©2008 IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.

A Simple Way to Improve the Security of Bluetooth Devices

Peter Dell
Curtin University of Technology
P.T.Dell@curtin.edu.au

Khwaja Shan-ul-Hasan Ghori
Curtin University of Technology
K.Ghori@curtin.edu.au

Abstract

Bluetooth is a de facto standard feature in mobile devices such as smart phones, PDAs and similar devices. While this provides great convenience to the user, there are a number of security issues for which exploits are widely available. This fact, combined with the growing sophistication of devices, creates the potential for serious loss in the event of a security breach. This paper investigates the use of Bluetooth profiles by the public and finds that some potentially high-risk profiles are not widely used. A subsequent investigation of a number of devices determined that no way of configuring individual profiles was available. The paper concludes with a recommendation that devices allow users to configure individual Bluetooth profiles.

1. Introduction

Bluetooth is a system for short-range wireless communication and is intended to allow devices within physical proximity of each other to communicate. As it is becoming universal among mobile devices, and as almost everybody has a mobile device, most people have a Bluetooth device in their possession most of the time.

The prevalence of Bluetooth devices makes possible a wide range of applications, such as proximity-based location services [1], mobile commerce applications such as 'eWallets' [2], and even triggering face-to-face interactions that would not otherwise occur [3].

However, as has been the experience with Internet-based e-commerce [4], the development of such applications would be hindered by problems with the underlying Bluetooth communication medium. Security problems, either real or perceived, can be a significant barrier to new technologies as they contribute to people's reluctance to use such systems.

This paper reports on a potentially serious – yet easily rectified – security issue with Bluetooth implementations in a wide range of mobile devices.

2. Security of Bluetooth profiles

Communication between Bluetooth devices is governed by profiles. These can be considered as use-cases, and essentially define parameters for the various protocols at different layers in the Bluetooth protocol stack to enable particular applications. Some profiles provide specialised applications and build on the services provided by more general profiles; consequently, profiles can be considered as hierarchical with dependencies existing between different layers of the hierarchy.

While some profiles provide only limited scope for security breaches, compromising others could potentially be very serious. For example, the Advanced Audio Distribution Profile (A2DP) provides a wireless audio service that typically supports 'walkman' functionality; if it were compromised the consequences would not be particularly severe in most cases. On the other hand, profiles such as Dial-up Networking (DUN) or SIM Access Profile (SAP) could potentially allow the attacker to access network services at the expense of the device owner, and compromising Serial Port Profile (SPP) or Generic Object Exchange Profile (GOEP) could lead to disclosure of confidential data stored on the device. With the increasing prevalence of 'smart phones', Personal Digital Assistants (PDAs), Blackberries and similar devices – with large storage capacities and access to a wide range of network services – comes a growing risk of damage as a result of these latter security breaches.

Services implemented using these profiles can be advertised using Service Discovery Protocol (SDP), itself based on Service Discovery Application Profile (SDAP) and which is becoming increasingly widespread. SDP is a client-server protocol that allows Bluetooth devices to browse the services offered by other devices or to search for specific services.

978-0-7695-3297-4/08 $25.00 © 2008 IEEE
DOI 10.1109/SAINT.2008.39

IEEE computer society

Although the standard does allow for authentication, this is optional and SDP is typically not authenticated. Consequently, it is possible to remotely determine the profiles available on practically any Bluetooth device that supports SDP.

Where Bluetooth profiles are authenticated, this is typically provided by a PIN (Personal Identification Number), raising significant security concerns. Although the Bluetooth standard suggests that there should be ever-increasing delays between PIN attempts to defeat brute-force cracking, this can easily be circumvented by the attacker changing their Bluetooth address between each attempt [5]. Further, Bluetooth PINs can often be cracked in less than a second after eavesdropping the Bluetooth pairing process [6]. For these reasons, and given that the majority of Bluetooth PINs are four-digit numbers – despite the standard permitting up to 16 digits being used – Bluetooth PIN authentication should not be regarded as secure.

The security risk posed by Bluetooth is not just theoretical; a growing number of tools to carry out attacks can be obtained easily from the Internet, some of which are described in Table 1.

Compounding the risk, a number of research projects have demonstrated that potentially insecure Bluetooth devices can commonly be found in urban areas [7, 8, 9, 10, 11]. Further, such devices are often within range for sufficient time for attacks to be carried out [7].

Clearly, then, there is widespread potential for damage such as information or service theft. A wide range of profiles is advertised by many devices and it seems likely that in some cases these services are not actually used. For example, consider the hypothetical scenario of a user who enables Bluetooth in order to use a Bluetooth headset, and in doing so enables a range of other services that they never use. This creates an unnecessary security risk to the user for no benefit whatsoever.

In order to determine the proportion of people exposed to this risk, this paper reports results of a web-based survey to determine which Bluetooth services are actually used by device owners. The survey was composed of two sections; the first obtained demographic details and whether the respondent used Bluetooth; if Bluetooth was used, the respondent was prompted with questions from the second section to obtain data about how Bluetooth was used. Note that the second section did not refer to specific Bluetooth profiles, but rather asked users about which actions they performed using Bluetooth. This was done for two reasons: first, most respondents would be unlikely to understand technical profile names such as "Object Push Profile". Second, there is considerable similarity between various profiles; for example, Hands-Free Profile and Headset Profile both provide the user with much the same functionality, albeit via different implementations. A list of the actions assessed by the survey is provided in Table 2.

Table 1. Common Bluetooth attacks and tools

Attack	*Description*
Information theft	The most common form of this attack is known as BlueSnarfing. Examples of software to conduct these attacks are *Bloover*, which attacks phones supporting J2ME, and *HeloMoto*, which attacks some Motorola V-Series phones. Further, many attacks can be devised using the standard tools available in Linux.
Service theft	Using the victim's device to access network services such as telephony or SMS. An example of this attack is the *Mosquito* virus, which sends SMS messages from the victim's device.
Denial of service	Deliberately consuming resources on the victim's device so as to prevent legitimate use. An example is the *BlueSmack* tool, which can immediately disable a range of Bluetooth devices.
BlueJacking	BlueJacking involves sending short, unsolicited messages to the target device. While not particularly serious, this attack could potentially be used to over-write information in the victim's phonebook. *BlueJack* is also the name of a tool commonly used to perform this kind of attack.
BluePrinting	Tools such as *BlueStumbler*, *RedFang* and *BluePrint* can be used to identify details such as the make, model and unique address of a Bluetooth device. While not an attack in itself, identifying these details can facilitate subsequent attacks of other types.
BlueBugging	In BlueBug attacks the attacker creates a serial connection to the victim's device without the need for authentication. The connection can subsequently be used to conduct information and service theft attacks. Many tools can be used to conduct this kind of attack, including *Gnokii*, a suite of open-source Bluetooth utilities.

Table 2. Bluetooth actions assessed by the survey

Synchronising contact, calendar or email data between my mobile/cell phone and PC
Connecting a wireless headset to my mobile/cell phone
Using my mobile/cell phone with a car kit
Uploading files to my mobile/cell phone via Bluetooth
Downloading files from my mobile/cell phone via Bluetooth
Using my mobile/cell phone as a dial-up modem
Using my mobile/cell phone to send faxes
Using my mobile/cell phone as a portable media or MP3 player
Other (please specify)

3. Results

The survey attracted 123 responses, the vast majority of whom (78%) were between the ages of 20 and 39. Responses were received from 14 countries, however just over half of the responses (54%) were received from Australia. Chi-squared testing revealed no significant difference between Australian and other responses ($\chi 2 = 3.551$, $p = 0.314$).

It was considered that that results might have been skewed by the high proportion of respondents in the 'Computer or IT professional' category (35% of respondents), who could be more or less likely to use Bluetooth features than other respondents. Statistical analysis again revealed no significant correlation between respondents membership of this category and their use of Bluetooth, however ($\chi 2 = 4.802$, $p = 0.187$).

Some functions were considerably more popular than others. Figure 1 illustrates the percentage of Bluetooth users who used each function. The most popular application is transferring files between mobile phone and PC. It is likely that transferring ring-tones is partly responsible for this, as well as the prevalence of cameras in mobile phones leading to the transfer of photographs to the user's PC.

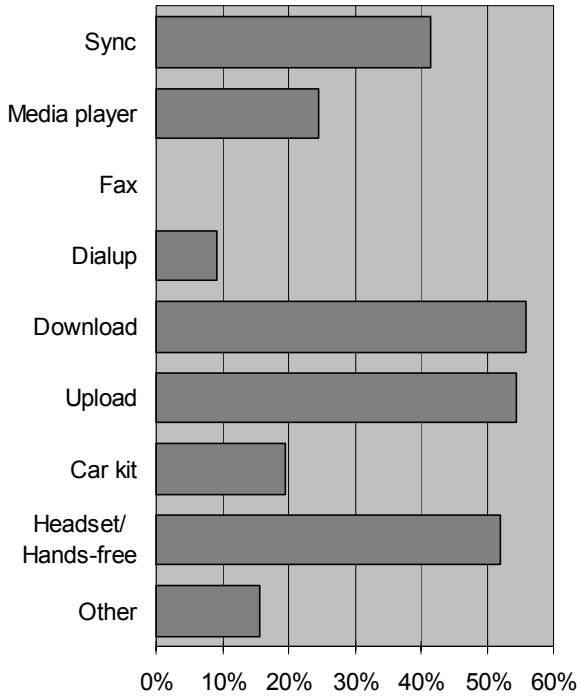

Figure 1. Relative popularity of Bluetooth functions

Only two functions were reported by a majority of Bluetooth users: uploading and downloading files, and using a headset or hands-free device. The marked difference in popularity between different applications also supports the hypothesis that a considerable proportion of users are required to enable services they do not use.

To further explore this problem, a range of phones were tested to determine which profiles that may pose more serious security risks were advertised. Results of this testing are summarised in Table 3. None of the devices tested allowed users to configure individual profiles, yet all devices advertised a range of profiles that are unlikely to all be required.

Table 3. Profiles advertised by various devices

Device	*DUN*	*OPP*	*SYNC*	*GOEP*	*SPP*
Compaq iPaq		Y			Y
I-mate PDA	Y	Y			Y
LG KE970	Y	Y			
LG TU 550		Y	Y		Y
Motorola RAZR maxxV6	Y	Y			
Motorola V360	Y	Y			
Motorola V3i	Y	Y			
Nokia 6120 Classic	Y	Y	Y		
Nokia 6280	Y	Y	Y	Y	Y
Nokia 6600	Y	Y		Y	Y
Sony Ericsson K610i	Y	Y		Y	Y

Most alarming about these results is the popularity of the Dial-Up Networking profile. 33% of Bluetooth devices detected in a field study [7] advertised the Dialup Networking service and nine of the eleven devices tested also advertised this service if Bluetooth was enabled, yet only 9% of the Bluetooth users in this survey reported actually using this service. Clearly, this presents an unnecessary risk for a large number of devices. Other profiles also appear to present unnecessary risks to lesser degrees.

Also alarming in these figures is the popularity of the Serial Port Profile (SPP), which provides the basis for a number of other profiles including SIM Access, Dial-up Networking, File Transfer Profile and Synchronization Profile. Thus, even if SPP is not used specifically, compromising this profile might allow an attacker the ability to compromise these other services.

A last, interesting footnote in the data is that one respondent who reported "Other" Bluetooth uses explicitly specified "Bluesniffing, BlueSnarfing and Bluejacking" as the other purposes for which they used it. While a single respondent obviously has no statistical significance, this serves to amplify the warnings about potential Bluetooth security risks.

4. Conclusions

The security of mobile/cell phone and similar devices could be improved by allowing the user to turn off individual profiles, and we recommend that device manufacturers provide this functionality in user interfaces. This will help to provide a more secure platform for the wide range of applications for which Bluetooth can be used.

5. References

[1] C. Steinfield, "The Development of Location Based Services in Mobile Commerce", In B. Priessl, H. Bouwman, and C. Steinfield (eds.), *Elife After the Dot.Com Bust*, Springer, Berlin, 2004, pp. 177-197

[2] S. Buttery and A. Sago, "Future applications of Bluetooth", *BT Technology Journal*, 21(3), 2003, pp. 48-55.

[3] N. Eagle and A. Pentland, "Social Serendipity: Mobilizing Social Software", *Pervasive Computing*, 4(2), 2005, pp. 28-34.

[4] S. Elliot and S. Fowell, "Expectations versus reality: a snapshot of consumer experiences with Internet retailing", *International Journal of Information Management*, 20(5), 2000, pp. 323-336.

[5] O. Whitehouse, "Bluetooth: Red Fang, Blue Fang", CanSecWest 2004, http://cansecwest.com/csw04archive.html.

[6] Y. Shaked and A. Wool, "Cracking the Bluetooth PIN", *Proceedings of the Third International Conference on Mobile Systems, Applications, and Services*, June 6-8, 2005, Seattle.

[7] K.S. Ghori and P. Dell, "Is Perth a Secure Place? A Western Australian Field Study of Bluetooth Security", *Proceedings of the International Telecommunications Society Asia-Australasian Regional Conference*, Perth, Western Australia, August 26-28, 2007.

[8] A. Gostev. *Bluetooth: London 2006*, http://www.viruslist.com/en/analysis?pubid=188833782.

[9] A.J. Solon, M.J. Callaghan, J. Harkin and T.M. McGinnity, "Case Study on the Bluetooth Vulnerabilities in Mobile Devices", *International Journal of Computer Science and Network Security*, 6(4), 2006, pp. 125-129.

[10] J. Su, K.K.W. Chan, A.G. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara and A. Goel, "A Preliminary Investigation of Worm Infections in a Bluetooth Environment", *Proceedings of the 4th ACM Workshop on Recurring Malcode*, Association for Computing Machinery, 2006, pp. 9-16.

[11] M. Herfurt (2004) *Bluesnarfing @ CeBIT 2004: Detecting and attacking Bluetooth-enable cellphones at the Hannover fairground*, Salzburg Research.