Is Perth a secure place: a Western Australian field study of Bluetooth security

Khwaja Shan-ul-Hasan Ghori, Peter Dell

Curtin University of Technology, Perth, Australia

Abstract

Bluetooth, a wireless technology for building short-range communication links, poses a number of security risks, including disclosure of confidential data and unauthorised control of functions such as telephony and data services. The use of these devices is increasing, and many Bluetooth devices store sensitive or valuable data. This increases the motivation for intruders to attack devices over Bluetooth connections.

This paper reports the extent of the potential for Bluetooth security problems in Perth, Western Australia. It finds that there are many devices potentially vulnerable to attack via Bluetooth, and that it is feasible to easily access a large number of Bluetooth devices for a sufficiently long duration to cause damage. These findings, taken in conjunction with known existing Bluetooth threats and attacks, indicate a very real Bluetooth security risk. The paper concludes with issues to be investigated in future so that corporate IT departments, end users and manufacturers can provide optimum security, thus reducing the potential for successful Bluetooth attacks in the future.

1. Introduction

Bluetooth is a wireless technology for building a short range communication links with various types of devices (McDermott-Wells, 2005), such as between a cell phone acting and a hands-free headset. Bluetooth has a range of up to 10 metres, and possibly up to 100 metres by increasing the transmitter's power (Sairam *et al*., 2002).

Previous studies of Bluetooth security have indicated that many Bluetooth implementations have security flaws and that it is possible to retrieve data from many such devices if Bluetooth is enabled. A field study conducted in London revealed more than 2,000 Bluetooth devices that were insecure (Gostev, 2006), while an experimental Bluetooth attack by security experts at an IT exhibition in Germany demonstrated that Bluetooth attacks are not just theoretical: the experiment recorded 1,269 vulnerable devices that were disclosing personal information (Herfurt, 2004).

However, research on Bluetooth security like that in London and Germany has never been conducted in Australia. Further, the London study did not investigate potential differences between different types of location, and the research in Germany may be misleading because it was conducted at an IT fair, so was not necessarily representative of the general public.

Therefore, in this paper, we investigate the extent of the Bluetooth security problem in Perth, Western Australia, and consider results from two different location categories: Group (1) includes places where business people are likely to congregate, such as the lobbies of office towers or nearby cafés, and Group (2) includes places more representative of the general public, such as like shopping centres.

The remainder of this paper is organized in to six sections. After a brief introduction we discuss the various security flaws associated with Bluetooth in Section 2. Section 3 describes the questions investigated in this project, while Section 4 describes the research method used, including the instruments used in the field. Following the research method and design is discussion of the results (Section 5), leading to conclusions discussed in Section 6. Finally, Section 7 identifies recommendations for further research.

2. Security Flaws in Bluetooth

Bluetooth has gained widespread acceptance around the world and is supported by a wide range of devices, and because Bluetooth has a user friendly nature, these devices are becoming more personal to many users than a personal computer (Dagon *et al*., 2004). While WiFi has gained wide recognition as a potential threat to security by home users and business people, Bluetooth has not (Potter, 2006) and the number of users who trust Bluetooth capable devices to store sensitive information has increased (Dagon *et al.*, 2004). This could motivate a large number of intruders to attack such devices over Bluetooth. Such attacks are technically possible because there are many Bluetooth security issues. These are described in the following subsections.

2.1 Information Theft

In this type of attack, a mobile device is compromised to reveal sensitive information such as contact information, phone numbers, programs, and applications stored on smart phones (Dagon *et al.*, 2004). Various tools are available to hackers to conduct information theft, such as the *HeloMoto* tool, which can be used to extract personal information from early Motorola V-Series phones (c.f. Trifinite 2006a).

2.2 Spamming Unsolicited Information (Bluejacking)

Bluejacking is the term used to describe “spamming” mobile phones via Bluetooth. The attacker alters the phonebook contact on their Bluetooth device by writing a message such as “Drink Coke” in the name field, and then sends this message to all Bluetooth devices within range (Dagon *et al.*, 2004). Bluejacking is normally harmless, however, the attack can be extended to overwrite the victim’s phonebook by sending phonebook contacts with common names such as “Work” or “Home” (Janssens, 2005). There are online resources available which provide detailed and exact guides on how to Bluejack with specific Bluetooth devices (c.f. Jellyellie, 2004).

2.3 Theft-of-Service Attacks

Theft-of-service attacks are those attacks in which an attacker hijacks the victim’s phone resources, and may result in the attacker placing long-distance phone calls, sending SMS messages, and the like (Dagon *et al.*, 2004). Hacking tools are available that can be used to discover all available services on Bluetooth devices (InsightConsulting, 2006).

2.4 Denial of Service Attacks

Denial of Service (DoS) attacks are those attacks in which an attacker overflows mobile devices by sending huge amounts of replicated information, corrupted data packets and inaccurate file formats. There are several tools available to launch such attacks, of which *BlueSmack* is an example (c.f. Trifinite, 2006b).

2.5 Virus and Worm Attacks

Bluetooth can form a transmission vector for viruses and worms. *Cabir* is a well-known Bluetooth worm which automatically replicates itself to other Bluetooth devices within range (Potter, 2005).

2.6 Brute-Force Attack

Brute-force attacks on Bluetooth are commonly referred as Blueprinting. In these attacks, the attacker is able to remotely determine the characteristics of the device under attack, such as its unique Bluetooth device address, service description records, device model, and so on. Tools such as *Blueprint* are available in the public domain to conduct brute-force attacks (c.f. Trifinite, 2006c).

2.7 BlueSnarfing

BlueSnarfing refers to an attack in which the attacker gains access to the victim's mobile phone without authentication and gives the attacker full access to potentially sensitive information stored on the phone such as phonebook, calendar, business card, phone properties, and so on (Janssens, 2005).

2.8 BlueBugging

BlueBugging is an extended form of the BlueSnarfing attack. In addition to full access of sensitive data, an attacker is able to send commands to the target device to force it initiate phone calls, send text messages, access the Internet, intercept communications, and so on (McFedries, 2005). Tools such as *BlueBug* and *Gnokii* can be used by attackers to conduct BlueBug attacks (InsightConsulting, 2006).

3. Research Question

The range of Bluetooth security issues described in the previous section may pose a serious threat to organisations that use Bluetooth devices, particularly if such devices are poorly configured. The two previous reports suggest that such devices may be frequently encountered, although these studies may not be representative and no such research has been conducted in Australia. Therefore, this study sought to investigate the state of Bluetooth security in Perth, Western Australia. In order to do this, the following questions were asked.

1. Which services are commonly advertised by Bluetooth devices in Perth, Western Australia?

2. What types of Bluetooth device are common in Perth, Western Australia?

4. Research Method

These questions were investigated in a field study in which the researchers monitored public places for Bluetooth signals. The target locations chosen to conduct this research were divided in to two groups referred to as Group (1) and Group (2). The target locations in Group (1) included well-known office towers in the Central Business District. Many of these towers have their own lobby cafes where office workers have breakfast, meet for lunch or coffee and so on, and most have seating areas available in the lobby within range of the cafés. Even where there is no café present, people often congregate in the lobby or nearby for various reasons, such as meeting others, to smoke a cigarette, and so on. The target locations in Group (2) included places where people congregate in shopping areas, such as cafés, food-courts and malls. Thus, while locations in Group (1) tend to be frequented by business professionals, locations in Group (2) are more oriented towards the general public.

A laptop with a Bluetooth adapter and Bluetooth scanning software were used to conduct data collection. Although the adapter used allowed the researchers to detect devices within a range of up to 100 metres, practically all Bluetooth devices support a much shorter range of up to approximately 10 metres and so devices detected by the researchers were likely within close proximity.

Devices were able to be detected when set to “visible” mode in the Bluetooth settings of the device. For example, the Nokia 6280 allows the user to configure the device as “shown to all” or “hidden”. If the device is configured as “shown to all” it will be discoverable by other Bluetooth devices within range without authentication. This renders a device potentially insecure since attackers can detect it and gather information about it.

5. Results and Discussion

The following table illustrates a summary of the data collected from both Group (1) and Group (2) sites as part of this research.

Location	Total Devices Found	Total Time Spent
Group (1) Sites	772	705 minutes
Group (2) Sites	963	386 minutes

Table 1: A summary of the data collected from the field

These data clearly show that there are significant numbers of Bluetooth devices that were discoverable in a short time.

Before proceeding any further with the discussion, it is important to define the different types of Bluetooth services discovered in the field. A summary of Bluetooth services is shown in the following table.

Bluetooth Services	Functions
Generic Object Exchange Profile (GOEP)	Used to transfer objects such as a picture or document to another device using OBEX (Object Exchange) protocol.
Dial-up Networking Profile (DUN)	Allows users to connect the Internet using Bluetooth enabled phones.
Object Push Profile (OPP)	Used to instruct how data objects such as business cards are exchanged between two Bluetooth devices.
Synchronization Profile (SYNC)	Used to ensure accuracy and consistency of data objects exchanged between Bluetooth enabled devices.
Headset Profile (HSP)	Used to instruct how Bluetooth headset establishes communications with Bluetooth phones.
Serial Port Profile (SPP)	Provide a set of procedures that enable two Bluetooth enabled devices establish communication over virtual serial ports.
SIM Access Profile (SAP)	Allows car phones to access a SIM card in a Bluetooth enabled mobile phone.
Service Discovery Protocol (SDP)	Allows applications to discover which services are available to a particular Bluetooth device.
Basic Imaging Profile (BIP)	Allow users to send, browse, and retrieve images to and from a remotely controlled imaging device.
Audio / Video Remote Control Device (AVRCP)	Enable Bluetooth phones to work as a single remote control for all audio / video equipments.
Advanced Audio Distribution Profile (A2DP)	Defines how devices can stream audio from a source media to a sink.
Human Interface Device Profile (HID)	Allow mobile phones to be used as a keyboard or a mouse.
Personal Area Networking Profile (PAN)	Defines how Bluetooth devices form an ad-hoc network and access a remote network using network access points.

Table 2: A summary of different Bluetooth service types (BluetoothSIG 2007 and Gratton 2002)

The following figure shows the number of devices which advertised each service.

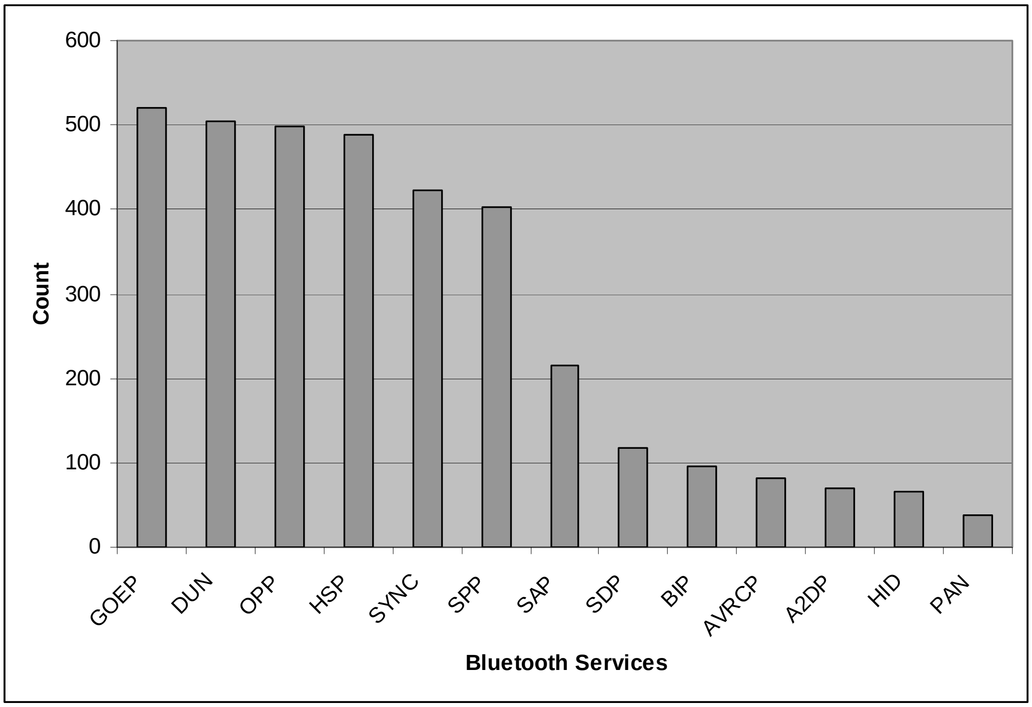

Figure 1: Number of devices advertising Bluetooth services

Not all of the Bluetooth services above present serious security threats. For example, the ability for an attacker to use a mobile phone as an audio/video remote control device (AVRCD) probably does not pose a major risk, even if the phone is compromised. Likewise, the human interface device (HID) profile also likely presents only a minor risk at most, since attackers are unlikely to be able to cause any major damage by compromising a device that has the ability to act as a keyboard or a mouse. It is only those services that allow the access of data or paid services that are risky, such as Generic Object Exchange (GOEP), Dial-up Networking (DUN), and Synchronization (SYNC). Object Push (OPP) might also be a problem if it allows attackers to push viruses or worms to devices. Therefore, the following analysis will focus only on these four services which are perceived as presenting serious risks.

5.1 Discussion of Research Question 1

This section considers the first question, which asked which Bluetooth services were commonly advertised in Perth. The following figure illustrates the proportion of Bluetooth devices advertising each of the four services regarded as security risks, categorised by the type of location.

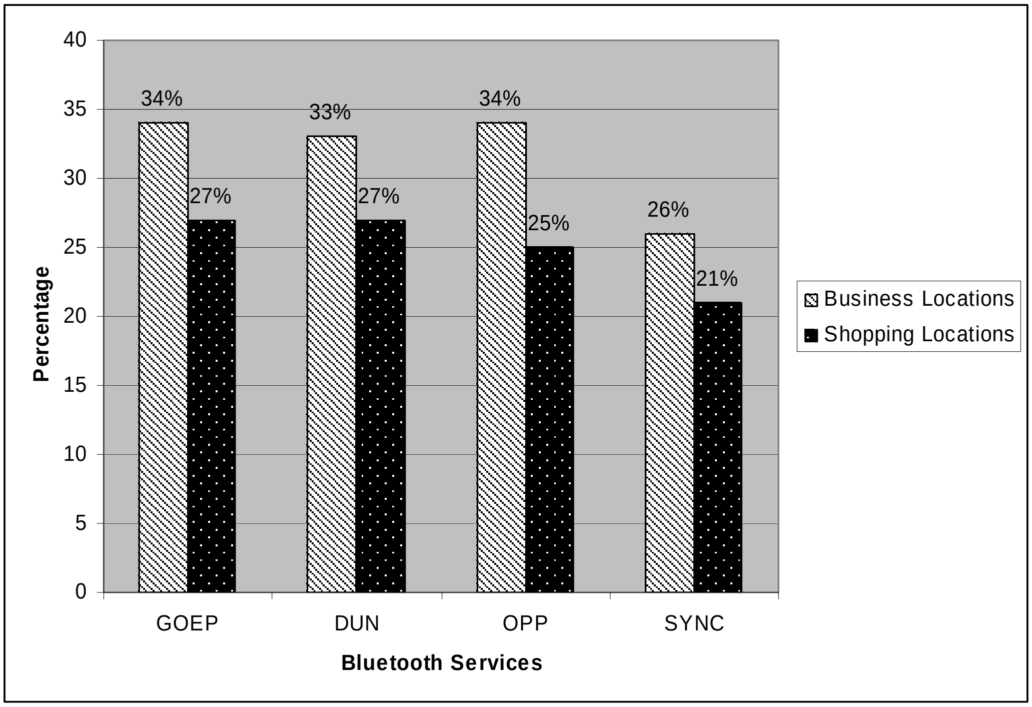

Figure 2: Number of critical services with the type of location

This issue was investigated because demographic differences between locations could lead to devices with different capabilities being more prevalent in some areas than others, although the findings suggest that there is only a marginal difference between the services advertised by devices in business and shopping locations.

This finding is significant because it indicates that approximately one third of Bluetooth devices in business locations advertise services that may pose a security risk, and if one assumes that such devices may store business-related data, the risk of such a device being compromised could equate to a business risk. A similar proportion of devices found in shopping districts also advertise services which may be a potential security risk, and while these devices may be less of a target for data theft, the consequences of other attacks such as toll fraud from unauthorised access to DUN could be damaging.

Further, these devices were frequently within range for long enough for an attack to take place. The following figure illustrates the average time Bluetooth services were in range in different locations.

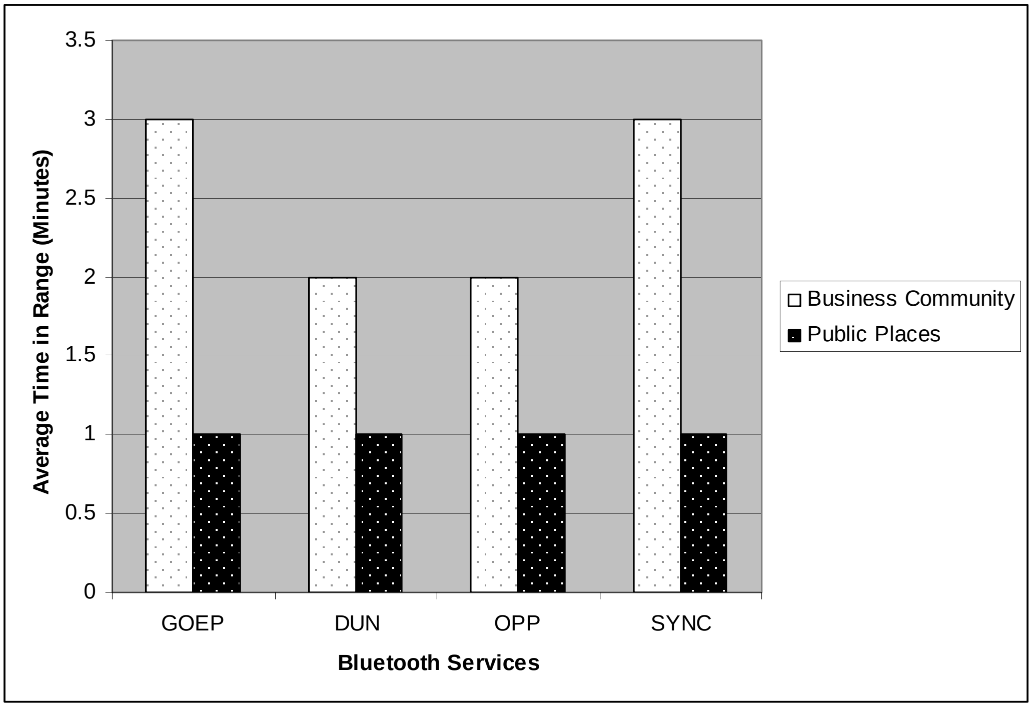

Figure 3: Average time in range of Bluetooth Services

The above figure clearly indicates that critical Bluetooth services were within range for longer periods in business locations than in shopping locations. On average, devices supporting OPP were in range for about three minutes – easily long enough to launch a successful BlueBug attack, which may only take few seconds depending on what is required. In some cases, devices were within range for much longer, for example, in one office location there were nine devices that supported critical Bluetooth services and which remained in range for more than 10 minutes.

The prevalence of devices with potentially serious impact of a security breach, combined with the fact that such devices are often within range for long enough period to launch an attack, leads the researchers to conclude that there is indeed a significant Bluetooth security risk in Perth. Security professionals are therefore advised to ensure that devices within their organisation are secure if they are not doing so already.

It is particularly interesting to note that DUN was supported by so many devices. It is very unlikely that the owners of these devices use their mobile phones to connect to the Internet. It is likely that most of these devices enable network access services such as DUN by default. This presents an unnecessary risk with potentially severe consequences, since unauthorised network access could quickly result in high monetary cost to the victim.

5.3 Discussion of Research Question 2

This question asked what types of Bluetooth device were common in Perth. Such devices include mobile phones, smart-phones, handheld computers, GPS systems, and many others. This study is primarily concerned with the prevalence of devices that may store sensitive devices, particularly smart phones and handheld computers, in comparison to basic mobile phones. The following graph illustrates the breakdown of mobile phones and sensitive devices.

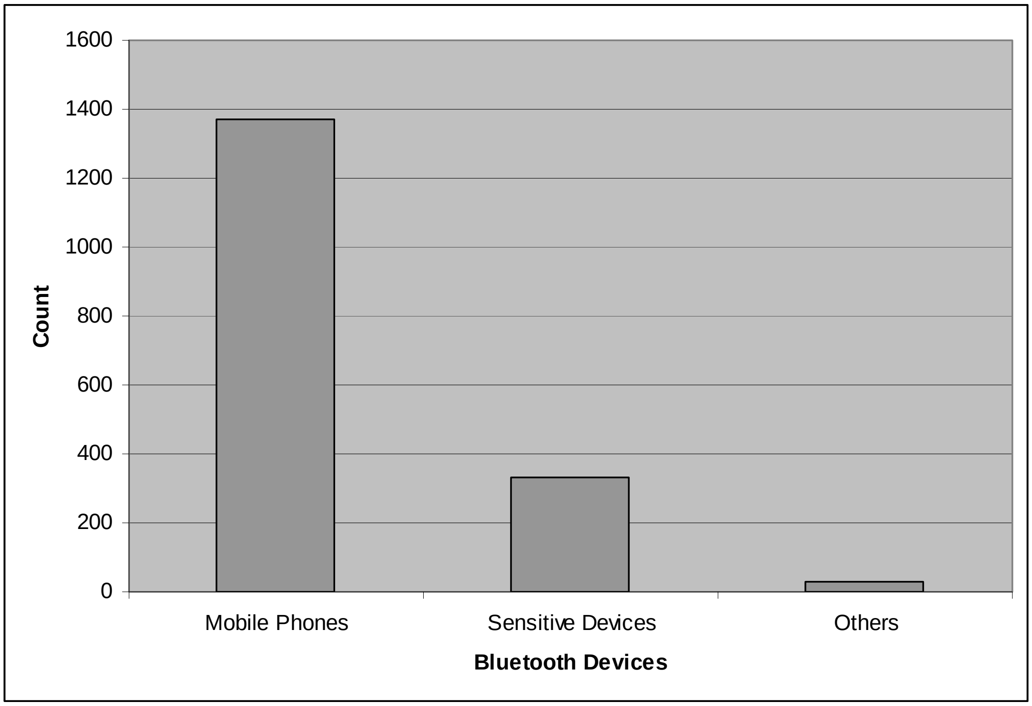

Figure 4: Types of Bluetooth devices common in Perth, Western Australia

The sensitive devices column groups together all devices that may store sensitive data, such as smart phones, PDAs, and so on. Devices included in the "Others" column include all other devices, such as headsets or hands-free devices, cordless phones, and so on.

This figure shows that attackers in Perth could potentially access a large number of Bluetooth devices. While basic mobile phones currently far outnumber sensitive devices, it is likely that the ratio will change in favour of sensitive devices over time, and even at present the number of sensitive devices is considerable. This suggests that a risk exists currently and is likely to grow in the future.

It is also interesting to examine which manufacturers' devices are common. This information is illustrated in the following figure.

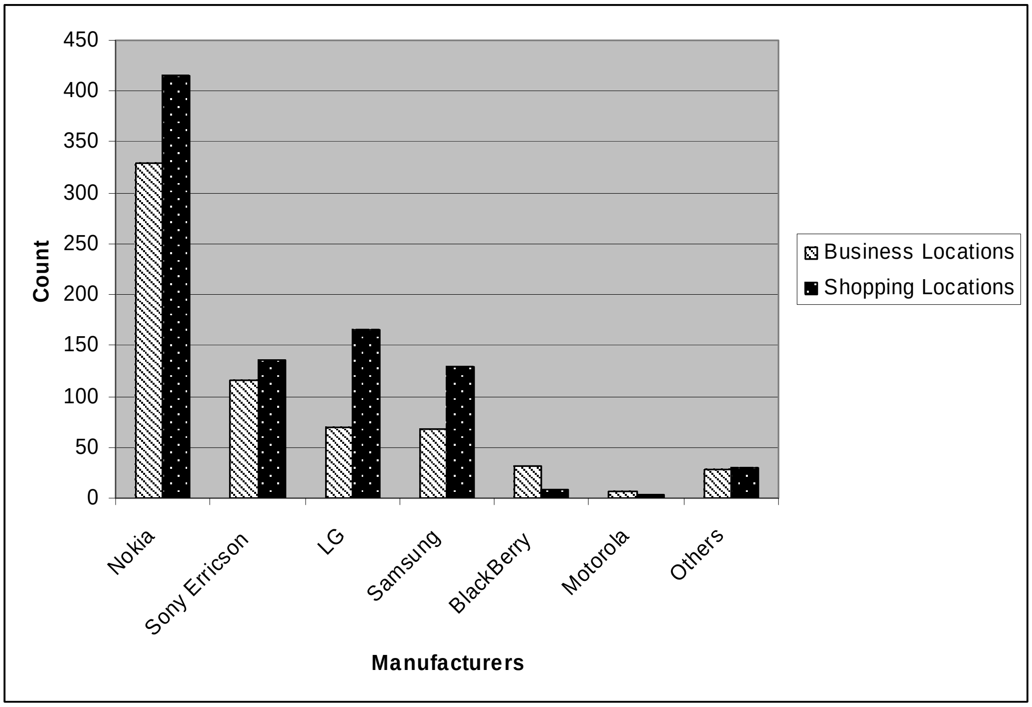

Figure 5: Manufacturers in business locations and shopping locations

The figure indicates that Nokia is clearly the most common brand of Bluetooth device in Perth; this, of course, is not surprising since Nokia is a world leader in mobile communications devices. The impact for Bluetooth security is that an attack such as a virus or worm aimed at Nokia devices could spread quickly, since the more homogeneous the network, the more rapidly a virus or worm will spread (O'Donnell and Sethu, 2005). Further, there is considerable amount of information about Nokia products available on the Internet, including information about security, due to the popularity of Nokia-branded products around the world.

It is concluded that mobile phones are the most frequently encountered Bluetooth devices in Perth, but sensitive devices form a sizable proportion of the total. The results also raise the question why there were so many of these devices with Bluetooth enabled; the researchers speculate that the reason so many Bluetooth devices were discovered is because of the popularity of Bluetooth hands-free devices. Many users may use Bluetooth only for this purpose, and consequently Bluetooth is permanently enabled on their phones. It is not realistic to expect users to disable Bluetooth, and it is also acknowledged that no software is perfect – flaws will always exist in any complex software – and therefore it is recommended that manufacturers of Bluetooth devices explore the possibility of users being able to configure which Bluetooth profiles are enabled.

6. Conclusions

To make conclusions about the current state of Bluetooth security in Perth, it is important to examine it with regard to different Bluetooth security risks. These risks are:

1. Disclosure of data
2. Unauthorised network access
3. Viruses and worms

6.1 Disclosure of Data

Disclosure of data is considered as a realistic Bluetooth security risk in Perth. The number of Bluetooth devices present, particularly those with GOEP and SYNC profiles enabled, combined with the proportion of Bluetooth devices that potentially contain sensitive information, suggests that security flaws in devices could have very serious consequences. Many such flaws have been discovered by attackers in the past and tools to exploit them are widely available. It is reasonable to expect this situation to continue, and therefore it is recommended that organisations take extreme care when adopting devices with Bluetooth capabilities.

The results suggest that Bluetooth attacks could occur in both business and shopping districts in Perth. Thus, there is a risk to personal privacy as well as to business, since many people store information, including pictures, of friends, family, and colleagues in their phones. In this way, a Bluetooth attack could exploit not only the privacy of the person who owns the phone but also of people they know, and contact details could be used by an attacker to gain further information through social engineering.

6.2 Unauthorised Network Access

The results also indicate that an intruder could initiate a Bluetooth attack with the aim of obtaining access to network services; about 30 percent of the total discovered devices recorded facilitated dial-up networking. Such an attack could leave the victim with a considerable financial loss, for example if the attacker instructed the mobile device to dial premium numbers (Jamaluddin *et al.*, 2004). An attacker could also use the victim's device to perform illegal activities, which could cause legal difficulties for the victim, for example if the device was instructed to download prohibited materials.

6.3 Viruses and Worms

The research suggests that a virus or worm propagated via Bluetooth could have a significant impact in Perth, given the prevalence of potentially insecure devices advertising GOEP or OPP profiles. Security experts believe that new viruses specifically created for mobile devices are likely to spread in the future (Leavitt, 2005).

Further, an interesting feature of the data collected revealed that key individuals could effectively become a kind of Bluetooth "Typhoid Mary" or "super-spreader". Several potentially vulnerable devices were consistently found in key locations such as office lobbies and cafés; conjecture by the researchers is that these devices belonged to employees such as a security guard, concierge or waiter. Regardless of the reason for the devices consistently being located in the same place, however, the effect of such a device becoming infected could be dramatic as they are likely to come within range of a very large number of other devices.

7. Future Research

There are a number of issues deserving of further research. First, to understand the nature of the risk, it would be useful to identify what data people store on Bluetooth devices. Such research could inform corporate security policies, and could also help efforts to build user awareness about the risks they can encounter when carrying an insecure Bluetooth device.

Second, the authors recommend research to determine the extent to which Bluetooth is acknowledged and addressed by corporate security policies, and the level of knowledge IT departments have about Bluetooth security.

Lastly, it would be useful to conduct simulations to determine the rate at which a worm or virus could spread throughout Perth. This would help to better understand the risk involved if an outbreak or such an attack were to occur.

8. References

BluetoothSIG (2007) *Profiles Overview: Bluetooth Wireless Technology Profiles*, Available: www.bluetooth.com/Bluetooth/Learn/Works/Profiles_Overview.htm, Accessed: 3 May 2007.

Dagon, D., Martin, T. & Starner, T. (2004) Mobile phones as computing devices: the viruses are coming!, *IEEE Pervasive Computing*, Vol. 3, No. 4, pp. 11-15.

Gostev, A. (2006) *Bluetooth: London 2006*, Available: www.viruslist.com/en/analysis?pubid=188833782 Accessed: 4 October 2006.

Gratton, D.A. (2002) *Bluetooth Profiles: The Definitive Guide*, Prentice Hall PTR.

Herfurt, M. (2004) *Bluesnarfing @ CeBIT 2004: Detecting and attacking Bluetooth-enable cellphones at the Hannover fairground*, Available: www.salzburgresearch.at/research/publications_detail_e.php?pub_id=152, Accessed: 24 August 2006.

InsightConsulting (2006) How can Bluetooth services and devices be effectively secured? Simple steps to stop the security blues slipping in through Bluetooth, *Computer & Fraud Security*, Vol. 2006, No. 1, pp. 4-7.

Jamaluddin, J., Zotou, N., Edwards, R. & Coulton, P. (2004) Mobile Phone Vulnerabilities: A New Generation of Malware, *Proceedings of the 2004 IEEE International Symposium on Consumer Electronics*, 1-3 September, Reading, UK.

Janssens, S. (2005) *Preliminary study: Bluetooth security*, Available: ftp.vub.ac.be/~sijansse/2e%20lic/BT/Voorstudie/PreliminaryStudy.pdf, Accessed: 24 August 2006.

Jellyellie (2004) *Detailed instructions on how to bluejack*, Available: www.bluejackq.com/how-to-bluejack.shtml, Accessed: 7 October 2006.

Leavitt, N. (2005) Mobile Phones: The Next Frontier for Hackers, *Computer Society*, Vol. 38, No. 4, pp. 20-23.

McDermott-Wells, P. (2005) What is Bluetooth?, *IEEE Potentials*, Vol. 23, No. 5, pp. 33-35.

McFedries, P. (2005) Bluetooth cavities, *IEEE Spectrum*, Vol. 42, No. 6, p. 88.

O'Donnell, A.J. & Sethu, H. (2005) Software Diversity as a Defense Against Viral Propagation: Models and Simulations, *Proceedings of the 19th Workshop on Principles of Advanced and Distributed Simulation*, 1-3 June.

Potter, B. (2005) Bluetooth attacks start to bite, *Network Security*, Vol. 2005, No. 2, pp. 14-15.

Potter, B. (2006) Bluetooth security moves, *Network Security*, Vol. 2006, No. 3, pp. 19-20.

Sairam, K.V.S.S.S.S., Gunasekaran, N. & Redd, S.R. (2002) Bluetooth in wireless communication, *IEEE Communications Magazine*, Vol. 40, No. 6, pp. 90-96.

Trifinite (2006a) *trifinite.downloads: trifinite.tools*, Available: trifinite.org/trifinite_downloads.html, Accessed: 5 October 2006.

Trifinite (2006b) *BlueSmack*, Available: trifinite.org/trifinite_stuff_bluesmack.html, Accessed: 5 October 2006.

Trifinite (2006c) *Blueprinting*, Available: trifinite.org/trifinite_stuff_blueprinting.html, Accessed: 5 October 2006.