



Development of Tool for Managing Bluetooth Data Transfer Logs in Mobile Platform

Olaiya Folorunsho*

Department of Computer Science
Oye-Ekiti, Nigeria

Mariam Biola Bello

Department of Computer Science Federal University,
Achievers University, Owo, Nigeria

Abstract—The Bluetooth System has a unique connection establishment procedure. Its uniqueness is due to the fact that Bluetooth units know nothing about one another prior to connection. Bluetooth transfer log is an application used to keep the record of the files that are been sent out and received. The following tasks have to be performed by the Bluetooth unit for a connection to be established: find out the address of the device to be connected to, guess the clock of the device's clock. In this paper, the Bluetooth transfer log was designed using Java platform (Netbeans). The result show that two or more nokia devices could kept the information concerning the time in which the file was sent, the name of file, then afterward to clear log, a picture password has to be generated by the server.

Keywords: Bluetooth System, Transfer Log, Java Platform, Picture Password, Server

1. Introduction

Bluetooth is a proprietary open wireless technology standard for exchanging data over short distances (using short wavelength radio transmissions in the ISM band from 2400-2480 MHz) from fixed and mobile devices, creating personal area networks (PANs) with high levels of security. Created by telecoms vendor Ericsson in 1994, it was originally conceived as a wireless alternative to RS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Wireless Bluetooth technology is a universal specification that facilitates communication between mobile phones, laptops or other portable devices. The idea behind the Bluetooth technology is to support short range wireless transmissions in an universal way by using the unlicensed 2,4GHz short-range radio frequency bandwidth. Bluetooth allows users to form clusters of 8 maximum connected devices that form a star shaped network named a piconet. The main device from the cluster is named a master; all other devices are named slaves. Two Bluetooth devices can transfer data with a maximum speed of 2.1Mbps. In order to minimize the interference between different piconet structures Bluetooth uses a radio technology called frequency hopping spread spectrum (FHSS). This is accomplished by using an algorithm for a pseudo-random frequency changing from a set of 79 frequencies.

1.1 Bluetooth Management

Bluetooth is managed by the Bluetooth Special Interest Group, which has more than 15,000 member companies in the areas of telecommunication, computing, networking, and consumer electronics. [Newton, 2007] The SIG oversees the development of the specification, manages the qualification program, and protects the trademarks. To be marketed as a Bluetooth device, it must be qualified to standards defined by the SIG. A network of patents is required to implement the technology and is only licensed to those qualifying devices; thus the protocol, whilst open, may be regarded as proprietary.

1.1.1 Uses

Bluetooth is a standard wire-replacement communications protocol primarily designed for low power consumption, with a short range (power-class-dependent, but effective ranges vary in practice; see table below) based on low-cost transceiver microchips in each device (Newton, 2007). Because the devices use a radio (broadcast) communications system, they do not have to be in visual line of sight of each other, however a quasi-optical wireless path must be viable. [Newton, 2007]

Table 1.1: Power-class-dependent ranges vary.

Class	Maximum Permitted Power		Range (m)
	(mW)	(dBm)	
Class 1	100	20	~100
Class 2	2.5	4	~10
Class 3	1	0	~5

The effective range varies due to propagation conditions, material coverage, production sample variations, antenna configurations and battery conditions. In most cases the effective range of class 2 devices is extended if they connect to a class 1 transceiver, compared to a pure class 2 network. This is accomplished by the higher sensitivity and transmission power of Class 1 devices.

Table 1.2: Power-class-dependent range vary

Version	Data rate	Maximum application throughput
Version 1.2	1 Mbit/s	0.7 Mbit/s
Version 2.0 + Enhanced Data Rate(EDR)	3 Mbit/s	2.1 Mbit/s
Version 3.0 + High Speed (HS)	See Version 3.0 + High Speed.	
Version 4.0	See Version 4.OLE	

1.1.2. Bluetooth Profiles

To use Bluetooth wireless technology, a device has to be able to interpret certain Bluetooth profiles, which are definitions of possible applications and specify general behaviors that Bluetooth enabled devices use to communicate with other Bluetooth devices. These profiles include settings to parameterize and to control the communication from start. Adherence to profiles saves the time for transmitting the parameters anew before the bi-directional link becomes effective. There are a wide range of Bluetooth profiles that describe many different types of applications or use cases for devices.

1.1.3. Bluetooth Profile Mismatch

If you want two Bluetooth enabled devices to work together, they need to have the same profile. This is in reality a lot simpler than it sounds, and for the most part, profiles will match if the two devices are related to each other. For instance, if you wanted to connect a mobile phone to a headset, then you would need to have the same profile in both devices. In this case, the hands free profile would be required. If there is data that a user has on your mobile phone and needs to print off, both the phone and the printer will need the basic printing profile.

For Bluetooth devices to connect to each other so they can work together, they need to be paired. Pairing or bonding means that the two devices are exchanging their passwords or passkeys. Once paired, all of the data that is sent between the two devices is encrypted, meaning that any device that is not paired with the other two is unable to translate the data. However, there are occasions when pairing is not necessary, such as exchanging business cards. There is a setting on most devices to lower the security for these lower grade transfers. For mobile devices (e.g. mobile phones) bonding mostly does not initiate any form of security authentications.

Staying with pairing, another error message that you may come across is that devices “cannot be found”. This is normally because the device you are trying to connect to either is off, or is not in “discoverable mode”. To solve this issue, you simply need to turn the device you are trying to connect to on, or switch it into discoverable mode. If you are scared that someone will hack into your device, you can always turn it back to non-discoverable mode after you are finished. However, Bluetooth technology is quite robust as far as security is concerned. Research has shown that mobile phones with Bluetooth devices do not keep any form of user activity log and do not employ any method of authentication. This research will provide a tool that can be installed for Bluetooth devices on mobile phone to keep log of data transfer and provide a means of authentication to initiate sharing.

1.4 Picture Password Algorithm

Picture Password is a visual login technique that matches the capabilities and limitations of most handheld devices and provides a simple and intuitive way for users to authenticate.

This technique selects the image to clear the log of the Bluetooth transfer. The user must provide the image that was used during the clearing of transfer log. If the image chosen to clear the log is not equal to the image used as what has been set to clear log, the user will not be allowed to log clear the transfer log

A user selects one image to form password and an images. Every image has been assigned its alphanumeric values thus the calculations of the user password details are based on the stored values.

2.1. BLUETOOTH PROTOCOL ARCHITECTURE

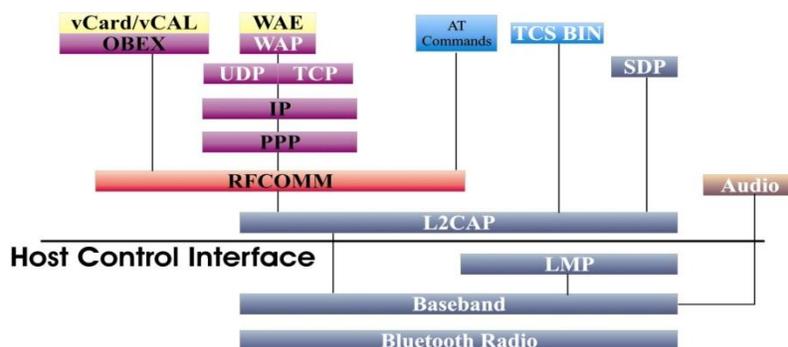


Fig. 2.1: Bluetooth Specification Protocol Stack

3.0. OVERVIEW OF THE PROPOSED SYSTEM

The design and development process was done using Netbeans to develop a Bluetooth log with following steps.

- Develop the file transfer log; file that contains separate lines for requests, i.e. the data sent and the data receive
- Develop a public pin; designated authority as an encryption key that combines with private key from the sender derived from the public key used to receive data
- Develop the device log
- Insert a picture based password to clear log

Picture Password is a visual login technique that matches the capabilities and limitations of most handheld devices and provides a simple and intuitive way for users to authenticate.

This technique selects the image to clear the log of the Bluetooth transfer. The user must provide the image that was used during the clearing of transfer log. If the image chosen to clear the log is not equal to the image used as what as been set to clear log, the user will not be allowed to log clear the transfer log.

Every image has been assigned its alphanumeric values thus the calculations of the user password details are based on the stored values

- Design the Graphical User Interface (GUI)
Bluetooth technology is quite robust as far as security is concerned. Research has shown that mobile phones with Bluetooth devices do not keep any form of user activity log and do not employ any method of authentication. This research will provide a tool that can be installed for Bluetooth devices on mobile phone to keep log of data transfer and provide a means of authentication to initiate sharing. It is pertinent to be security conscious when it comes to file handling on devices especially mobile phones. File can easily be transferred without the owner of the device noticing any crooked transaction on the mobile device.

4.0 INTEGRATION OF SYSTEM COMPONENTS

4.1 Build automation

In order to integrate all the components of the design, a java-based build tool known as Apache Ant was used. A build tool is a programming utility that is used when building a new version of a program and Apache Ant is a software tool for automating software build processes. It was implemented using the Java language, requires the Java platform, and is best suited to building Java projects. Ant uses XML to describe the build process and its dependencies and the default the XML file is named build.xml. Build automation is the act of scripting or automating a wide variety of tasks that software developers do in their day-to-day activities including things like:

- Compiling computer source code into binary code
- Packaging binary code
- Running tests
- Deployment to production systems
- Creating documentation and or release notes.

4.2 Packaging

In order to ensure that the developed application installs seamlessly on any Mobile Phone, the Midlets package consists of a JAD and a JAR file. We describe these two parts in the following subsections.

4.2.1 JAD Files

Java Application Descriptor (JAD) is a single text file containing information about the MIDlet. The information stored in this file depends on the version of Mobile Information Data Program (MIDP) in our project its version 2.0. It comprises the path where the JAR file can be downloaded.

4.2.2 JAR Files

The JAR files (Java Archive Files) hold the Manifest file that contains some of the attributes of the JAD file and also contains all classes of the MIDlet and the resources it needs. The reason for storing the same information in the JAD and JAR files is for verification of the vendor of the MIDlet application.

4.3 OPERATION OF THE SYSTEM



Fig. 4.1: The application home page

ing for Bluetooth devices in the vicinity

Fig 4.2: When searching for bluetooth devices in the vicinity



Fig 4.3: The list of bluetooth devices it found, if any of the client or server dont have the application,file wont be sent to device found



Fig 4.4: Application page for selecting data that should be transferred

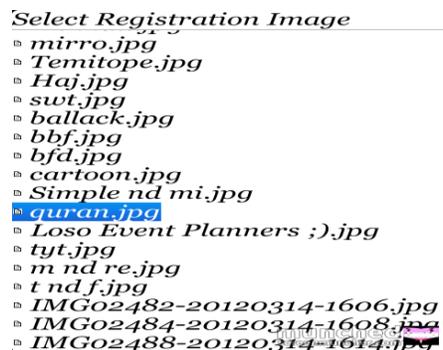


Fig 4.5: Page phase of after registration of image the user would like to use to clear log,after when the data has been sent to the client.

Registration Image



Fig 4.6: Page phase of regristrating the image

Verify using Image

- system/
- store/
- SDCard/



Fig 4.7: here is the opposite phase of the application, after when the user has registered am image. this is for theb clearing of the log, when the image is verified the log clears automatically.

Verify using Image

- Temitope.jpg
- Haj.jpg
- swt.jpg
- ballack.jpg
- bbf.jpg
- bfd.jpg
- cartoon.jpg
- Simple nd mi.jpg
- quran.jpg
- Loso Event Planners ;) .jpg
- tyt.jpg
- m nd re.jpg
- t nd f.jpg
- IMG02482-20120314-1606.jpg
- IMG02484-20120314-1608.jpg
- IMG02488-20120314-1614.jpg
- IMG02481-20120314-1606.jpg

Fig 4.8: Verifying using the image been registered

Verification Image



Fig 4.9: Image been verified.

After all the following steps are taken the system takes the itemised actions;

- INSTALISING CYPTOSYSTEM
- SAVING KEY
- SUCCESSFUL
- LOG DELETED

4.6 Experimental Setup

PHONE Client/server	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
RESULT	S	S	F	S	S	S	F	F	S						

Table 4.1: Experimental setup
S – Successful F- Fail

4.7 Result

Connection is been established by pairing with the other device, the file is then transferred from the client to the server. The log is automatically kept as a result of transfer log. The server registers a picture password, so no client can clear the log. Before the log can be clear the server has to verify the picture password which he/she has registered. After the imagine has been registered, cryptosystem is installed, it saves the key and then it means the log is successfully cleared

5.0 Conclusion

Bluetooth transfer enable one to secure, data transfer from one mobile to another with password and surpassed by new generation because this brilliant technology brings a lot of knowledge and surprise. Java is a versatile language used to create any application for any platform; nowadays the mobile technology is very important. An opportunity to design and develop an application for mobile is great because this technology is growing everyday and Bluetooth is the future warehouse technology that is growing fast. This device will provide a tool for creating a log after when data is been sent from one device to another which have moved beyond mere sending by focusing on accuracy and security measure.

References

[1] Beynon-Davies, P. (2004). "Database Systems, 3rd Edition", Palgrave, Houndmills, Basingstoke.

[2] Date, C. J. (2003), "an introduction to database Systems, Fifth Edition", Addison Wesley ISBN 0-201-51381-1.

[3] J. Haartsen, "Bluetooth towards ubiquitous wireless connectivity," Revue HF, Soc. Belge Ing. Telecommun. & Electron, pp. 8–16, 2000.

[4] Roh .J.S, (2006) .“Performance analysis and evaluation of Bluetooth networks in wireless channel environment,” in ICSNC '06: Proceedings of the International Conference on Systems and Networks Communication. Washington, DC, USA: IEEE Computer Society, pp. 61–65.

[5] Kardach, Jim (2008-05-03). "How Bluetooth got its name" . Retrieved 2009-02-24.

Kroenke, David M. and David J. Auer, Database concepts, 3rd Ed. New York: Prentice, 2007.

[6] Lightstone, S.; Teorey, T.; Nadeau, T. (2007). Physical Database Design: the database professionals guide to exploiting indexes, views, storage, and more. Morgan Kaufmann Press ISBN 0-12- 369389-6.

[7] Monson, Heidi (1999-12-14). "Bluetooth Technology and Implications" . SysOpt.com. Retrieved 2009-02-17.

[8] Newton, Harold. (2007). Newton’s telecom dictionary. New York: Flatiron Publishing.