BLUETOOTH VULNERABILITIES ON SMART PHONES RUNNING IN IOS AND ANDROID OPERATING SYSTEM

Prepared by:

TARIQ ABDULAZIZ D FATANI

Supervisor:

DR BHARANIDHARAN SHANMUGAM

A project report submitted in partial fulfillment of the requirements for the award of degree of Master of Science (Information Security)

13 May 2013

DECLARATION

I declare that this thesis entitled “Bluetooth vulnerabilities on smart phones running in iOS and android operating system are the result of my own research except for citation in the references. The thesis has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Signature : ....

Name : ....

Date : ....

DEDICATION

To my beloved Mother and Family

ACKNOWLEDGMENT

In this project, there are several people I need to thank. Firstly, I would have not completed this project with the help and support of my supervisor Dr.Bharanidharan Shanmugam who gave me a lot of ideas for this project. He also gave me a positive perspective, guidance, courage for me to carry out my project. To you Dr, I thank you.

I have to thank God for giving me the blessed and built my inner strength to work on my project and having a great family that understands and care for me. In addition, thank you to all of my friends for the motivation and the knowledge we shared.

ABSTRAK

Teknologi Bluetooth menjadi sebahagian daripada kehidupan seharian kita. Ia dibina ke dalam banyak produk seperti telefon bimbit, komputer, kereta, dan peralatan perubatan. Selain itu, ia membolehkan perkongsian muzik, foto, video, dan lain-lain maklumat tanpa wayar di antara dua peranti berpasangan dengan menggunakan gelombang radio. Teknologi ini menghantar maklumat di dalam ruang peribadi anda sendiri, yang dipanggil Rangkaian Kawasan Peribadi anda atau "PAN (Personal Area Network)" pada jarak kurang daripada 10 meter. Kelemahan dan Exploitasi Bersama atau CVE (Common Vulnerabilities and Exploits) dan Pangkalan Data Kelemahan Negara telah mencatatkan peningkatan yang ketara dalam kelemahan yang dilaporkan dalam beberapa susunan popular perisian Bluetooth khas Symbian dan J2ME OS. Objektif kajian ini adalah untuk mencari kelemahan Bluetooth yang sedia ada di IOS dan Android OS dengan menggunakan alat yang ada yang mendakwa boleh atau dapat menembusi telefon bimbit Bluetooth dan berkemungkinan dapat mencari (kira-kira tiga) langkah-langkah pencegahan untuk keluar dari kelemahan. Metodologi kajian ini akan menjadi siasatan awal, analisis, ujian dan penilaian. Senario daripada experimen ini ialah dengan memasang semua alat serangan di mundur 5r4 dan rnu terhadap peranti telefon pintar dan memerhati pemberitahuan peranti bersama-sama dengan beberapa maklumat yang dapat dikumpul. Eksperimen telah membuktikan peranti telefon pintar mempunyai lebih perlindungan terhadap jenis serangan kerana dalam kebanyakan senario, pengguna perlu menerima sambungan. Walau bagaimanapun, serangan berjaya untuk peranti dengan interaktiviti rendah seperti headphone Bluetooth menunjukkan bahawa ia dapat menyuntik atau merakam bunyi dalam alat-alat ini tanpa sambungan yang sediada atau sah. Oleh itu, alat-alat ini mempunyai memerlukan mekanisme keselamatan yang lebih baik.

ABSTRACT

Bluetooth technology becomes a part of our daily lives. It is built into a many products such as mobile phones, computers, cars, and medical devices. Moreover, it allows sharing music, photos, videos, and other information wirelessly between two paired devices using radio waves. This technology sends information within your own personal space, which is called your Personal Area Network or "PAN" at distances less than 10 meters. The Common Vulnerabilities and Exploits (CVE) and National Vulnerability Database have recorded a sharp increase in reported vulnerabilities for several popular Bluetooth software stacks specially in Symbian and J2ME OS. The objective of this research is to find existing Bluetooth vulnerability in iOS and Android OS by using available tools that claim ability to penetrate mobile phone Bluetooth and to find possible (approximately three) preventive measures to eliminate vulnerabilities. The methodology of this research will be preliminary investigation, analysis, test and evaluation. The scenario of the experiment was by installing all attack tools in Backtrack 5r4 and rnu it against the smartphone devices and observe the devices notification along with possible information that has been gathered. The experiments have proved smart phone devices are more protective against different types of attacks because in most of the scenarios, the user has to accept the connection. However the successful attacks for the devices with low interactivity such as Bluetooth headphones revealed that it is possible to inject or record sounds in these devices without authenticated connection. Thus these devices need to have better security mechanism.

Table of Contents

CHAPTER	TITLE		PAGE
	DECLARATION		**II**
	DEDICATION		**III**
	ACKNOWLEDGMENT		**IV**
	ABSTRAK		**V**
	ABSTRACT		**VI**
	LIST OF TABLES		**XII**
	LIST OF FIGURES		**XIV**
1	**INTRODUCTION**		**1**
	1.1	Introduction	1
	1.2	Background of the problem	2
	1.3	Problem Statement	3
	1.4	Aim	3
	1.5	Research Questions	3
	1.6	Objectives	3
	1.7	Scope	4
	1.8	Summary	4
2	**LITERATURE REVIEW**		**5**

2.1 Introduction 5

2.2 Bluetooth Technology 5

2.2.1 Bluetooth Evolution 6

2.3 Bluetooth Architecture 8

2.3.1 Bluetooth Vulnerabilities 9

2.4 Bluetooth Attacks 14

2.4.1 BlueSnarfing attack 14

2.4.2 BlueBugging attack 14

2.4.3 BlueJack attack 15

2.5 Hacking Tools and technique 16

2.5.1 Bluebug 16

2.5.2 Blooover II 16

2.5.3 Blueprinting 17

2.5.4 Carwhisperer 18

2.5.5 Wholesale sniffing 19

2.5.6 BlueSnarf 20

2.5.7 BlueBump 20

2.5.8 BlueSmack 20

2.5.9 HeloMoto 20

2.5.10 BlueDump 21

2.5.11 BlueChop 21

2.6 Hacking Bluetooth 21

2.6.1 Bluetooth Discovery 21

2.6.2 Bluetooth Connecting 24

2.7 Bluetooth version on smart phone 25

2.8 Summary 25

3 METHODOLOGY 26

3.1 Introduction 26

3.2 Research Design 26

3.3 Preliminary Investigation 27

3.3.1 Requirement 27

3.3.2 Environment setup 28

3.4 Analysis 32

3.4.1 Data Collection 32

3.5 Testing and Evaluation 33

3.5.1 Method of evaluation 33

3.6 Summary 33

4 ANALYSIS 34

4.1 Introduction 34

4.2 Experimental Setup 34

4.2.1 Devices 34

4.2.2 HCI Tools 35

4.2.3 Pinging Devices 37

4.2.4 RFCOMM Connections 38

4.3 Bluetooth Attack 38

4.3.1 Surveillance 38

4.3.2 Obfuscation 40

4.3.3 Fuzzer 43

4.3.4 Sniffing 44

4.3.5 Unauthorized Direct Data Access 46

4.4 Bluetooth Attack Steps 48

4.4.1 HCITool 48

4.4.2 BTScanner 48

4.4.3 l2Ping 53

4.4.4 SDPTool 54

4.4.5 HCITool info 56

4.4.6 PSM_scan 58

4.4.7 Rfcomm_scan 59

4.4.8 BlueBugger 63

4.4.9 BlueMaho 72

4.4.10 Carwhisperer 79

5 RESULT 80

5.1 Introduction 80

5.2 Gathering Devices Information 80

5.3 Android OS 81

5.4 iOS devices 85

5.5 Countermeasure 85

6 CONCLUSION 86

6.1 Introduction 86

6.2 Further Improvements 86

6.3 CONCLUSION 87

REFERENCES 88

APPENDIX A **91**

APPENDIX B **115**

LIST OF TABLES

TABLE NO.	TITLE	PAGE
2.1	Bluetooth Features (Source: Alfaiate, 2012)	7
2.2	Bluetooth adapter classes (source: Haines, 2010)	8
2.3	Vulnerabilities and exploits in Bluetooth (source: Abhijit Bose, 2006)	10
2.4	Bluetooth version on smart phone	25
4.1	BTScanner basic device information	49
4.2	BTScanner Devices details	50
4.3	L2Ping devices results	53
4.4	SDPTool Browse Details	54
4.5	HCITool info Details	56
4.6	PSM-Scan results	58
4.7	RFComm_Scan Results	60
4.8	Galaxy Nexus 2 open channels	63
4.9	Galaxy Nexus 2 BlueBugger attack results	64
4.10	iPhone 5 open channels	67
4.11	Samsung Galaxy S3 opens channels	68
4.12	Samsung Galaxy S3 BlueBugger attack results	68
4.13	iPhone 3Gs open channels	71
4.14	Galaxy Nexus 2 BlueMaho tools attack and results	74
4.15	iPhone BlueMaho tools attack and results	75
4.16	Samsung Galaxy S3 BlueMaho tools attack and results	76
4.17	iPhone 3Gs BlueMaho tools attack and results	77
0.1	SDPTool results	91
0.1	BlueBugger attack on Galaxy Nexus	115

0.2 BlueBugger attack on iPhone 5 116

0.3 BlueBugger attack on Galaxy S3 117

0.4 BlueBugger attack on iPhone 3Gs 118

0.5 BlueMaho Suit Attack in Galaxy Nexus 119

0.6 BlueMaho Suit Attack in iPhone 5 120

0.7 BlueMaho Suit Attack in Galaxy S3 121

0.8 BlueMaho Suit Attack in iPhone 3Gs 122

LIST OF FIGURES

FIGURE NO.	TITLE	PAGE
2.1	Bluetooth Stack (source: Adam Laurie, 2004)	9
2.2	Bluetooth Piconet and Scatternet Configuration (Source: Christian Barnes, 2002)	19
3.1	Research Methodology	27
3.2	BlueHell interface	29
3.3	BlueScanner interface (Source: airodump.net)	30
3.4	BlueDiving Interface (Source: airodump.net)	32
4.1	iPhone 3Gs, iPhone 5 (Google)	35
4.2	Galaxy Nexus 4 and Samsung Galaxy S3 (Google)	35
4.3	Jabra EXTREME2 v4 (Google)	35
4.4	BlueHell interface	39
4.5	Bluetooth default configuration	40
4.6	Bluetooth configuration after running command.	41
4.7	spooftooph commands	42
4.8	Bdaddr command	43
4.9	BSS main usage	44
4.10	HCIDump sniffing	45
4.11	BlueBugger Usage	46
4.12	BlueSnarfer Usage	47
4.13	HCITool scan	48
4.14	BlueMaho main interface	72
4.15	BlueMaho Exploits	73
4.16	BlueMaho Tools	73
4.17	Carwhisperer attack	79

5.1	Samsung Galaxy S3 IMEI	81
5.2	Samsung Galaxy S3 contacts	82
5.3	Samsung Galaxy S3 dialing number	83
5.4	Google Galaxy Nexus contacts	83
5.5	Galaxy Nexus dialing number	84

CHAPTER 1

INTRODUCTION

1.1 Introduction

Bluetooth technology becomes a part of our daily lives. It is built into many products such as mobile phones, computers, cars, and medical devices. Moreover, it allows sharing music, photos, videos, and other information wirelessly between two paired devices using radio waves. This technology sends information within your own personal space, which is called your Personal Area Network or "PAN" at distances less than 10 meters.

Bluetooth technology was invented in 1994 by engineers at Ericsson, a Swedish company. In 1998, a group of companies agreed to work together using Bluetooth technology as a way to connect their products. These companies formed the Bluetooth Special Interest Group (SIG) (Bluetooth.com). It was dated back to discoveries pioneered by the military in the 1940s. The name "Bluetooth" is actually very old from the 10th century Danish King Harald Blåtand - or Harold Bluetooth in English. King Blåtand was instrumental in uniting warring factions in parts of what are now Norway, Sweden and Denmark.

It was originally intended to be a wireless replacement for wire cables between headsets and phones or computers, keyboards and mice. Nowadays, it is used to connect TVs, music players and even home healthcare devices.

1.2 Background of the problem

With the widespread adoption of Bluetooth device comes the unavoidable implementation problems that cause unexpected things to happen. The adoption of standard technologies in mobile networks and the ability to constantly connect to the Internet, offer many functionalities and services to users such as sending and downloading tiles with attachments, some of which maybe infected. Most Bluetooth based attacks are based on a simple and common flaw. The problem allows hackers to create worms that spread from one to other smart phones without user intervention. The majority of the resulting exploits are due to programming flaws and incorrect implementation of Bluetooth protocols for pairing, data transfer and device discovery. The Common Vulnerabilities and Exploits (CVE) and National Vulnerability Database have recorded a sharp increase in reported vulnerabilities for several popular Bluetooth software stacks.

Moreover, users often are very poor at reading documentation, understanding risks and threats, and generally at changing defaults. Most attacks revolve around users not changing the default settings on their devices. That, coupled with poor user interface (UI) design, creates situations where users are unaware that something bad is happening or about to happen. Moreover, documentation until recently did not fully explain the risks of certain actions. Furthermore, Bluetooth should offer a more reliable protection to their users. In fact, security should not be pushed back to users and a mechanism should exist to prevent undesired access. However, analysts have argued that the capability of the current mobile phones makes it impossible for a virus to infect such devices.

1.3 Problem Statement

Bluetooth technology in mobile phones running Symbian and Java operating system were vulnerable to many attacking tools such as BlueBugger, BlueSnarfer, and others which could copy or delete private information, sniffing, dial phone number, or smack Bluetooth stack. These tools would be able to do the same impact in smart phones that have different operating systems and last version of Bluetooth version.

1.4 Aim

This study aims to evaluate and the audit of security in Bluetooth Smart Phone Devices, on usability, focusing on Android and iPhone Operating Systems.

1.5 Research Questions

- What are the existing Bluetooth vulnerabilities in iOS and Android OS?
- What are the countermeasures proposed to protect/safeguard smartphone device?

1.6 Objectives

- **To find existing Bluetooth vulnerability in iOS and Android OS:** there are many tools in the market that by popular claim is a threat to mobile phone security. Many of the tools exploit in a Personal Area Network (PAN), the Bluetooth feature of a smart phone to gain unusual access. The tools are known to provide the intruder with many different accesses to the victim device – like access to files, contacts, etc., allows the attacker to copy or delete those files or turn off the device. Some tools are rumored to allow the attacker to make phone calls or send SMSs.

- **To find counter measure for vulnerability:** the scandalous claims require attentive study of the actual vulnerabilities, the methods of access, the amount of access that may be granted, and finding out many (approximately three) preventive measures that need to be taken to safeguard our personal devices.

1.7 Scope

- iPhone 3GS, 5 (iOS 6, 5.x)
- Galaxy Nexus 2 (Android v4)
- Samsung Galaxy S3 (Android v4)
- BackTrack 5r3

1.8 Summary

This chapter has discussed and explains why this project needs to be conducted by identifying the background of the problem, aim of the project and also the scope to be done. The next chapter will discuss about the literature review on the previous work which is related in this project.

REFERENCES

A BypassingSecurityModelforAnonymous Bluetooth Peers. (2005). *International Conference on Wireless Networks, Communications and Mobile Computing* , 6.

A, S. S. (n.d.). Analysis of Bluetooth Threats and v4.0 Security Features . 4.

Abhijit Bose, K. G. (2006). On Mobile Viruses Exploiting Messaging and Bluetooth Services . *IEEE*, 1-10.

Adam Laurie, M. H. (2004, 12 27-29). *Bluetooth Hacking.* Retrieved 11 20, 2012, from trifinite.org: trifinite.org

airodump.net. (n.d.). *bluetooth security & vulnerablilities*. Retrieved 11 15, 2012, from airodump.net: http://airodump.net/bluetooth-security-vulnerabilities/

Alfaiate, J. F. (2012). Bluetooth security analysis for mobile phones . *IEEE*, 1-6.

Bluetooth.com. (n.d.). *Welcome to Bluetooth Technology 101*. Retrieved 11 03, 2012, from Blutooth.com: http://www.bluetooth.com/Pages/Fast-Facts.aspx

Christian Barnes, T. B. (2002). *Hack Proofing your wireless network.* Rockland: Syngress.

Dr. Ashley L. Podhradsky, C. C. (2012). The Bluetooth Honeypot Project . *IEEE* , 10.

Hager, C. M. (2003). An analysis of Bluetooth security vulnerabilities . *IEEE*, 1825 - 1831 vol.3 .

Haines, B. (2010). CHAPTER 3 - Bluetooth Attacks. In *Seven Deadliest Wireless Technologies Attacks* (pp. 43-55). Boston: Syngress.

L. Carettoni, C. M. (2007). Studying Bluetooth Malware Propagation: The BlueBag Project . *IEEE*, 17-25.

Layton, C. F. (n.d.). *How Bluetooth Works*. Retrieved 9 22, 2012, from howstuffworks: http://electronics.howstuffworks.com/bluetooth.htm

Masagca, M. T. (2011). An Investigation of Bluetooth Security Threats . *IEEE* , 7.

Muhammad Muslim Mansor, M. I. (2010, October). BTFRIEND: BLUETOOTH SECURITY ALERT SYSTEM . *IEEE Symposium on Industrial Electronics and Applications* , 5.

Scarfone, J. P. (2011, September). Guide to Bluetooth Security (Draft) . *National Institute of Standards and Technology NIST*, 49.

Swiat. (2011, 7 12). *MS11-053: Vulnerability in the Bluetooth stack could allow remote code execution*. Retrieved 9 20, 2012, from Technet.com: http://blogs.technet.com/b/srd/archive/2011/07/12/ms11-053-vulnerability-in-the-bluetooth-stack-could-allow-remote-code-execution.aspx

Tarique, N. B.-N. (2012, January). BLUETOOTH SECURITY THREATS AND SOLUTIONS: A SURVEY . *International Journal of Distributed and Parallel systems, 3*(1), 148.

trifinite.org. (n.d.). *BlueBug*. Retrieved 9 29, 2012, from trifinite.org: http://trifinite.org/trifinite_stuff_bluebug.html