(12) UK Patent Application (19) GB (11) 2 439 364 (13) A

(43) Date of A Publication 27.12.2007

(21) Application No: 0612120.6

(22) Date of Filing: 19.06.2006

(71) Applicant(s):
Symbian Software Ltd
(Incorporated in the United Kingdom)
2-6 Boundary Row, Southwark, LONDON, SE1 8HP, United Kingdom

(72) Inventor(s):
John Turner
Tim Howes

(74) Agent and/or Address for Service:
Symbian Software Ltd
2-6 Boundary Row, Southwark, LONDON, SE1 8HP, United Kingdom

(51) INT CL:
H04M 11/00 (2006.01) ***H04L 12/56*** (2006.01)
H04M 1/00 (2006.01) ***H04Q 7/38*** (2006.01)

(52) UK CL (Edition X):
H4L LDGR LDGX LEUD LRCMS

(56) Documents Cited:
GB 2412819 A **GB 2409789 A**
US 20030050009 A1 **US 20020044661 A1**

(58) Field of Search:
UK CL (Edition X) **H4L**
INT CL **H04L, H04M, H04Q**
Other: **Online : wpi ; epodoc ; paj**

(54) Abstract Title**: Security in bluetooth enabled computing devices**

(57) A Bluetooth-equipped device is provided with a maintained list of banned devices from which no connection will be accepted. This enables a destination device to avoid receiving malware or other connections with malicious intent from Bluetooth-equipped source devices whose identity is on the banned device list without any user intervention. In a preferred embodiment a Bluetooth profiles permission bitmap may be used to permit access to the destination device to be granted on a per-service basis instead of having to trust the source device with access to all available services, as is currently the case.

Petitioner has added line numbering to all pages and romanettes to pages (i)-(iv). Otherwise, it leaves the original page numbering.

MICROSOFT CORP.
EXHIBIT 1228

Original Printed on Recycled Paper

GB 2 439 364 A

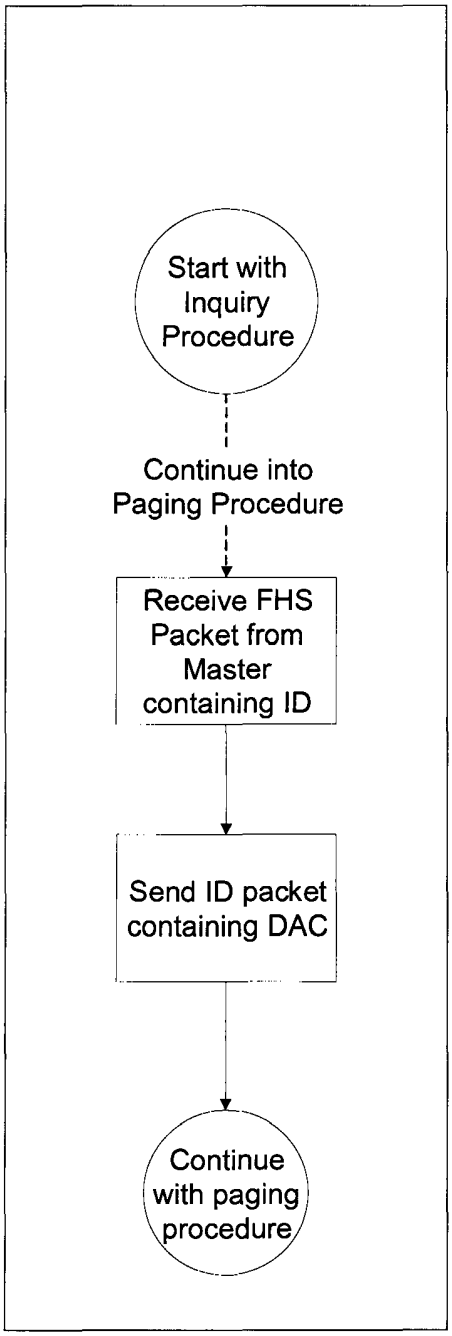
Start with Inquiry Procedure
Continue into Paging Procedure
Receive FHS Packet from Master containing ID
Send ID packet containing DAC
Continue with paging procedure

Figure 1

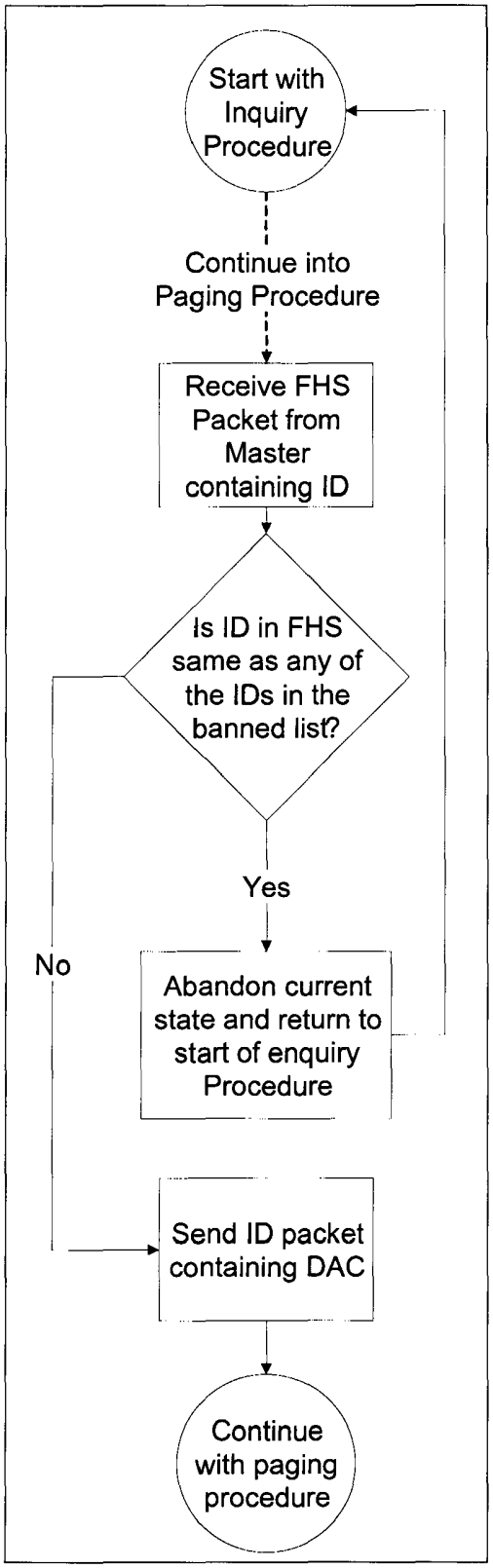
Start with Inquiry Procedure
Continue into Paging Procedure
Receive FHS Packet from Master containing ID
Is ID in FHS same as any of the IDs in the banned list?
Yes
No
Abandon current state and return to start of enquiry Procedure
Send ID packet containing DAC
Continue with paging procedure

Figure 2

GAP	Generic Access Profile	1
SDAP	Service Discovery Application Profile	1
CTP	Cordless Telephony Profile	0
IP	Intercom Profile	0
SPP	Serial Port Profile	1
HS	Headset Profile	1
DNP	Dial-up Networking Profile	0
FP	Fax Profile	0
LAP	Local Area Network Access Profile	0
GOEP	Generic Object Exchange Profile	0
OPP	Object Push Profile	0
FTP	File Transfer Profile	0
SP	Synchronization Profile	0
ESDP	Extended Service Discovery Profile	0
A2DP	Advanced Audio Distribution Profile	0
AVRCP	Audio Video Remote Control Profile	0
BIP	Basic Imaging Profile	0
BPP	Basic Printing Profile	0
CIP	Common ISDN Access Profile	0
GAVDP	Generic Audio Video Distribution Profile	0
HFR	Hands-Free Profile	1
HCRP	Hardcopy Cable Replacement Profile	0
HID	Human Interface Device Profile	0
PAN	Personal Area Networking Profile	0
SAP	SIM Access Profile	0

Bluetooth Profile Permissions Bitmap 110011000000000000010000

Figure 3

2439364

Improving Security in Bluetooth Enabled Computing Devices

This invention discloses improvements in the security of Bluetooth-enabled computing devices.

The term 'computing device' includes, limitation, Desktop and Laptop computers, Personal Digital Assistants (PDAs), Mobile Telephones, Smartphones, Digital Cameras and Digital Music Players. It also includes converged devices incorporating the functionality of one or more of the classes of such devices, together with many other industrial and domestic electronic appliances.

In the last ten years, it has become increasingly common for computing devices to be equipped with wireless networking technologies. One of these is Bluetooth™, also known as IEEE 802.15.1, a short-range wireless technology enabling various types of computing devices to be interconnected for a variety of purposes. Full details of the protocols and the hardware appear on the official Bluetooth web site at http://www.bluetooth.com.

Although Bluetooth can be used to wirelessly connect any type of computing device to any other, because of its low power consumption and its ability to eliminate the need to carry around bulky cables, it has become particularly popular for use in conjunction with portable battery operated devices such as mobile telephones and personal digital assistants (PDAs).

For example, Bluetooth headsets for mobile telephones are in widespread use, replacing the wired hands-free version. Other common uses for this technology in portable devices include linking them to desktop computers for the transfer of files and synchronisation of various types of data, and the use of Bluetooth to send messages between one mobile device and another, including multimedia messages that may include sound, photographs, and video clips.

But because Bluetooth technology can also be used to create ad-hoc wireless connections that can transfer any type of data between one device and another, it has become a target for anyone searching for security flaws in protocols that might allow them unauthorised access to Bluetooth-enabled

computing devices. Bluetooth has the potential to become a vehicle for the transmission of malicious programs (known as *malware*) such as computer viruses and trojan horses. It is known that this type of infection can invade any type of computing device, and the risk is significantly greater when a computing device is able to connect to other devices.

Bluetooth does provide various security mechanisms that can be used to prevent unwanted connections to a device and a subsequent infection by malware. These include verifying the authenticity of the remote device and asking the user whether they wish to accept the connection. Furthermore, if a connection does result in some type of file transfer, users can be prompted as to whether they wish to accept such a transfer. If they do accept a transfer, and an executable program file is transferred to them, they can also be prompted as to whether they wish to install or run the executable program. Should the program appear to originate from an unknown or untrusted source, a further warning can be given.

Despite the security measures described above, which can require a user of a Bluetooth device to accept an initial connection and ignore three further warnings, it is known that users of Bluetooth-enabled devices are becoming infected by malware. For example, users of mobile telephones running Symbian OS, the advanced operating system for smartphones from Symbian Ltd, have been targeted by malware such as the so called 'Cabir' 'Mabir' and 'Lasco' worms, which are capable of spreading from one mobile telephone to another via Bluetooth connections.

Despite the multiple positive decisions that a user has to make and the warnings they have to ignore, BBC reports indicate that this type of infection has been found in 17 different countries (see http://news.bbc.co.uk/1/hi/technology/4445125.stm). It is clear, therefore, that users do not always heed warnings given at the installation phase about the dangers of untrusted software.

In order to understand why this is so, let us consider the following scenario, which corresponds fairly closely to the way that malware such as Cabir spreads from one device to another. An item of malware running on device A keeps trying to create a connection to device B to transmit a copy of itself,

thereby infecting device B. Because of the repeated connection attempts, the user of device B will be bombarded with questions as to whether they should accept the connection from device A. Refusing the request means they will be asked the same question again in a few seconds, requiring another refusal, followed by another request, and so on.

In such a situation, the user has a limited number of options:

1. Switch off the phone. Users are understandably reluctant to do this.
2. Switch Bluetooth off. This is likely to be inconvenient, most obviously when the user is relying on a Bluetooth device such as a headset.
3. Switch Bluetooth to *non-discoverable* mode, which prevents the device from responding to inquiry requests from other Bluetooth devices. Doing this means that it will not be possible to initiate a session with any devices that haven't been communicated with previously; this is less drastic than switching off either the phone or the Bluetooth functionality, but does mean that all welcome inquiries are prevented as well as all unwelcome ones.
4. Physically move out of range of the remote device. Again, this may not be possible, especially since Bluetooth is not directional and there is no way of telling where the requests are coming from.
5. Deny each individual connection attempt. This is tiresome; the continual requests for connection are such a nuisance that the user is worn down, and comes to believe that the only way to stop the continual requests for connection is to ignore the warnings and accept a copy of the malware onto their device.

The perception behind this invention is that there is a weakness in the Bluetooth specifications in that they provide no mechanism which can be used to block any single given remote device from making any connections to the local device. This invention provides a remedy for this weakness, and enables a Bluetooth enabled device to maintain a list of remote devices from which all connection requests will be ignored without reference to the user.

According to a first aspect of the present invention there is provided a method of operating a first computing device having Bluetooth wireless networking

capability, the method comprising maintaining a list of unique identifiers of banned computing devices on the first computing device, whereby the first computing device is able to avoid accepting a connection from a second computing device seeking without user intervention if the unique identity of the second computing device matches an identifier in the list.

According to a second aspect of the present invention there is provided a computing device arranged to operate in accordance with a method of the first aspect.

According to a third aspect of the present invention there is provided an operating system for causing a computing device to operate in accordance with a method of the first aspect.

Embodiments of the present invention will now be described, by way of further example only, with reference to the accompanying drawings, in which:-

Figure 1 shows a paging procedure between Bluetooth equipped devices in accordance with the prior art;

Figure 2 shows a paging procedure between Bluetooth equipped devices in accordance with the present invention; and

Figure 3 shows a list of Bluetooth profiles, including an example of a Bluetooth profiles permissions bitmap.

Those skilled in the art will be aware that most Bluetooth stack implementations are able to maintain, at the request of the user, a list of *paired* and trusted devices. This list is used by the Bluetooth security manager to bypass some of the Bluetooth security mechanisms. In particular, devices on the paired list maintain stored link keys which can be used for authentication purposes with no user interaction.

In this invention, a complementary list of *banned* devices is maintained by the Bluetooth security manager. The complementary list contents can be a straightforward list of the unique IDs that are allocated to all Bluetooth devices; these are similar to the unique MAC addresses allocated to Ethernet network cards, and are 48 bits long.

The ID of any device seeking to establish a connection (which would be either a *source* or a *master* device in Bluetooth parlance) is always disclosed in the FHS (Frequency Hopping Synchronization) packet that the seeking device sends as part of the Bluetooth *paging procedure* to any other computing device (which would be a *destination* or a *slave* device in Bluetooth parlance) with which it was seeking to establish a connection.

Prior to this invention, a Bluetooth slave device participating in the paging procedure would have received this FHS packet from the master, and would have responded by entering step 2 of the slave response state and then sent the master an ID packet containing its device access code. This procedure is shown in figure 1.

However, a slave device implementing this invention is arranged to store a list of banned devices to which access via a Bluetooth connection will always be denied. Hence, the slave device firstly compares the transmitted ID of the master contained in the FHS with the ID entries in its banned list; if there is a match, then the slave device remains silent and neither responds to the FHS packet nor continues with the specified steps of the slave response states. It terminates all participation in the paging procedure and returns to the start of the inquiry procedure, when it may once again be discovered by source devices. This procedure is shown in figure 2.

This invention does not prevent the source Bluetooth device from attempting to page the destination device again; nor does it prevent the source Bluetooth device from seeking to re-discover the destination device via the enquiry phase. What this invention does do is ensure that as soon as a device implementing it finds out that the ID source device is on its banned list, it immediately terminates the session completely transparently from the user of the device, whose user experience is thereby improved, and who would not be repeatedly paged into accepting an unwanted connection simply to make the repeated paging requests go away.

A number of mechanisms can be used to add Bluetooth IDs to the banned list. These may include without being limited to the following:

1. Giving the user the option to add the ID of a source device to the banned list whenever they refuse a connection attempt from the device.
2. Automatically adding the ID of a source device to the list after a certain number of refused connection attempts, either in total or within a given time period.
3. Adding an ID to the list if it had been received from a known and trusted source; so, for example, an infected device in a particular physical environment such as a company site could be effectively quarantined from all devices in the environment.

An extension of this invention permits the security mechanisms of the Bluetooth paging procedure to allow per-profile configuration. Bluetooth *profiles* are separate collections of various mandatory and optional elements and parameters of the Bluetooth protocols and specifications each of which define a particular set of functionality. A list of the currently available Bluetooth profiles is shown in Figure 3.

At present, without this invention, once a source device is trusted by a destination, the source device can gain access to all the services provided by any Bluetooth profile that might be available on the destination. In order to prevent this dangerously wide access, the banned list described above can be modified by replacing it with a table that links device IDs in paired tuples with a permissions bitmap signifying which Bluetooth profiles that those IDs would be allowed to access. The usual convention for such a bitmap would be for a zero (0) bit to represent a barred service and for a set (1) bit to represent allowed services. Figure 3 shows a permissions bitmap for a Bluetooth headset, where the bitmap 110011000000000000010000 indicates that the (mandatory) Generic Access Profile and Service Discovery Application Profile are both allowable, together with the Headset Profile and Hands-free Profile, and the Serial Port Profile on which they both depend.

In conjunction with a default permissions bitmap, this table would effectively function as both a blacklist and as a whitelist. Any Bluetooth source device whose ID did not appear in the table would be able to use the default set of

permissions; but this set could be restricted or extended for any device whose ID did appear in the table.

Thus, a completely banned ID would have its ID paired with a bitmap in which all bits were zero, and a totally trusted ID would have its ID paired with a bitmap in which all the bits were set to 1.

Between these extremes, a destination device would implement either per-profile configuration at the level of the mandatory Service Discovery Application Profile (SDAP), or per-service configuration at the level of the Bluetooth Service Discovery Protocol (SDP) on which SDAP depends. In either case, the responses that the destination device gives to the source device would depend not on the actual capabilities of the device, but would depend on the permissions bitmap of the source device. The destination device would deny the availability of any profiles or services to which the client did not have permission to access. This would effectively bar an unauthorised device from accessing them.

Alternatively, a destination device could immediately terminate any Bluetooth connection for any source device where the table indicated that the required profile or service had been disallowed but would permit an extension where the table indicated that the required profile or service was allowable.

By means of this extension, a user may trust a source device that wished to send pictures to them without notification, but the user would not necessarily want that same device to have open access to their Bluetooth telephony or modem functionality; this would expose the user to having their communications hijacked by a malicious user (which is an attack known as *bluebugging*).

A principle benefit of the list of banned or blacklisted devices is that it can be used to at least reduce the spread of viruses such as Cabir and its variants by means of Bluetooth. It can also minimise the effect of denial-of-service attacks, in which a device is continually bombarded with connection requests from a malicious source.

In the extended version of the invention using the Bluetooth profiles permissions bitmap, it permits access to a destination device to be granted on

a per-service basis instead of having to trust a source device with access to all available services, as is currently the case.

Although the present invention has been described with reference to particular embodiments, it will be appreciated that modifications may be effected whilst remaining within the scope of the present invention as defined by the appended claims.

Claims:

1. A method of operating a first computing device having Bluetooth wireless networking capability, the method comprising maintaining a list of unique identifiers of banned computing devices on the first computing device, whereby the first computing device is able to avoid accepting a connection from a second computing device seeking without user intervention if the unique identity of the second computing device matches an identifier in the list.

2. A method according to claim 1 wherein the first computing device obtains the unique identity of the second computing device from the FHS packet transmitted as part of a paging procedure.

3. A method according to claim 1 or claim 2 wherein a refusal by the first computing device of a connection attempt by the second computing device causes the unique identity of the second computing device to be added to the list.

4. A method according to claim 1 or claim 2 wherein a refusal by the first computing device of a connection attempt by the second computing device causes the unique identity of the second computing device to be added to the list only if the number of such refusals exceeds a threshold set either by the manufacturer or the user of the device.

5. A method according to claim 1 or claim 2 wherein the first computing device adds the unique identity of the second computing device to the list in response to a notification received from a third party by electronic or other means.

6. A method according to any one of the preceding claims wherein the list comprises a table containing unique identifiers and permissions bitmaps for indicating services allowed for a device corresponding to any unique identifier, and in which the first computing device

automatically refuses connections if the respective permission bitmap for the unique identifier of the second computing device indicates that the service it has requested is barred.

7. A method according to claim 6 wherein a default permissions bitmap is used by the first computing device when the unique identifier of the second computing device does not appear in the table.

8. A method according to claim 6 wherein the first computing device refuses a connection attempt by the second computing device prior to any services being requested if the permission bitmap paired with its unique identifier indicates that all services are banned.

9. A computing device arranged to operate in accordance with a method as claimed in any one of claims 1 to 8.

10. An operating system for causing a computing device to operate in accordance with a method as claimed in any one of claims 1 to 8.

The Patent Office

For Innovation

11

Application No: GB0612120.6 **Examiner:** Mr Richard Howe

Claims searched: 1-10 **Date of search:** 5 September 2006

Patents Act 1977: Search Report under Section 17

Documents considered to be relevant:

Category	Relevant to claims	Identity of document and passage or figure of particular relevance
A	1,9,10	GB2412819 A Nokia - see abstract
A	1,9,10	GB2409789 A Nokia - see abstract
A	1,9,10	US2003/0050009 A1 Kurisko et al - see abstract
A	1,9,10	US2002/0044661 A1 Jakobsson et al - see abstract

Categories:

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art
Y	Document indicating lack of inventive step if combined with one or more other documents of same category	P	Document published on or after the declared priority date but before the filing date of this invention
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application

Field of Search:

Search of GB, EP, WO & US patent documents classified in the following areas of the UKC^{X} :

H4L

Worldwide search of patent documents classified in the following areas of the IPC

H04L; H04M; H04Q

The following online and other databases have been used in the preparation of this search report

Online : wpi ; epodoc ; paj