
Remco Hobo, Jeffrey Barendse

University of Amsterdam

Revision 1.3 – 5th June 2005

Abstract

Since a few years Bluetooth has been implemented in a broad range of devices. Many of these devices are set in discoverable mode. Since Bluetooth devices can be uniquely identified using their MAC-address it is possible to track the movement of a Bluetooth device, and therefore the person carrying it, provided that discoverable mode is enabled on the device. Using Bluetooth equipment with extended range we have performed two tests to investigate the possibility of tracking large groups of people carrying Bluetooth devices over a large geographical distance. The results of these tests are presented in this document. Subsequently, implications of these results on the field of privacy invasion and the spreading of Bluetooth-enabled viruses are discussed.

Preface

This report is made on behalf of the University of Amsterdam (UvA) and the Intrusion and Detection Systems class. It is the result of a research project we conducted over a period of four weeks in May 2005.

Acknowledgements

We would like to thank the University of Amsterdam for supplying the Bluetooth dongles and the omni-antennas we used for our tests. We also would like to thank Maarten Carels and Jaap van Ginkel for their guidance and advice during the project.

Contents

Chapter 1

Introduction

Since a few years Bluetooth has been implemented in a broad range of devices. Bluetooth makes it possible to communicate between devices over a short distance. Just like a network card in a PC these devices have a number aswell, the Media Access Control (MAC) address. With this address it is possible to identify the device, and to find out which manufacturing company has made the device. This can for example be a phone of the brands Nokia, Sony Ericson etcetera, or a computer of the brand Apple. Note that the type of the device is not part of the MAC-address. Still, it is possible to identify device-types till a certain extend, because most devices of the same type also have an address that only differs in the last few digits.

According to the specifications of Bluetooth it is possible to communicate within a range of 10 meters with other Bluetooth devices [1] [**?**]. It is however possible to communicate over a much larger distance using the right equipment. Knowing this we started a project to see if we were able to track people over a large distance. This report is the endresult of this project.

The research described in this report involves storing information on Bluetooth devices and deriving conclusions on the movement of people. This information is privacy sensitive and may be subject to possible misuse. Since it was impossible to ask the owners of the Bluetooth devices that were scanned for permission to use this information, we have only conducted passive tests. Further more, all privacy sensitive information gathered during the research period has been destroyed after the completion of the research.

This document starts with a technical description on Bluetooth's inner workings. After that the details of the research we performed are discussed. Chapter 4 presents the results of our research. Finally, the document ends with a conclusion and some suggestions for future research.

[1] See section 2.4 for more information.

Chapter 2

Bluetooth

2.1 Introduction

Bluetooth is an open specification for wireless short-range communications of data and voice between (mobile) devices.[2] It specifies how mobile devices like phones, computers and PDA's interconnect with each other. The first generation of Bluetooth permits exchange of data up to a rate of 721 Kbit + 56 Kbit/3 (voice channels) per second, even in areas with much electromagnetic disturbance. It transmits and receives via a short-range radio link using a globally available frequency band. It uses the unlicensed 2.4 GHz Industrial, Scientific, Medical (ISM) band.

The Bluetooth wireless technology was developed by the Bluetooth Special Interest Group (SIG) formed by Ericsson, Intel, and Nokia as a replacement for cable and infrared connections for mobile devices. The SIG was formally announced on May 20, 1999 and later joined by many other companies as Associate or Adopter members.[3]

2.2 Transmission protocol

Bluetooth radio uses the very crowded 2.4 Ghz ISM band. Devices like cordless phones, microwave ovens, garage door openers and baby monitors al make use of the same band. This results in lots of noise on this band. Bluetooth uses a frequency hopping spectrum technology to handle this noise[1]. The 2.4 Ghz ISM band is divided in 79 separate channels of 1 MHz each (2.402 to 2.480 GHz).

The Bluetooth radio transmission protocol hops 1600 times per second. This minimizes the exposure to noisy channels. This hopping interval also enables the possibility to discard bad voice packets without interfering the voice conversation. Bluetooth also uses Forward Error Correction (FEC) of data packets, so bad packets are often recoverable on a noisy channel without retransmission. Bluetooth uses a master-slave structure. The ID of the master is used to algorithmically generate a unique frequency hopping pattern. Slaves utilize a clock offset parameter to synchronize their patterns into alignment with the master.

Besides frequency hopping Bluetooth also makes use of Time Division Duplexing (TDD). Transactions are divided into dedicated time slots for the master

and the slave. A complete transmit/receive cycle between the master and the slave is called a frame. A frame is divided into 625 microsecond slots. Bluetooth can aggregate slots in one direction of the transmission (i.e. asymmetric transmission). This eliminates turnaround time and reduces packet overhead, because the slave can acknowledge a received slot per aggregation of slots instead of each slot separate. Bluetooth supports 1/1, 1/3 and 1/5 framing. For example, 1/3 means a aggregation of 3 slots with the master information and an acknowledgement of the slave in 1 slot. The maximum capacity of Bluetooth framing is 712Kbps (1/5 framing).

2.3 Discovery

The discovery and link management between Bluetooth devices is described in the Generic Access Profile (GAP)[8]. The discoverable mode of a Bluetooth device is described in the GAP. A Bluetooth device shall be either in non-discoverable mode or in a discoverable mode. When a Bluetooth device is in non-discoverable mode, it will not enter the INQUIRY_RESPONSE state. Other devices can't find this device in non-discoverable mode with a simple response request. The general discoverable mode is used by devices that need to be discoverable. The purpose is to respond to a device that makes a general inquiry (inquiry using the GIAC). Devices that are in non-discoverable mode can still be discovered by a brute force MAC-address scan, but in most cases this costs too much time. For example, because of the channel hopping and TDD, the time to scan one address can take several seconds. If you were able to scan one address every second, you would need almost 9 milion years. Offcourse you can leave out a large piece of the address-space because it is not very likely that MAC-addresses of PC networkcards are use for Bluetooth devices aswell. Still the devices would be gone long before you can complete your brute force scan if you have non-stationary devices. This can be considered as some form of protection.

2.4 Range

Bluetooth is based on radio frequency technology. How this exactly works is far beyond the scope of the project and thus this report. Still, there are things which are important to know.

As told before, the 2.4 Ghz ISM band is crowded and therefore contains lot of noise. But that is not all. The higher the frequency, the worse it is able to traverse through solid materials, liquids and gasses (i.e. fog). Concrete walls are notorious for being major signal blockers (for example, if you drive into a tunnel with your car, your radio only receives static). Anonther obstacle is water. This material is known to react at this frequency (this is why a microwave oven operates at 2.4 GHz aswell)[12]. It is ofcourse true that when you use enough power for a transmitter, you are able to get through these materials, but still a lot of the signal will be absorbed.

Bluetooth devices are catogerized in three classes of transmission power. Class I devices have a maximum transmision power of 100 mW EIRP, which in most countries is the maximum legal transmission power for 2.4 GHz. Devices

such as computers are often Class I devices. Achieving a tanges of 100 meter should be possible using these devices. As told in the introduction, Bluetooth designed is for operation within within 10 meter. Devices capable of that range are often Class II devices and may transmit at 2.5 mW EIRP. Almost all devices such as phones, headsets and all other gadgets with Bluetooth are Class II. For very short ranges (10 cm) there are Class III devices which only transmit with 1 mW EIRP.

So, the range at which you can use Bluetooth depends on what class the devices are in, and what the environment is like.

Chapter 3

Research setup

3.1 Introduction

The previous chapter discussed Bluetooth's discoverable mode. To investigate the possibility of tracking people that have their Bluetooth devices set in this mode we performed two tests. The first is a multi-site test to track people who travel between two busy trainstations in The Netherlands. The second was a continuous scan, performed at a single trainstation during a five-day period. The first part of this chapter describes the different testsites. After that we explain more about the equipment used for the tests. Finally, more detailed information on the two different tests is given.

3.2 Locations

For our multi-site scan we decided we wanted to track a group of commuters taking the train from one major train station to another. Amsterdam Central Station (CS) and Utrecht CS where chosen for this purpose. The train travelling from Amsterdam CS to Utrecht CS passes a station called Amsterdam Amstel. This location was also added to the multi-site scan. Amstel station was also used for the continuous scan. For a map of these three locations see appendix A.

3.2.1 Location 1: Amsterdam CS

The first trainstation we chose for our research is Amsterdam CS. This station was chosen because it is the main station of our capital city, and because it is quite busy. We chose to monitor people travelling in trains towards Utrecht CS (more about this location in the next paragraph). Trains going to Utrecht from Amsterdam CS leave from platforms 7b, 5, 4 and 2. Platform 5 is in the middle, which makes it an excellent place to scan devices on all the mentioned platforms. Consequently, this is where we located our first scanningteam.

3.2.2 Location 2: Utrecht CS

The second station we chose for our multi-site test was Utrecht Central Station. This station is located in the center of the Netherlands. From Utrecht, trains depart to all corners of the country. Because of this central location Utrecht CS is one of the most busy trainstations in the Netherlands.

There is a direct train connection between Amsterdam CS and Utrecht CS. Trains take about half an hour to travel between these two stations. On Utrecht CS most trains coming from Amsterdam CS arrive on platform 12. We decided to position our second scanningteam outside the exit of platform 12. This means that most people with Bluetooth devices coming from Amsterdam need to get off the train to be picked up by our equipment. There is another exit wich leads to a tunnel underneath all platforms, but there are only a few people who actually use it.

3.2.3 Location 3: Amsterdam Amstel

The third location we used during our tests was the trainstation Amsterdam Amstel. This station is located near Amsterdam CS, and all trains travelling from Amsterdam to Utrecht come through this station. Also, subway trains to and from Amsterdam CS come by this station. The position between Amsterdam CS and Utrecht CS made it a perfect location to use for our multi-site scan. For a map of Amstel's surroundings see appendix A.

Our university lab is located in the building of the "Hogeschool van Amsterdam". This building happens to stand next to the Amstel station. Because we also wanted to do a continuous scan over a five-day period we decided to position the scanning equipment at this station inside our lab, looking out on the station. This way we where able to use this site for both the multi-site and the continuous scan.

3.3 Equipment

To do the actual scanning we used a number of Bluetooth USB dongles. For our project we used Linksys Bluetooth USB Adapters (Model No. USBBT100).[9] These Class I adapters normally have a small antenna connected to them, which has a gain of 1.6 dBi. Preliminary tests showed that this is not enough to scan inside a train from the platform next to it. We therefore removed the old antenna and added a Hawking Hi-Gain antenna. This antenna has a gain of 6dBi. Since we wanted to scan under a broad angle, we used an omni-directional antenna (Model No. HAI6SIP).[6]

For the scans at Amsterdam CS and Utrecht CS we used two laptops, one installed with Debian[5], the other with Ubuntu[15]. For the scan at Amstel we used an ordinary PC. On the machines we installed bluez-utils[4], a Bluetooth protocol stack for Linux. We made a script which uses bluez's hcitool program to scan for Bluetooth devices that are set in discoverable mode. These results, along with the timestamp of the scan, were put in a logfile. As a result, a logfile holding all the scan results was generated. This file contains a device's MAC-address, it's class number (an hexadecimal number, identifying the type of device) and the timestamp at which the device was spotted. We chose not to resolve the names of the devices we scanned, because this would take too much

time. If hcitool tries to resolve a name, and the device has gone out of reach or is not responding in a timely fashion, the tool may wait up to as much as ten seconds per device[1]. This is far too long for the purpose of our research.

For our continuous scan we wanted to try and scan people carrying Bluetooth devices inside the Amsterdam Amstel station. To shield the antenna from people walking by in our own building, we cut open a Pringles[13] can (see figure 3.1). These cans are lined with aluminum on the inside and are used widely for radiowave manipulation. We removed the top and bottom, and cut it open on one side. We placed this over the omni-antenna that was taped to a window, and used tinfoil to cover the edges. Please note that this Pringles can was not installed to somehow focus the radio waves better, but just to keep the antenna from scanning for devices inside the buiding. This solution worked quite well, but some Bluetooth devices inside the buiding where still being scanned. Devices inside our lab and in the connecting rooms at the same level where still being picked up.

Figure 3.1: Pringles can

3.4 Performed tests

As said in the introduction, we performed two main tests: a multi-site scan and a continuous scan. Details about these tests are described in this section. Because of the odd setup at Amsterdam Amstel we decided to perform a number of preliminary tests, to see if this setup didn't cause too many problems. These tests are discussed first.

[1] The reason for this is the same as why a brute-force scan of all MAC-addresses would not work. See 2.3

3.4.1 Preliminary tests

Our lab at Amstel station is at the sixth floor of the building, and the station is about fourty meters from the university. That leaves us with a gap of about 50 meters that we had to cross to scan Bluetooth devices inside the station. At the university's site of the train station, all windows have a metal frame. Outside the windows concrete pillars that support the building are located. This narrowed our view of the station somewhat. We could see most of the station except the left end of the station. Naturally this also obstructed the Bluetooth signal. Because we wanted to be sure our setup wasn't affected too much by the distance and the building's structure, we decided to perform some preliminary tests.

The Amstel station has two entrances. One is located at the far side of the station, and leads to the busses and trams. This exit is probably used most. The other exit is at the university's side. The station has two main staircases, one to the trains and subways travelling in the direction of the Amsterdam Arena, and one to the trains and subways travelling to Amsterdam CS.

Using the setup descibed in the previous section we where able to scan people walking to and from the station taking the entrance at the university side. We could also scan people on the first platform, as well as some people on the second platform. This means we could scan people waiting for the train from Amsterdam CS in the direction of Utrecht. Also, we where able to monitor people taking the subway to the Amsterdam Arena and further. We can not scan people standing on the outmost left side of the station, but can scan the two stairways to the station.

After this, we tested if we could scan inside the train from Amsterdam CS to Utrecht CS. We placed three persons in the train. One in the front of the train, one in the middle and one in the back. It turned out we could scan the person in the front of the train, and the one in the middle. Unfortunately the concrete pillars of the building obstructed us from scanning the back of the train. When a train departs from Amstel and the back end comes into view, it has too much speed, so it can not be scanned anymore. Trains passing the station without stopping can not be scanned either for this reason. Due to the fact that we had only three sets of omni-antennas and did not want to interrupt our continuous scan, we had to accept this fact for our multi-site scan. If we had had more equipment, we would have positioned this on the platform of the station to add more value to our multi-site scan.

As a result we concluded we could scan:

- All people taking the first stairway from the universities' view to the train in the direction of Utrecht and the subway to the Amsterdam Arena.
- About 75% of all people in the trains that stop at the Amstel station.
- All persons walking to and from the station using the university side entrance.
- Some people taking the second strairway to the trains and subways to Amsterdam CS.

3.4.2 Multi-site scan

To track people from Amsterdam CS to Utrecht CS we needed to make sure that there was a large enough amount of people travelling between these places. Between 16h00 and 18h00 hours it is rush hour at these stations. This makes it ideal to scan for Bluetooth devices. The multi-site scan was performed on the 18th of May, 2005. We started scanning on Amsterdam CS at 16h00, and ended around 18h00. Since trains travelling from Amsterdam to Utrecht take at least half an hour for the journey, and we wanted to spare our laptop batteries, we started scanning at Utrecht CS around 16h25, and ended 15 minutes after the last train scanned at Amsterdam CS arrived in Utrecht. This was at 18h45. Since trains from Amsterdam CS to Utrecht CS pass by the Amstel station, we extracted data from the continuous scan between 16h00 and 18h30, and added it to the data of the multi-site test.

3.4.3 Continuous scan

The continuous scan was performed at out lab, during a five-day period. We started our scan at Monday the 16th of May 2005 at 0h00, and ended on Friday the 20th at 23h59. During this time our equipment looked for Bluetooth devices at the Amstel station 24 hours a day. Because the building in which the lab resides is closed at night we started the scanning a couple of hours earlier, and ended a number of hours later. The device sightings found outside the set timeperiod where removed before calculating the results.

Chapter 4

Results

Each of the two tests described in the previous chapter provided us with a number of datafiles. One for each location of the multi-site scan, and one for the continuous scan. These files contain lists of timestamps when a device was discovered, the MAC-address of the device and the device class number. In order to be able to analyse these files and correlate the results we created a small Perl[11] program that imports the files into a Mysql[10] database and displays various statistics. To convert the class numbers to actual device types (e.g. phone, computer) we used an algorithm derived from the corresponding function used in hcitool. Vendor names where retrieved by comparing the first part of a device's MAC-address with the list[7] of organisational identifiers published by IEEE.

In the remainder of this chapter the results of the two tests are listed, together with conclusions that we where able to derive from these statistics. Finally, some miscellaneous findings are discussed.

4.1 Multi-site scan

The results of the multi-site scan can be divided into two parts: results concerning discovered MAC-addresses, and results dealing with discovered device classes and vendors. This section is split up accordingly.

4.1.1 MAC-addresses

After combining the results from the scans performed at the three different locations we where left with a total of 1877 device sightings. As table 4.1 shows most of these where found at Utrecht CS. This is because our scanning equipment was positioned at a busy part of the station. The equipment at Amsterdam Amstel picked up the smallest number of results, because this station is the smallest of the three, and because we only monitored one platform of this station.

When combining the device sightings we found 1712 unique MAC-addresses. 140 of these addresses where seen at more than one station, and 25 addresses where picked up at all three locations. Table 4.2 shows how the addresses that where found at two locations are divided.

Location	Sightings
Amsterdam CS	502
Amsterdam Amstel	317
Utrecht CS	1058
Total	1877

Table 4.1: Unique sightings

Locations	No. of addresses
Amsterdam CS & Amsterdam Amstel	44
Amsterdam CS & Utrecht CS	35
Amsterdam Amstel & Utrecht CS	36
Total	115

Table 4.2: Addresses seen twice

From this data we can conclude that a total of 44 people carrying Bluetooth devices in discoverable mode travelled from Amsterdam CS to Amsterdam Amstel during our scanning period. Because we did not pick up a signal from these people at Utrecht Central we can conclude that these people either departed the train before Utrecht CS, or continued towards other destinations using the same train.

A total of 25 people travelled from Amsterdam CS to Utrecht CS without being picked up at Amsterdam Amstel. The most likely cause of this is that the train these people used passed our scanner at Amsterdam Amstel at a speed to high for our equipment to be able to pick up the Bluetooth devices.

Finally, we found 36 people carrying Bluetooth devices that boarded a train at Amsterdam Amstel, and departed this train at Utrecht CS.

The above conclusions are made assuming that no people enabled or disabled their Bluetooth device during the course of our investigation. We assess the chance of this happening as fairly low, since most people do not even realise their device is in discoverable mode, and therefore never disable it.

4.1.2 Classes & vendors

The main goal of this research was to investigate the possibility of tracking people. We are however also able to extract other kinds of statistics from our tests. The two figures below reflect this. Figure 4.1 shows statistics on the different device classes we found during the multi-site test. Not surprisingly, most of the devices found where mobile phones. Figure 4.2 shows statistics on the chipset vendors in the discovered devices. These are not always the same as the phone vendor. For example, Nokia uses a lot of chipsets manufactured by a company called Matsushita in their mobile phones.

4.2 Continuous scan

As for the multi-site scan, the results for the continuous scan can be divided into information about discovered MAC-addresses, and information on device classes and chip vendors. These results are discussed in this section.

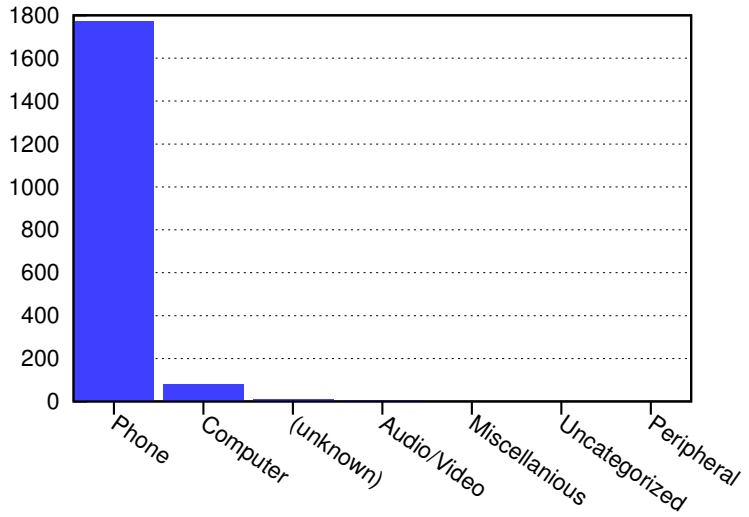

Figure 4.1: Device class statistics (multi-site)

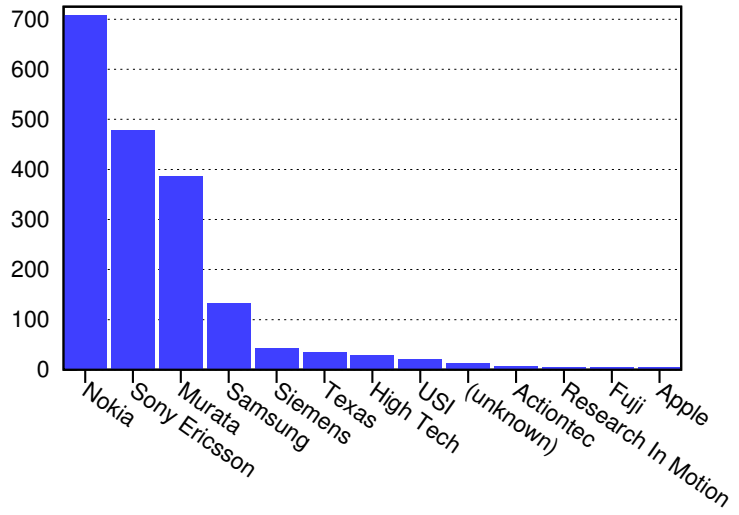

Figure 4.2: Chipset vendor statistics (multi-site)

4.2.1 MAC-addresses

To be able to extract some useful results concerning devices seen at multiple times of the day and multiple days of the week, we divided the results of the continuous scan into timeblocks. Each day is divided into three timeblocks: 00:00-9:59, 10:00-14:59, and 15:00-23:59. By using this division each block encapsulates one of the three times of day with the highest amount of people movement (two rush hours and lunchtime). For each of these blocks all unique MAC-addresses where stored. We chose this division strategy because it increases the chance of finding multiple occurances of the same MAC-addresses

in one day.

Processing the data according to the above procedure resulted in a total number of 6588 found devices in the five days of scanning. Among these discoveries where 3943 unique MAC-addresses. Figure 4.3 gives a clear layout of the number of devices found at each part of the day, and each day of the week.

Of the 3943 unique MAC-addresses we found 879 addresses where seen in multiple timeblocks. 1068 addresses where picked up on more than one day of the week.

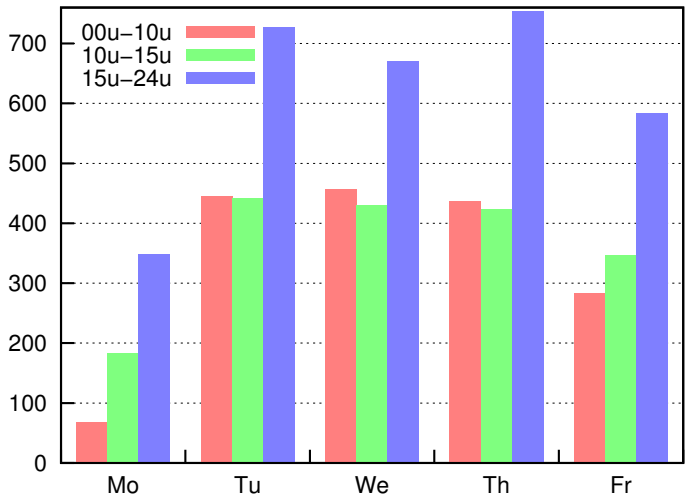

Figure 4.3: Sightings per timeblock

Because of the limited time available for this research we where not able to create detailed results per hour of the day. It is therefore not possible to derive conclusions from this test on things like which time of day is the busiest. It is however possible to draw some conclusions from this information. Firstly, the low amount of found devices on Monday is likely related to the fact that this day was a bank holiday in the Netherlands. Another conclusion we can derive is that a large number of people travel past Amsterdam Amstel multiple times a day, which is explained by the central location of this station.

4.2.2 Classes & vendors

Like the multi-site scan the continuous scan also allowed us to extract some information on different device classes and chipsets that are used in the Netherlands today. Figures 4.4 and 4.5 show statistics for device classes and chipset vendors respectively. As to be expected, the results are roughly the same as those shown in the previous section.

4.3 Miscellaneous findings

The testresults described above show that it is fairly easy to track people carrying discoverable Bluetooth devices over a large distance. It is also possible

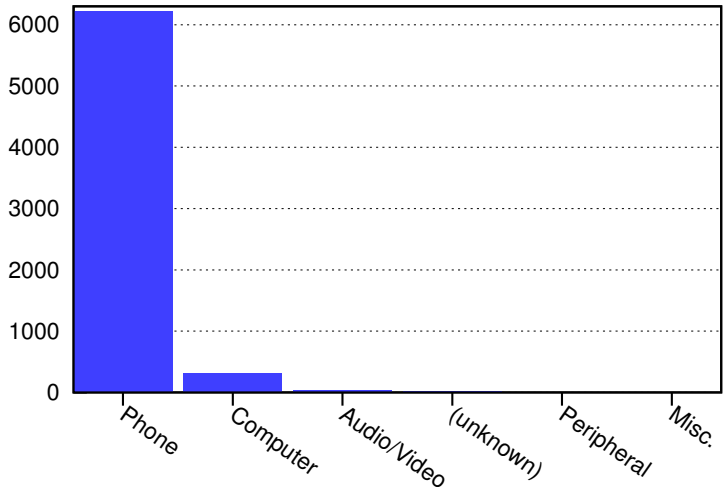

Figure 4.4: Device class statistics (continuous)

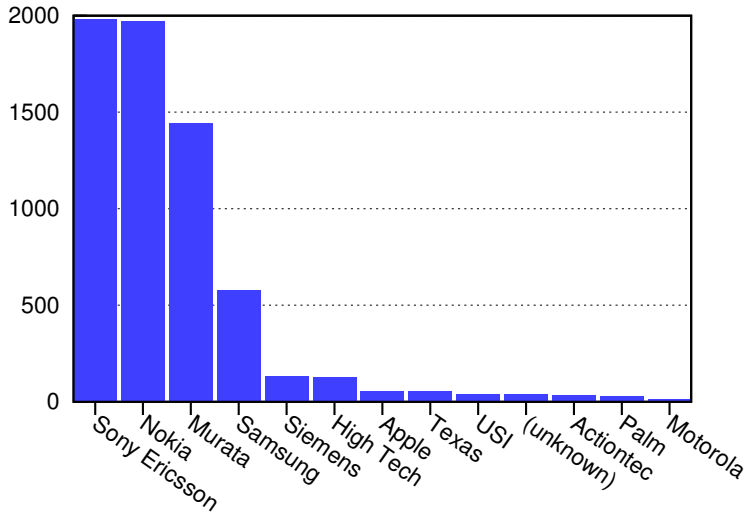

Figure 4.5: Chipset vendor statistics (continuous)

to discover patterns in the movement of people, if they pass locations multiple times a day (for example when they travel between home and work). During our research we also found a number of other interesting things. These are listed here.

While performing some preliminary tests we discovered that employees of the Dutch railways carry Bluetooth devices, and that nearly all of these devices are set in discoverable mode. We also found that the devices all have the same vendor, and use addresses from a specific range of MAC-addresses. Finally, the announced names of these Bluetooth devices all conform to the same (company) standard. All of this together allowed us to exactly pinpoint which of the devices

we found during our scans belong to railway employees.

The second interesting discovery we made during our tests is that the system administrator of our lab purposely leaves his Bluetooth-enabled phone in discoverable mode. Because we knew the MAC-address of this phone we decided to try and match it with the results of the continuous scan (after asking him for permission). The result of this was that we where able to extract the exact time he entered and left work on the days within the scanning period.

The third interesting thing we found is that on a large number of occasions more than one Bluetooth device was within the reach of our antennas at a single timestamp. This means that a theoretical virus or worm that replicates itself among all Bluetooth-enabled devices is able to distribute itself among many devices in short time. Bluetooth-enabled worms already exist in the wild[14], so it is not unlikely that such a worm will come to exist in the (near) future.

Chapter 5

Conclusion

With our research we have proved that it is possible to track people using Bluetooth-enabled devices as they travel over a large geographical distance, and to find out how often people visit a certain location. If the tracking information of the type of scans we performed is linked to actual identities (for example by extracting information like phonebook entries from someone's Bluetooth device) a lot of privacy sensitive information can be discovered. This information can be used for anything ranging from stalking a single person, to Orwellian scenarios as country-wide government spying on the travelling habits of civilians.

More specific, the information we discovered on devices carried by railway employees may be used by fare dodgers to find out if there is a conductor travelling on the same train. If this is used in combination with a signal strength meter it could even be possible to roughly estimate on which side of the train this individual is located, and if he is moving closer or not.

The example of the tracking of our system administrator we described in the previous chapter also has some implications. A company might, for example, require its employees to enable Bluetooth discoverable mode on their company-supplied phones so it can use this technique to keep track on the amount of time the employees spend at their desks. Burglers may also find information like this interesting to check from a distance if there are still people working late in a building. This type of thing may sound pointless at this time, since the number of people carrying Bluetooth devices is relatively low, but it is not unlikely that Bluetooth-enabled phones will soon be as common as ordinary cellphones are now.

Finally, as Bluetooth devices become more common, the risk of Bluetooth-enabled viruses and worms becomes greater too. Chapter 4 shows some interesting statistics on which vendor's devices form the most interesting targets for this type of thing.

5.1 Future work

The small tests we performed during our research already show some interesting results. However, to be able to find more detailed results more research is needed. Tests with a larger number of Bluetooth dongles over a larger geographical distance may be done to find these results. Another possibility is to use

trilateration and devicename discovery to retrieve more information. Finally, research may be done on ways to mitigate the number of devices that are in discoverable mode. Possible solutions to this problem may be to disable discoverable mode by default on new devices, and to inform people of the possible implications of enabling this function.

On the field of virus- and wormspreading it may be interesting to look into the similarities and differences between Bluetooth viruses and their biological equivalents.

If any further tests in the above areas are performed it is important that one respects and protects the privacy of anyone who's device is used during the research period, and that all privacy sensitive material is destroyed after the research has been concluded.

Appendix A

Maps

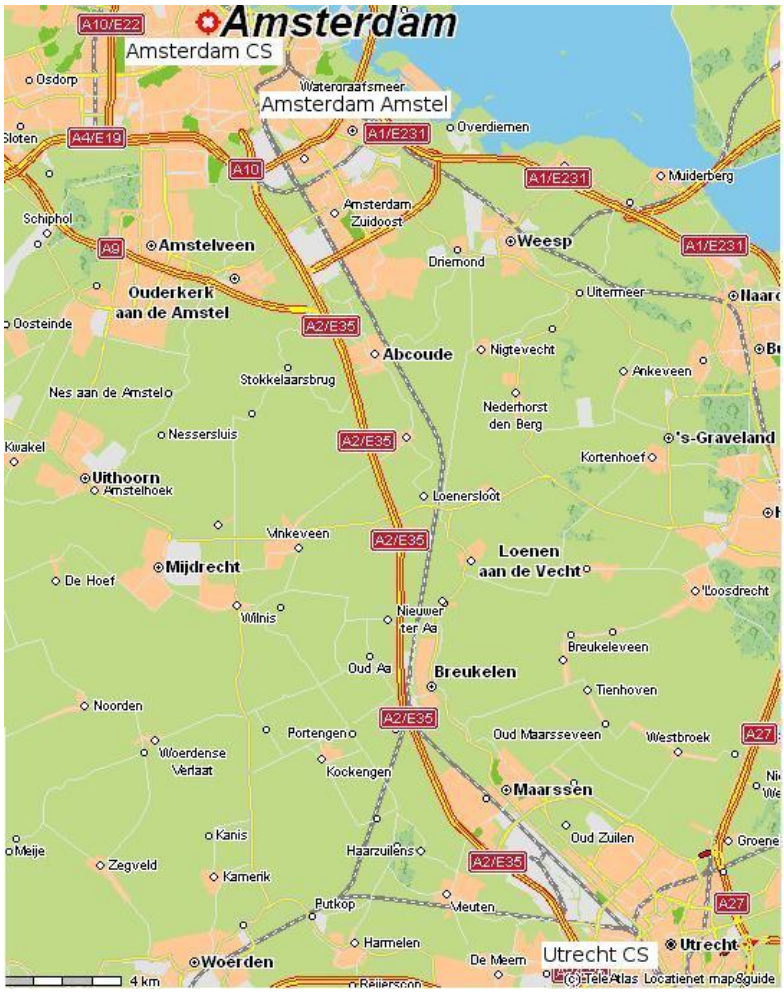

Figure A.1: Amsterdam CS to Utrecht CS route

Figure A.2: Amsterdam Amstel surroundings

Bibliography

[1] *Bluetooth Radio Basics*, Xilinx,
http://www.xilinx.com/esp/networks_telecom/bluetooth/pdf_files/radio_basics.pps

[2] *Bluetooth technology*, S. Khetarpal, 2004,
http://www.cs.wright.edu/~jstephen/ee737/ResearchPapers/Khetarpal.doc

[3] *Bluetooth website*,
http://www.bluetooth.com/

Bluetooth FAQ,
https://www.bluetooth.org/admin/bluetooth2/faq/view_record.php?id=49

[4] *Bluez-utils*,
http://www.bluez.org/download.html

[5] *Debian*,
http://www.debian.org/

[6] *Hawking Hi-Gain 6dBi Omni-Directional Wireless Antenna*,
http://www.hawkingtech.com/prodSpec.php?ProdID=145

[7] *IEEE OUI and Company_id Assignments*, May 2005,
http://standards.ieee.org/regauth/oui/

[8] *K1 Generic Access Profile*,
http://www.palowireless.com/infotooth/tutorial/k1_gap.asp

[9] *Linksys USBBT100 Bluetooth USB adapter*,
http://www.linksys.com/products/product.asp?grid=33&scid=38&prid=581

[10] *MySQL*,
http://www.mysql.com/

[11] *Perl*,
http://www.perl.org/

[12] Ekkehard Plicht, *WLAN Technical basics*, Februari 2003
http://wimo.de/cgi-bin/verteiler.pl?url=wlanbasics_e.htm

[13] *Pringles*, http://www.pringles-info.co.uk/

[14] *Symantec Security Response: SymbOS.Cabir*,
http://securityresponse.symantec.com/avcenter/venc/data/epoc.cabir.html

[15] *Ubuntu Linux*,
http://www.ubuntulinux.org/