COPYRIGHT © 2011 IJCIT, ISSN 2078-5828 (PRINT), ISSN 2218-5224 (ONLINE), VOLUME 01, ISSUE 02, MANUSCRIPT CODE: 110109

Modified Approach of RFCOMM Implementation to Protect Bluetooth Technology from Bluebug Attack

Hasbiha Hossain, Upama Kabir *and* Shaila Rahman

Abstract— Bluetooth wireless technology is an inexpensive, short-range radio technology that eliminates the need for proprietary cabling between devices such as notebook PCs, hand held PCs, personal digital assistants (PDAs), cameras, and printers etc. This thesis paper provides an overview of Bluetooth technology, protocol stack, some of the Vulnerabilities, risks and also protection technique of bluetooth enables mobile phones. Bluetooth enable mobile phone exchanges important data or files, image, sms, personal videos etc. When bluetooth is turn on, it is time to attack from attacker. Some brilliant attacker wants to take scope to harm bluetooth enable mobile phones by using proper steps. BlueBug is the name of a bluetooth security loophole on some bluetooth enabled cell phones. By bluebug attack, a mobile phone can be damaged or lost important information .Not only they can make calls, they can send messages, read phone books, examine calendars, etc. When a user put balance in mobile , it can be make zero by bluebug attack. It is a dangerous attack. Attacker uses rfcomm for communication between two devices. But bluetooth rfcomm has no authentication and attacker use this scope. In this thesis my vision is to protect bluetooth enable device from attacker by proposing a modified approach of RFCOMM implementation.

Index Terms— Host Controller Interface, Object Exchange Protocol, Service Discovery Protocol, Radio Frequency Communication.

1 INTRODUCTION

WIRELESS technology is a great invention of modern science. The technology refers electromagnetic waves to transmit the signal, which can travel through the space and also received by the antenna. Now a day, two years baby communicates with his father by mobile phone. So, men try to keep in touch with technology. Bluetooth is an example of wireless radio technology. Bluetooth exchanges data over short distance communication. Wi-Fi uses the same radio frequencies as bluetooth but with higher power where bluetooth is most famous for high speed data transfer and low power consumption.

Bluetooth logo is trademarked by the privately held trade association named the bluetooth Special Interest Group (SIG)[1]. Bluetooth devices into three different power classes Power Class 1 – long rang devices (100m), Power Class 2 – normal or standard range devices (10m), and Power Class 3 – short (10cm)-range operation.

- ***Hasbiha Hossain*** *is with the Department of Computer Science and Engineering, University of Asia Pacific (www.uap-bd.edu), Dhanmondi, Dhaka-1209, Bangladesh. E-mail: hasbiha@gmail.com.*
- ***Upama Kabir*** *is with the Department of Computer Science and Engineering, Dhaka University, Dhaka, Bangladesh. E-mail: upama@univdhaka.edu.*
- ***Shaila Rahman*** *is with the Department of Computer Science and Engineering, University of Asia Pacific (www.uap-bd.edu), Dhanmondi, Dhaka-1209, Bangladesh. E-mail: shaila@uap-bd.edu.*

2 BLUETOOTH TECHNOLOGY

Bluetooth is a cable replacement technology. It is standard for short range wireless communication [1]. Bluetooth was first invented by telecoms vendor Ericsson in 1994.

2.1 Bluetooth Features

Bluetooth has two way data transfer system [2]. Asynchronous Connectionless Communications Link (ACL).Synchronous Connection-orientated Communications Link (SCL). Bluetooth has 3 class. Bluetooth support ad hoc networking. Bluetooth network topologies called piconet and scatternet. It has low power, low cost, small size, and built-in security. It offer 2.4 GHz ISM band and frequency hopping techniques with the carrier modulated using Gaussian frequency shift keying (GFSK). It has 79 channels.

2.2 How Does Bluetooth Work?

Bluetooth is dynamic and very fast technology. Bluetooth architecture is not easy, rather it is complex. It connects other device by using frequency hopping in time slots .It creates ad hoc networks. When bluetooth devices first connect, a piconet master initiates the connection, others are slave devices. Piconet has one master device, seven active slave devices .There is no direct communication between slave units [3]. Two or more piconets create scatternet, a master is only one piconet. Any devices that share a master must be on the same piconet. Different piconets have a common device which is scatternet member to relay data

between the piconets.

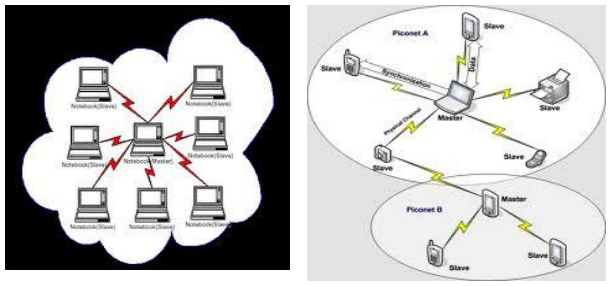

Fig. 1: Bluetooth Piconet and Scatternet

In piconet, if slave device see a device want to communicate directly to each other, they create a new piconet, among them one acting as a Master.

2.3 Figures

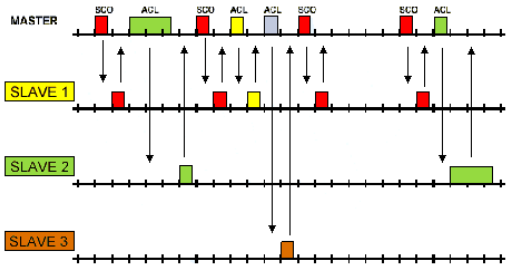

Fig. 2: Bluetooth working Procedure

3 BLUETOOTH PROTOCOL STACK

In bluetooth protocol stack, radio layer is the lowest layer. It avoids interference from other signals by hopping to a new frequency after transmitting or receiving a packet. RF operation uses a shaped, binary frequency modulation to minimize transceiver complexity.

Bluetooth base band layer is upward of radio layer. It manages physical channels and links. This layer checks error correction, data whitening, hop selection and bluetooth security.

LMP provide link setup, authentication, and link configuration.

A host controller interface creates command line access to the baseband layer and LMP for control and to receive status information.

L2CAP provides data services to the upper level host protocols. It provides connection-oriented and connectionless data services. It has multiplexing capability, segmentation and reassembly operation, and group abstractions [15].

RFCOMM provides a simple reliable data stream to the user, similar to TCP. It support two device types modems; computers and printers. TCS used to setup and control speech and data calls between Bluetooth devices [4].

SDP used to detect which services are available and what type of characteristics of those services and what parameters are used to connect to them. When a mobile phone connect to a bluetooth headset, SDP browse and check bluetooth profiles and the protocol multiplexer settings needed to connect to each of them.

OBEX is used for simple data exchange (object push, file transfer, basic imaging, basic printing, phone book access, etc.). It is similar to Hypertext Transfer Protocol (HTTP) but it does not require the resources that an HTTP server requires.

AT protocol use for telephony modem. AT commands provide for bluetooth device, make/break connections and inquiry.

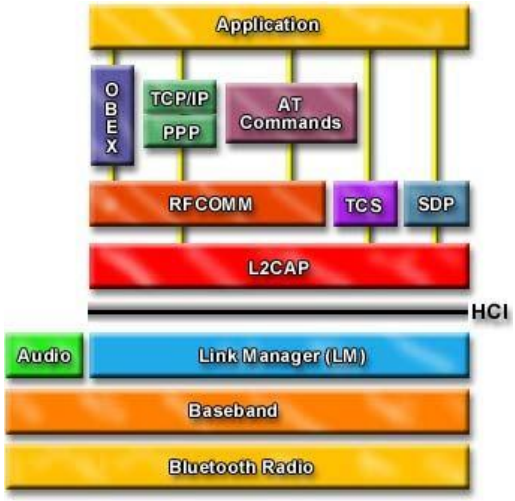

Fig. 3: Bluetooth Architecture

4 BLUETOOTH SECURITY

While bluetooth has its benefits, bluetooth has some vulnerability. These vulnerability occur bluetooth insecure [5]. Bluetooth is susceptible to spying and remote access, it also susceptible to denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation.

4.1 Bluebug Attack

Bluebugging is a hacking mechanism [6]. It is dangerous and most powerful attack where an attacker hack mobile phone. It takes total control of a victim's phone .It allows hackers to reading/writing phone book entries ,send/read sms, call numbers, monitor phone calls and causing costs on the vulnerable phones .It also do everything that backdoor and bluesnarfing allows. Bluebugging caused by lack of awareness, which means that anyone with the right knowledge and tool and take control a phone. Bluebug user can listen to any conversation. It allows call forwarding, where user can receive calls .firmware update does not stop hackers from penetrating devices.

4.2 Attack procedure

After scanning Bluetooth mac address, sdptool browse that Bluetooth device. Attacker use Bluetooth rfcommProtocol for direct connection. With minicom tool modem initialization complete. AT commands to a mobile phone or GSM / GPRS modem use a terminal program. AT sends the characters to the mobile phone or GSM / GPRS modem. It then displays the response it receives from the mobile phone or GSM / GPRS modem on the screen. Now user ready to use dial with hacked mobile. Bluebugging is dangerous, where mobile phone balance can totally make zero in this way controlling power.

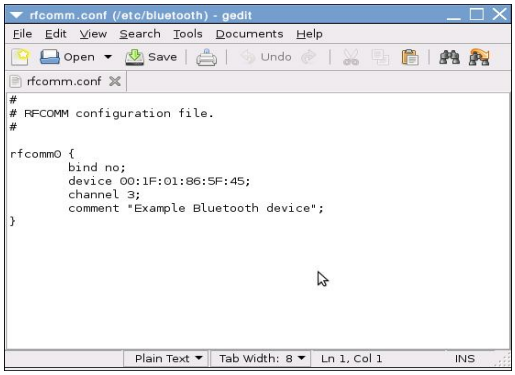

Fig. 4: RFCOMM configuration

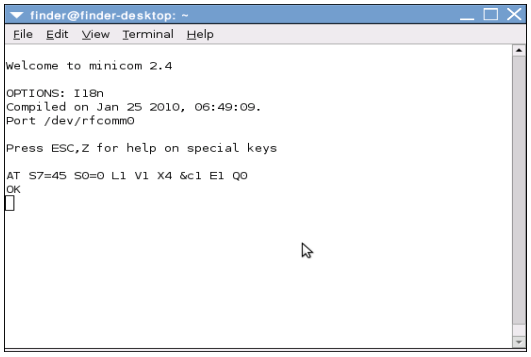

Fig. 5: Modem initialization

5 AUTHENTICATION APPROACH

RFCOMM is a direct connection between two devices.

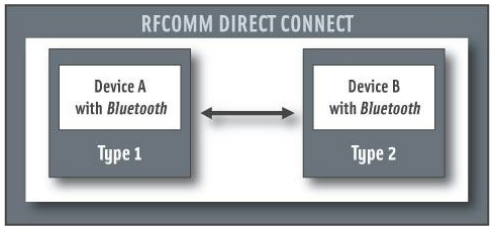

Fig. 6: RFCOMM direct connection

When hcitool scan and find bluetooth devices with mac address or bluetooth address, rfcomm bind the bd address to communicate. As there is no authentication or check, anybody like some hacker takes this scope. With this RFCOMM, attackers very easily enter the new device and establish direct connection without authentication.

6 IMPLEMENTATION

6.1 Thesis Proposal

The thesis has proposed authentication approach for protection of bluebug attack. For this reason, Rfcomm procedure should be modified with existing process. Rfcomm should be used database for bluetooth device address or Mac address .where database store all bluetooth device address with location, company name, description ,manufacturer date, it's time or when it come in market etc all necessary information. After scanning, when match the device address that is already registered or in database stored then rfcomm give permission to communicate the particular device, otherwise it should not get permission.

6.2 Modified Approach

```
// Algorithom rfcomm authentication function
rfcomm_check_btdevice
{

        List bd_addr[50];
        new bd_addr[50];
        var i;
        var n;
        //compare (list bd_addr[50],new bd_addr[50])

for(i=0;i<=n; i++){
        if(list bd_addr[i]!=new bd_addr[i])
        {
                list bd_addr[i]+=new bd_addr[i];
                show new bd_addr[i];
        }
        else
        {
                device_addr_register();
        }

}
device_addr_register()
{
        struct new_bd_addr[i];
        mysql_query(&mysql, "select bd_address from database");
        bdresult=mysql_store_result(&mysql);
        if(result == NULL)
        {
                printf(" bdresult == NULL\n");
        }
        else
```

```
                {
                        printf("bdresult found\n");

        while((row=mysql_fetch_row(result)) != NULL)
        {
                printf("%s\n",row[i]);
        }
                mysql_free_bdresult(bdresult);
        }
        mysql_close(connection);
        }
}
```

7 CONCLUSION

Bluetooth enable mobile phone users should be conscious. User should take following steps to protect from attack. User should not use the phone in areas, where it could be stolen and should keep an eye out for possible attackers. When phone not in use, should keep in a briefcase or purse or in a pocket, but should not put lying on the table, because anyone who distracts user attention can then grab it. User should to use SIM PIN code, because it protect account, other information. In this paper, I discuss about Bluetooth protocol stack, also discuss Bluetooth problems and have proposed solution of rfcomm modification.

ACKNOWLEDGMENT

At first I am grateful to God for giving me idea, brave and intelligence to select an interesting and realistic topic for my Master s thesis. I would like to express my gratitude who have encouraged me for my thesis. I would like to thank my thesis supervisor Upama kabir, Associate Professor, Department of Computer Science and Engineering, Dhaka University. Her helpful suggestions, guidance and constant support inspire me to do the thesis work.. She has been highly available throughout the whole process of this thesis. I am very grateful to Shaila Rahman, Assistant professor, Department of Computer Science and Engineering, The University of Asia Pacific, Dhaka, who help me and give me direction by heart and soul to complete my thesis. Without her help I cannot proceed. Special thanks to honorable Aloke Kumar Saha, Head, Department of Computer Science and Engineering, The University of Asia Pacific, Dhaka, who always help in my work and fulfill all essential. His useful advices always help me to build my aim.

REFERENCES

[1] Monson Heidi, "Bluetooth Technology and implications ", 1999.

[2] Colleen Rodes, "Bluetooth Security", East Carolina university, 2006.

[3] Johnson Consulting, "How does Bluetooth work", http://www.swedetrack.com/images/bluet13.htm, 2004

[4] Mr. Lawrence Harte,"Introduction to Bluetooth, Technology, Market, Operations, Profiles and services ",2008 ,2nd Edition.

[5] Marek Bialoglowy, " Bluetooth Security Review Part-1",2005, http://www.symantec.com/connect/articles/bluetooth-security-review-part-1

[6] Gary Legg, Design Article, "The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulnerability ", 2005, http://wikipedia.org/wiki/Bluebugging

Hasbiha Hossain has been serving as a Lecturer of Computer Studies in Stamford College. She joined Stamford College in June 2010. She has passed Non Government Teachers Registration Examination (NTRCA) at 2009.

Upama Kabir obtained her MSc degree from the Department of Computer Science, University of Dhaka, Bangladesh in 1999 and her MS in Computer Science and Engineering from University of New South Wales, Australia in 2005. She worked as a Lecturer (1999–2003),as Assistant Professor (2003–2007), and has been working as Associate Professor from 2007 in the Department of Computer Science and Engineering, University of Dhaka, Bangladesh. Currently she is pursuing her PhD in Concordia University, Canada. She has received several academic awards. Her research interests include parallel processing and distributed systems and computer networking. She has several research publications in national and international proceedings and journals.

Shaila Rahman joined in The University of Asia Pacific (UAP) at 1999 after completing her M.Sc from Dhaka University (DU). She secured 4th position in M.Sc. She also secured the 4th position in B.Sc (Hons) in Applied Physics & Electronics from the same institution. Shaila Rahman teaches courses on Computer Networks, Data Communications, Information Systems, Microprocessors, Assembly Language, Computer Interfacing, Digital System Design, C/C++, Data Structure and Algorithms. She is conducting the course Mobile Communication in Masters Program of CSE (MCSE). Her current research interest includes Computer Networks and Distributed System, Wireless Networks, Wireless Ad hoc network, Sensor Network, Network Security. She supervised the thesis works of several undergraduate students at UAP. It is praiseworthy to mention that more than fifteen thesis groups in undergraduate level completed successfully under her acute supervision. Her research works published in IEEE, ICCIT, NCCPB, ICCPB. Ms. Rahman has also published two journals on Cryptography and Outsourcing. Ms. Rahman serves as acting head when the head of the department remains on leave. She also serves as an external examiner in the CSE department of Dhaka University. Moreover, She is the convener of the Cultural and Debating club. She is also member of Research and Publication Unit and Programming Contest Club.