Case Study on the Bluetooth Vulnerabilities in Mobile Devices

AJ.Solon, MJ.Callaghan, J.Harkin and TM.McGinnity,

Faculty of Engineering, University of Ulster, Derry, Northern Ireland

Summary

As the widespread use and acceptance of Bluetooth continues concerns are being raised related to security vulnerabilities and privacy issues inherent in the use of this technology. Inadequate device resources and lack of user awareness has compounded this issue where the emphasis on design constraints, functionality and ease of use sometimes outweigh security concerns. Recently some concerns have being highlighted relating to the possible security vulnerabilities in commonly used devices, and also the possibility of the imperceptible tracking of device users through the use of distributed and connected Bluetooth sensor nodes. This paper discusses some of these issues and highlights a number of vulnerabilities in the current generation of Bluetooth enabled devices. In particular, the current methods being used to exploit these vulnerabilities are discussed and the results from a case study are presented which identify the percentage of popular devices susceptible to this type of misuse.

Key words:

Bluetooth Security, Bluesnarfing, Bluebug, Privacy.

Introduction

Bluetooth is a short range wireless communication technology developed for home, office and mobile Personal Area Networks use [1]. In recent years Bluetooth has been successfully integrated into mobile phones, Personal Digital Assistants (PDAs) and other consumer devices. An essential element in ensuring the widespread adoption and utilisation of Bluetooth technology by the general public is the requirement for a low expectation of end user technical ability and minimum levels of user setup and configuration for ease of use. As a consequence some users are not aware of the functionality Bluetooth offers and its potential for exploitation and in many cases leave the default settings on their devices unchanged, a situation compounded by the relatively low power consumption of the Bluetooth chipsets and consequent impact on battery usage. Some commonly used Bluetooth enabled devices are vulnerable to exploitation using a range of methods including Bluesnarf [2], Backdoor [3] and Bluebug [4]. These vulnerabilities can expose the user to a range of issues relating to privacy and security and are explored here. In particular, the issue of user-tracking exploiting this technology is highlighted and the results of a recent case study are also presented on the percentage of popular devices which are susceptible to this type of misuse. Section 2 of this paper identifies a number of recent exploitation techniques and their implications. Section 3 discusses an architecture for the imperceptible and passive tracking of Bluetooth users and section 4 presents the results of a study related to the use of this architecture for passive tracking.

2. Bluetooth vulnerabilities

Bluesnarf attacks [2] are the use of Bluetooth technology to access restricted areas of a users' device without their knowledge or approval for the purpose of capturing data e.g. contacts, images, lists of called missed, received or dialed, calendars, business cards and the device's International Mobile Equipment Identity (IMEI). Bluesnarfing works by using the push profile of the Object Exchange protocol (OBEX) [5] which is built-in Bluetooth functionality for exchanging electronic business cards. Instead of pushing a business card the Bluesnarf attack pulls using a "get" request looking for files with known names e.g. phonebook file (telecom/pb.vcf) or calendar file (telecom/cal.vcs). This vulnerability exists due to the manner in which the OBEX push profile was implemented in some early Bluetooth phones, which did not require authentication from other Bluetooth devices attempting to communicate with it. Accessing information by Bluesnarfing was thought to only be possible if the users device is in "discoverable" or "visible" mode, but Bluesnarf attacks have being carried out on devices set to "non-discoverable" mode [2]. To achieve this the Bluesnarfing software needs to address the device by its unique 48-bit Bluetooth device name. For example, uncovering the device name is possible using software applications such as RedFang [6]. This application uses a brute-force approach to discover device addresses by systematically generating every possible combination of characters and recording those combinations which get a response. Fortunately this approach is time consuming, potentially taking hours of computation.

Manuscript received April 25, 2006.
Manuscript revised April 30 , 2006.

The subsequent release of the Bluetooth specification 1.2 [1] has addressed this problem by adding an anonymity mode that masks a device's Bluetooth physical address. In addition a major privacy concern related to this type of attack is the possibility of obtaining the IMEI of a device which can then be utilised to uniquely identify a phone on a mobile network and could also be used in illegal phone cloning. This could give someone the ability to use a cloned subscriber identity module (SIM) card to track a mobile device and by inference the user carrier without their knowledge. Recent firmware upgrades have corrected this problem but many phone owners have not installed them. A list of mobile phones which were vulnerable to the Bluesnarf attack are available here [2]. The Backdoor attack [2] involves establishing a trust relationship through a devices pairing mechanism and also ensuring that the established relationship no longer appears in the users register of paired devices. The only time the owner can be aware of the connection is if they are observing their device at the precise moment a connection is established. Once the pairing has being established the attacker will be able to utilise any resource on the target that the device allows access to without the owner's knowledge or consent, for example, file transfers and access to other services including the Internet, WAP and GPRS gateways. Once successfully completed the Backdoor attack enables other vulnerabilities, e.g. Bluesnarf without the usual restrictions applying. The Bluebug attack [2] creates a serial profile connection to a device giving full access to the AT command set which can then be exploited using widely available tools including PPP for networking and Gnokii [7] for messaging, contact management, diverts and initiating calls. Using this exploit it is possible to use the phone to initiate calls, send and read SMS messages, connect to data services and monitor conversations without the knowledge of the phone owner. Again a successful Bluebug attack enables other vulnerabilities e.g. Bluesnarfing. Recent firmware upgrades have corrected this problem but as before many phone owners have not installed them. A list of mobile phones vulnerable to the Bluebug type attacks are available here [2].

Each Bluetooth device is uniquely identified by a fixed address which an active Bluetooth chipset in visible mode (Inquiry Scan Mode enabled) openly discloses to devices scanning any given area. This need for visibility is a fundamental requirement for establishing Bluetooth connections but this characteristic could be misused with the potential to imperceptibly track the device user. Exploiting this characteristic requires a large number of synchronized and connected Bluetooth nodes which when correctly implemented could provide accurate data on the device user's movements within a fixed area, passively and without the owners' permission or awareness.

To further investigate the scope and implications of this issue an extended version of the Bluetrack system [8] from Rostock University in Germany was deployed over the University of Ulster, Magee campus covering a large physical area with a high concentration and throughput of pedestrian traffic. The Bluetrack system consists of distributed sensor nodes which actively retrieve information from Bluetooth devices within their range. This information includes a device's Bluetooth address, name and manufacturer which can then be time stamped and stored centrally for further analysis or manipulation. The next section discusses the system architecture and implementation process used to gather this data.

3. Bluetrack Implementation and Extensions

The Bluetrack system is illustrated in Fig. 1 and is composed of distributed Bluetooth inquiry nodes (transceivers) relaying detected device information back to a central server across a standard TCP/IP connection. The distributed nodes periodically scan their environment for Bluetooth enabled devices using the Bluetooth inquiry procedure. Data on any discovered devices are written to a server side database where it is time stamped and tagged showing where and when the device was discovered. Access to this data and system configuration is via a web browser. The stored data is then compared to the IEEE registration authority's Organizationally Unique Identifier (OUI) listing for registered Bluetooth addresses which identifies the device manufacturer [9].

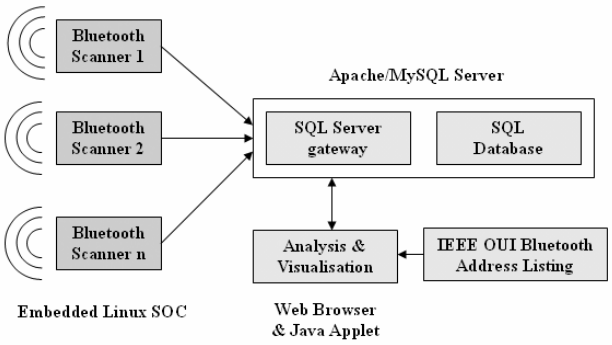
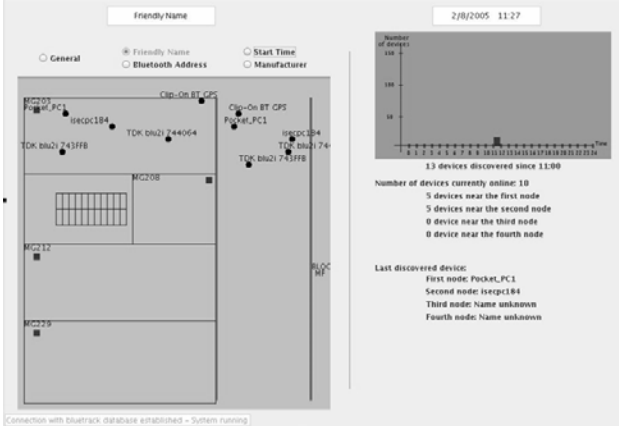


Fig. 1: System Architecture.

In addition the device model can be identified using the Bluetooth friendly name which over 20% of users leave as default on their devices and do not change after purchase. Fig.2 illustrates a Graphical User Interface (GUI) which was developed as a front end to the system which enhanced the default interface provided by the administration software on the server [10].



13 devices discovered since 11:00

Number of devices currently online: 10
5 devices near the first node
5 devices near the second node
0 device near the third node
0 device near the fourth node

Last discovered device:
First node: Pocket_PC1
Second node: isecpc184
Third node: Name unknown
Fourth node: Name unknown

Connection with bluetrack database established – System running

Fig. 2: Screenshot showing Bluetooth devices present.

The GUI consists of a map of the area covered by the nodes, the location of the transceivers (red squares) and the identified devices (black dots) with associated Bluetooth friendly name. The graph on the right hand side of the GUI displays the number of devices detected during user selected time scales and provides a range of statistics related to where devices were discovered and in what order.

4. Case Study

The data presented in this section was gathered over a five day period during the University autumn teaching semester using strategically placed nodes. In this study two issues will be investigated, firstly the percentage of commonly used devices with Bluetooth vulnerabilities and secondly, the use of Bluetooth technology as a means of passively and imperceptibly tracking device users.

4.1 Devices vulnerable to attack

Over 340 Bluetooth enabled devices were detected during the five day period of this study with the percentage of devices detected broken down by manufacturer comparable in magnitude to their market share [11]. Of the node devices detected 69 specific manufacturers and models using only the default Bluetooth friendly name on the mobile phone. Of these mobile devices 10 were found to be vulnerable to Bluesnarf or Bluebug attacks, however, none of the devices detected in this particular survey were at risk from a Backdoor attack. Fig.3 illustrates the percentage of the 69 detected vulnerable devices by manufacturer. If the level of model identification could be improved using Blueprint [12] for example, then based on the figures above, over 50 out of the 340 devices detected could be at risk to attack.

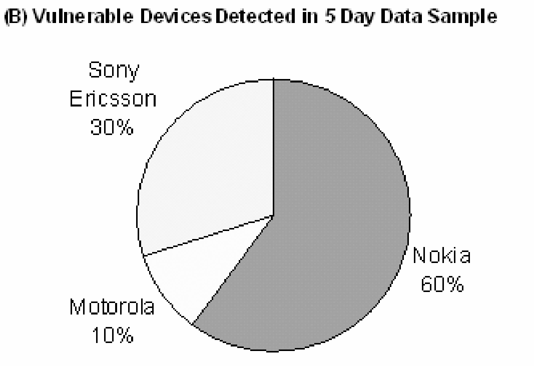


Fig. 3 Possible vulnerable devices detected by manufacturer

4.2 Passive user tracking

In addition to detecting devices vulnerable to attack, the possibility of using Bluetooth enabled devices to passively track users was also investigated. The detection system used in this study allowed the presence of a user in a particular area to be confirmed but with a limited level of accuracy. However, with the adoption of the new Bluetooth 1.2 standard [1] a more accurate level of device tracking should be feasible, as this standard proposes an "Inquiry with RSSI" mechanism that also measures signal strength. The tracking data recorded over a five day period detected an average of 115 unique devices on a daily basis. Figure 4 presents an example location profile of one mobile device with the Bluetooth friendly name GX25, which the system tracked. Through further investigation it was found that the device belonged to a student in the engineering building. Using this proposed detection system clearly highlights the student's attendance patterns during the day. The detected presence of GX25 on two different nodes ('isecWireless-128' located in room MG208 and the 'isecWireless-133' node in room MG203) was due to the close proximity of the nodes. This issue could be resolved by moving the nodes to ensure their areas of coverage do not overlap. Similarly Fig. 5 shows the detection of two devices (Linneything' and 'K700i') over a one day period. Again the issue of some overlap between nodes is a problem however it does show the users movements within the building and could be fine-tuned and extended if needed to get a more complete and accurate picture of their movements if needed. Statistics similar to Figures 4 and 5 could also be generated for any of the other 339 devices detected during the test period. However the examples presented provided a better profile of the benefits from tracking Bluetooth devices.

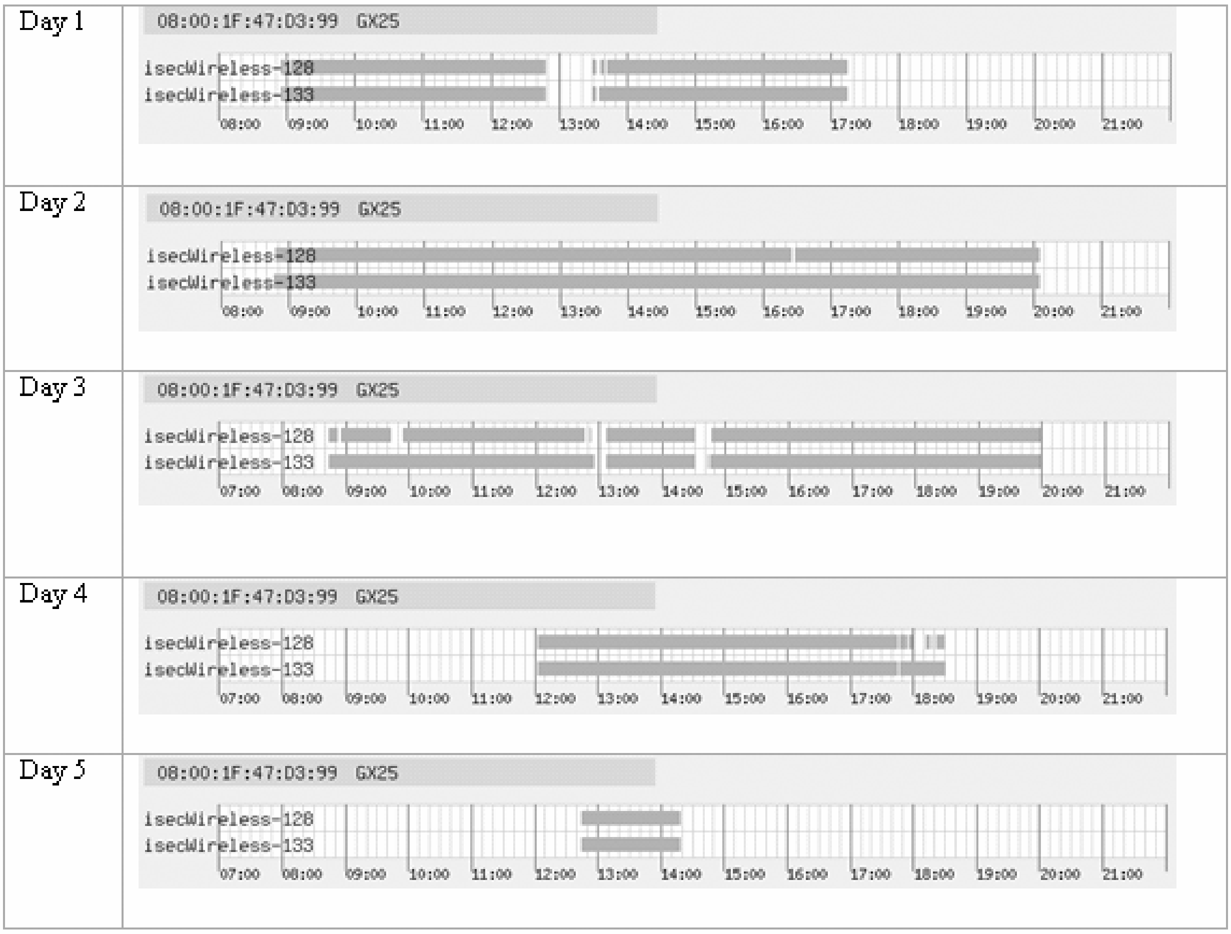


Fig. 4: Sample trace of device tracking data.

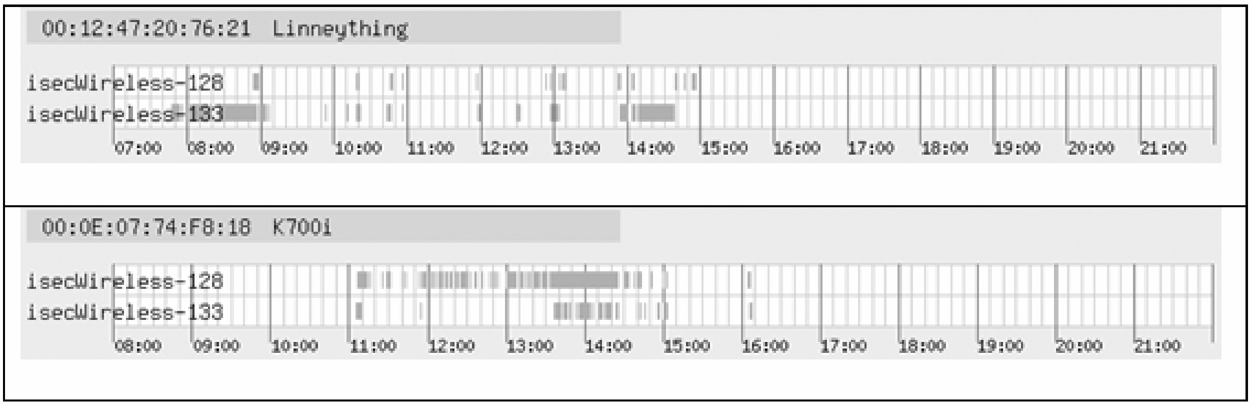


Fig. 5: Two samples of intermittent device tracking.

5. Summary and scope for future work

Nokia and Sony Ericsson have acknowledged the existence of these vulnerabilities and the potential for attacks of this nature on some of their mobile devices [13]. As a preventative measure both manufacturers advised users to set their Bluetooth devices to 'undiscoverable' or to simply turn the Bluetooth functionality off. Nokia stated that they will not be releasing a fix for vulnerable devices as the potential for attacks are limited and not expected to be a regular occurrence while Sony Ericsson advised their customers to upgrade their phones through a Sony Ericsson service centre [13]. In the short term this problem may continue to be an issue but given the short shelf live of many of these products will reduce in medium short term. The problem of user tracking is more complex as it is not clear how this issue could be resolved given that unique and invariant Bluetooth addresses are the fundamental prerequisite for establishing device connections. However, it may simply be a trade off between the potential sacrifice of an element of personal freedom, and the flexibility and functionality offered by Bluetooth technology. Future directions will investigate the possibility of using Blueprinting [12] in the detection system to increase the percentage of device models which can be identified.

References

[1] Official Bluetooth Website, http://www.bluetooth.com/, Site visited 02/12/05.

[2] B. L. & A. Laurie, "Serious flaws in Bluetooth security lead to disclosure of personal data", A.L. Digital Ltd. Technical report, http://bluestumbler.org/, Site visited 02/12/05.

[3] Herfurt, M., "Bluesnarf @ CeBIT 2004", Technical Report, Salzburg Research Forschungsgesellschaft mbH http://www.trifinite.org/Downloads/BlueSnarf_CeBIT2004.pdf.

[4] Haase, M., Handy, M., and D. Timmermann, "Bluetrack-Imperceptible Tracking of Bluetooth devices", UbiComp 2004, Nottingham, Great Britain, UK, September 2004.

[5] Bluetrack Project Homepage, http://www-md.e-technik.uni-rostock.de/forschung/projekte/BlueTrack, Site visited 02/12/05.

[6] RedFang Bluetooth Discovery Tool, http://www.securiteam.com/tools/5JP0I1FAAE.html, Site visited 02/12/05.

[7] Gnokii Toolkit Homepage, http://www.gnokii.org, Site visited 02/12/05.

[8] Haase, M., Nickel, T., Esins, S., and R. Möckel, "Bluetrack-Imperceptible Tracking of Bluetooth devices", CeBIT 2004 Poster presentation, http://www-md.e-technik.uni-rostock.de/ma/hm27/bluetrack-eng.pdf.

[9] IEEE Bluetooth OUI listing, Site visited 02/12/05. http://standards.ieee.org/regauth/oui/index.shtml,

[10] PhpMyAdmin Project Homepage, http://www.phpmyadmin.net, Site visited 02/12/05.

[11] IDC Western Europe Second Quarter Mobile Phone Report, http://www.idc.com, Site visited 02/12/05.

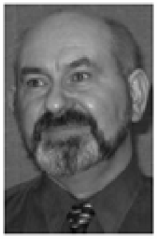
[12] Mulliner, C., and M. Herfurt, "Blueprinting - Remote Device Identification Techniques", 21st Chaos Communication Congress (21C3), Berlin, Germany, December 2004.

[13] ZDNet Technology News Homepage, http://news.zdnet.co.uk, Site visited 02/12/05.

Anthony Solon graduated from the University of Ulster in 2002 with an honors degree in Computing Science and a diploma in industrial studies. He is currently a Research Officer in the Intelligent Systems Engineering Laboratory at the University of Ulster and is completing a PhD in the area of Mobile Intelligent Multimedia.

Michael Callaghan is a Lecturer in the School of Computing and Intelligent Systems at the University of Ulster. He holds a Bachelor of Technology in Electronic Engineering and a Masters of Science in Computing and Design. He is a member of Intelligent Systems Engineering Laboratory with the University of Ulster.

Jim Harkin is a Lecturer in the School of Computing and Intelligent Systems at the University of Ulster. He holds a Bachelor of Technology in Electronic Engineering, Masters of Science and PhD from the University of Ulster, and is a member of the IEE. He is a member of Intelligent Systems Engineering Laboratory with the University of Ulster.



Martin McGinnity is Professor of Intelligent Systems Engineering at the University of Ulster. He holds a first class honors degree in physics, and a doctorate from the University of Durham. He is a Fellow of the IEE, member of the IEEE, and a Chartered Engineer and leads the research activities of the Intelligent Systems Engineering Laboratory. His research interests relate to the creation of intelligent computational systems and the area of intelligent systems in general.