

Intrusion Detection in Bluetooth enabled Mobile Phones

Kishor K Nair
(Student No: 2040 2333)

Dissertation submitted in partial fulfillment of the requirements for the degree *Master of Engineering in Computer Engineering* at the

**School of Electrical, Electronic and Computer Engineering,
Potchefstroom Campus,
North-West University,
South Africa**

Supervisor: Professor ASJ Helberg

November 2008

Declaration

I declare that this dissertation is a presentation of my original research work, conducted under the supervision of Prof. ASJ Helberg. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due reference to the literature. No part of this research has been submitted in the past, or is being submitted, for a degree or examination at any other University.

November 2008

KISHOR K NAIR

Acknowledgement

It is a pleasure to thank many people who made this dissertation possible.

This dissertation would not have been completed without Prof. ASJ Helberg who not only served as my supervisor but also encouraged, supported and advised me throughout my academic program. His guidance and advices were extremely valuable in contributing to the successful completion of this research.

I warmly thank Mrs. Cristel Eastes and Mrs. Leanie du Plessis of the Academic Administration for helping me throughout my curriculum.

I also extend my gratitude to my editor, Dr. Linda Snyman.

I am extending my sincere thanks to my father-in-law Mr. Chandra Mohan Pillai and family for helping and supporting me throughout this dissertation.

I owe my loving thanks to my wife Manju and my little daughter Keerthana for their support and sacrifices during the completion of this work.

Last but not least, I wish to thank my parents, PG Krishnan Nair and MS Santhakumari. To them I dedicate this work.

Abstract

Wireless technology has become one of the vital media of communication and Bluetooth is playing a major role in advancing its global spread, connecting electronic devices worldwide without cables. Bluetooth is recognized and globally accepted mainly through Bluetooth enabled mobile phones, which cover almost 60% of the Bluetooth market. However, with other technological innovations, the advancement in Bluetooth enabled mobile phones also caused serious security breaches. Although Bluetooth mobile phones are equipped with built-in security modes and policies, the intruders compromise the mobile phones through existing security vulnerabilities and limitations. Information stored in mobile phones, whether it is personal or corporate, is valuable to mobile phone users. Such information also seeks the attention of intruders. Moreover, an intruder can compromise the mobile phone, and use it as a medium to get into other mobile phones. Mobile phone users are unaware of this current dilemma. Therefore, the need to protect information, as well as mobile phone users to supervise their incoming connections, is very vital. An additional security mechanism was therefore realized, especially at the mobile phone's user level, and which could be useful to the mobile phone users. Bluetooth Logging Agent (BLA) is such a mechanism. It helps in alleviating the current security issues by making the users aware of their incoming Bluetooth connections and giving them an option to either accept or reject these connections. Besides this, the intrusion detection and verification module uses databases and rules to authenticate and verify all connections. The BLA when comparing to the existing security solutions is unique in that; it is equipped with a Bluetooth message logging module. This logging module reduces the security risks by monitoring the Bluetooth communication between the mobile phone and the remote device.

Table of Contents

| | |
|---|-----------|
| 1.1 INTRODUCTION | 15 |
| 1.2 MOTIVATION FOR THIS RESEARCH..... | 17 |
| 1.2.1 CRIME THROUGH BLUETOOTH-ENABLED MOBILE PHONES..... | 17 |
| 1.2.2 PROPAGATION OF VIRUSES AND TROJANS INTO CORPORATE NETWORKS VIA BLUETOOTH MOBILE PHONES | 18 |
| 1.2.3 THE INEFFICIENCY OF THE EXISTING BLUETOOTH PROTOCOL IMPLEMENTATION AND BLUETOOTH SECURITY MANAGER IN MOBILE PHONES | 19 |
| 1.2.4 BLUETOOTH UNAWARENESS OF MOBILE PHONE USERS | 20 |
| 1.3 ISSUES TO BE ADDRESSED | 20 |
| 1.3.1 WHAT IS BLUETOOTH WIRELESS TECHNOLOGY AND WHAT IS ITS SIGNIFICANCE IN MOBILE PHONES? | 21 |
| 1.3.2 WHAT IS BLUETOOTH SECURITY, AND HOW IMPORTANT IS IT IN MOBILE PHONES? | 21 |
| 1.3.3 THE PROVISION OF ADDITIONAL BLUETOOTH SECURITY MECHANISMS IN MOBILE PHONES | 22 |
| 1.4 PATH TO BLUETOOTH LOGGING AGENT (BLA)..... | 22 |
| 1.5 RESEARCH GOALS | 23 |
| 1.6 RESEARCH METHODOLOGY | 24 |
| 1.7 TEST STRATEGY | 25 |
| 1.8 TERMINOLOGY | 25 |
| 1.8.1 BLUETOOTH..... | 25 |
| 1.8.2 BLUETOOTH MOBILE PHONE | 26 |
| 1.8.3 BLUETOOTH PROTOCOL STACK..... | 26 |
| 1.8.4 BLUETOOTH DEVICE ADDRESS | 26 |
| 1.8.5 PICONET | 26 |
| 1.8.6 INQUIRY..... | 26 |
| 1.8.7 DISCOVERABLE MODE | 26 |
| 1.8.8 NON-DISCOVERABLE MODE..... | 27 |
| 1.8.9 LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL (L2CAP) | 27 |
| 1.8.10 L2CAP CHANNEL | 27 |
| 1.8.11 BLUETOOTH CONNECTION | 27 |
| 1.8.12 LINK KEY | 27 |
| 1.8.13 PAIRING | 27 |
| 1.8.14 PERSONAL IDENTIFICATION NUMBER (PIN)..... | 28 |
| 1.8.15 TRUSTED DEVICE | 28 |
| 1.8.16 INTRUSION..... | 28 |
| 1.8.17 INTRUSION DETECTION (ID) | 28 |
| 1.8.18 INTRUDERS..... | 28 |
| 1.8.19 INTRUSION DETECTION SYSTEMS (IDSs) | 28 |
| 1.8.20 VULNERABILITY | 28 |
| 1.8.21 VIRUS | 29 |

| | |
|---|-----------|
| 1.8.22 TROJAN..... | 29 |
| 1.9 DISSERTATION LAYOUT..... | 29 |
| 2.1 WHAT IS BLUETOOTH? | 31 |
| 2.2 THE HISTORY OF BLUETOOTH..... | 32 |
| 2.3 BLUETOOTH TECHNICAL SPECIFICATIONS..... | 33 |
| 2.3.1 SPECTRUM | 33 |
| 2.3.2 RANGE | 33 |
| 2.3.3 POWER | 33 |
| 2.3.4 DATA RATE..... | 33 |
| 2.3.5 CONNECTION SPECIFICATIONS | 33 |
| 2.4 BLUETOOTH PROTOCOL STACK..... | 34 |
| 2.4.1 BLUETOOTH CORE PROTOCOLS | 36 |
| 2.4.1.1 Baseband..... | 36 |
| 2.4.1.2 Link Management Protocol..... | 37 |
| 2.4.1.3 Logical Link Control and Adaptation Protocol..... | 37 |
| 2.4.1.4 Service Discovery Protocol..... | 37 |
| 2.4.2 CABLE REPLACEMENT PROTOCOL - RFCOMM | 38 |
| 2.4.3 TELEPHONY CONTROL PROTOCOLS..... | 38 |
| 2.4.3.1 TCS Binary..... | 38 |
| 2.4.3.2 AT- Commands | 38 |
| 2.4.4 ADOPTED PROTOCOLS | 39 |
| 2.4.4.1 PPP | 39 |
| 2.4.4.2 UDP/TCP/IP..... | 39 |
| 2.4.4.3 OBEX Protocol..... | 39 |
| 2.4.4.4 WAP..... | 39 |
| 2.5 BLUETOOTH PROFILES..... | 40 |
| 2.5.1 GENERIC ACCESS PROFILE (GAP)..... | 40 |
| 2.5.2 SERIAL PORT PROFILE (SPP) | 40 |
| 2.5.3 SERVICE DISCOVERY APPLICATION PROFILE (SDAP) | 40 |
| 2.5.4 GENERIC OBJECT EXCHANGE PROFILE (GOEP)..... | 40 |
| 2.5.5 OBJECT PUSH PROFILE (OPP)..... | 40 |
| 2.5.6 FILE TRANSFER PROFILE (FTP) | 40 |
| 2.5.7 SYNCHRONISATION PROFILE (SP) | 41 |
| 2.5.8 HEADSET PROFILE (HSP)..... | 41 |
| 2.5.9 HANDS-FREE PROFILE (HFP) | 41 |
| 2.5.10 CORDLESS TELEPHONY PROFILE (CTP) | 41 |
| 2.5.11 INTERCOM PROFILE (IP) | 41 |
| 2.5.12 DIAL-UP NETWORKING PROFILE (DUN)..... | 41 |
| 2.5.13 FAX PROFILE (FP) | 41 |
| 2.5.14 LAN (LOCAL AREA NETWORK) ACCESS PROFILE (LAP)..... | 41 |
| 2.6 NETWORK TOPOLOGY | 42 |
| 2.6.1 PICONET | 42 |
| 2.6.2 SCATTERNET | 43 |

| | |
|---|-----------|
| 2.7 OPERATIONAL PROCEDURES AND MODES..... | 44 |
| 2.7.1 INQUIRY PROCEDURE | 44 |
| 2.7.2 PAGING PROCEDURE..... | 44 |
| 2.7.3 CONNECTED MODE | 45 |
| 2.8 APPLICATIONS OF BLUETOOTH TECHNOLOGY..... | 45 |
| 2.8.1 INFOTAINMENT | 45 |
| 2.8.2 LOAD TRUCK MANAGEMENT..... | 46 |
| 2.8.3 DIAGNOSTICS..... | 46 |
| 2.8.4 MEDICAL | 46 |
| 2.8.5 AUTOMOTIVE | 46 |
| 2.8.6 POINT-OF-SALE PAYMENTS..... | 46 |
| 2.9 SUMMARY | 48 |
| 3.1 WHAT IS BLUETOOTH SECURITY? | 50 |
| 3.1.1 FREQUENCY HOPPING | 50 |
| 3.1.2 AUTHENTICATION | 50 |
| 3.1.3 ENCRYPTION | 51 |
| 3.2 BLUETOOTH SECURITY ARCHITECTURE | 51 |
| 3.2.1 BLUETOOTH SECURITY MODES | 52 |
| 3.2.2 BLUETOOTH SECURITY LEVELS | 52 |
| 3.2.2.1 <i>Authentication and Authorization</i> | 53 |
| 3.2.2.2 <i>Pairing and Bonding</i> | 53 |
| 3.2.3 BLUETOOTH SECURITY ARCHITECTURE..... | 53 |
| 3.3 WIRELESS SECURITY VULNERABILITIES | 55 |
| 3.3.1 WARDRIVING..... | 55 |
| 3.3.2 DENIAL OF SERVICE (DOS) ATTACKS | 56 |
| 3.3.3 MAN-IN-THE-MIDDLE ATTACKS..... | 57 |
| 3.3.4 ADDRESS RESOLUTION PROTOCOL (ARP) POISONING | 57 |
| 3.3.5 WIRED EQUIVALENT PRIVACY (WEP) INTRUSIONS | 58 |
| 3.4 BLUETOOTH SECURITY VULNERABILITIES..... | 59 |
| 3.4.1 FUNDAMENTAL VULNERABILITIES | 59 |
| 3.4.2 IMPLEMENTATION-INDUCED VULNERABILITIES..... | 60 |
| 3.5 BLUETOOTH SECURITY LIMITATIONS..... | 61 |
| 3.6 SUMMARY | 63 |
| 4.1 BLUETOOTH INTRUSIONS..... | 64 |
| 4.1.1 BLUEBUG | 64 |
| 4.1.2 BLUEJACKING | 66 |
| 4.1.3 BLUESNARF..... | 67 |
| 4.1.4 BLUESNARF++ | 67 |
| 4.1.5 BLUESMACK | 68 |
| 4.1.6 BLUEBUMP | 68 |

| | |
|---|------------|
| 4.1.7 BLUE_DUMP | 68 |
| 4.1.8 BLUECHOP | 68 |
| 4.1.9 HELOMOTO | 69 |
| 4.1.10 CAR WHISPERER | 69 |
| 4.1.11 WARNIBBLING | 69 |
| 4.1.12 BLUETOOTH VIRUSES AND WORMS | 70 |
| 4.1.12.1 Cabir..... | 70 |
| 4.1.12.2 Mibir.A..... | 70 |
| 4.1.12.3 Lasco.A..... | 71 |
| 4.1.12.4 Commwarrior..... | 71 |
| 4.2 THE NEED FOR AN ADDITIONAL BLUETOOTH SECURITY MECHANISM..... | 72 |
| 4.3 SUMMARY | 72 |
| 5.1 EXISTING BLUETOOTH SECURITY SOLUTIONS | 75 |
| 5.1.1 AIRDEFENSE BLUEWATCH™ | 75 |
| 5.1.2 RED-DETECT™ | 76 |
| 5.1.3 BLUEAUDITOR | 76 |
| 5.1.4 AIRMAGNET BLUESWEEP™ | 76 |
| 5.2 PROPOSED BLUETOOTH SECURITY SOLUTION..... | 77 |
| 5.3 SUMMARY | 79 |
| 6.1 BLA DEVELOPMENT PROCESS..... | 80 |
| 6.2 BLA ARCHITECTURE | 82 |
| 6.2.1 BLUETOOTH MODULE IN MOBILE PHONES..... | 84 |
| 6.2.2 BLA - BLUETOOTH MODULE INTERFACE (BBMI)..... | 86 |
| 6.2.3 INTRUSION DETECTION AND VERIFICATION MODULE (IDVM)..... | 86 |
| 6.2.3.1 Connection and Disconnection Module (CDM)..... | 86 |
| 6.2.3.2 Authentication Module (AM) | 89 |
| 6.2.3.3 Service Module (SM)..... | 91 |
| 6.2.4 LOGGING MODULE (LM) | 93 |
| 6.2.5 BLA DATABASE | 95 |
| 6.2.5.1 Connection Database (CDB)..... | 95 |
| 6.2.5.2 Trusted Devices Database (TDDB) | 95 |
| 6.2.5.3 Non trusted Devices Database (NTDDB)..... | 95 |
| 6.2.5.4 Services and Devices Mapping Database (SDMDB) | 95 |
| 6.2.5.5 Logging Database (LDB)..... | 95 |
| 6.2.6 MOBILE PHONE USER INTERFACE (MPUI)..... | 96 |
| 6.3 BLA AND BLUETOOTH MODULE INTERFACE..... | 96 |
| 6.4 SUMMARY | 97 |
| 7.1 PROTOTYPE COMPONENTS, ASSUMPTIONS..... | 98 |
| 7.2 BLA/BIS SPECIFICATIONS AND PRE-REQUISITES FOR DEPLOYMENT | 99 |
| 7.3 BLA/BIS COMMUNICATION MESSAGE TYPES..... | 100 |
| 7.4 BLA | 102 |
| 7.4.1 BLA MENU OPTIONS..... | 103 |

| | |
|--|------------|
| 7.4.1.1 Start BLA..... | 103 |
| 7.4.1.2 Accept Request..... | 104 |
| 7.4.1.3 Discard Request..... | 104 |
| 7.4.1.4 Log Packet..... | 105 |
| 7.4.1.5 Stop BLA..... | 106 |
| 7.4.1.6 Power off Bluetooth..... | 106 |
| 7.4.2 EXIT..... | 107 |
| 7.4.3 BLA DATABASE LAYOUT IN SMARTPHONE | 108 |
| 7.5 BIS..... | 111 |
| 7.5.1 BIS GENERAL MENU OPTIONS | 112 |
| 7.5.2 BIS SAFE REQUESTS MENU OPTIONS | 114 |
| 7.5.3 BIS INTRUSIONS MENU OPTIONS..... | 114 |
| 7.5.4 BIS RANDOM SAFE/UNSAFE REQUESTS MENU OPTIONS..... | 115 |
| 7.6 COMMUNICATION BETWEEN THE BIS AND BLA..... | 116 |
| 7.6.1 SAFE CONNECT REQUEST AND RESPONSE..... | 116 |
| 7.6.2 SAFE AUTHENTICATION REQUEST AND RESPONSE..... | 119 |
| 7.6.3 SAFE SERVICE ACCESS REQUEST AND RESPONSE | 122 |
| 7.6.4 CONNECTION ATTACK FROM BIS AND RESPONSE FROM BLA | 124 |
| 7.6.5 AUTHENTICATION ATTACK FROM BIS AND RESPONSE FROM BLA..... | 127 |
| 7.6.6 SERVICE ACCESS ATTACK FROM BIS AND RESPONSE FROM BLA | 128 |
| 7.6.7 RANDOM CONNECT REQUEST AND RESPONSE FROM BLA..... | 129 |
| 7.6.8 RANDOM AUTHENTICATION REQUEST AND RESPONSE FROM BLA..... | 133 |
| 7.6.9 RANDOM SERVICE ACCESS REQUEST AND RESPONSE FROM BLA | 134 |
| 7.6.10 SAFE REQUEST/RESPONSE SESSION BETWEEN BLA AND BIS..... | 136 |
| 7.6.11 BLA DISCARDING A REQUEST FROM BIS | 137 |
| 7.7 SUMMARY | 139 |
| 8.1 RESEARCH SYNOPSIS..... | 140 |
| 8.2 SIGNIFICANCE OF THE BLA PROTOTYPE..... | 141 |
| 8.3 VERIFICATION AND VALIDATION OF TEST RESULTS | 143 |
| 8.4 HOW VALUABLE IS BLA TO MOBILE PHONE MANUFACTURES | 145 |
| 8.5 FEASIBILITY OF IMPLEMENTING THE BLA PROTOTYPE IN MOBILE PHONES | 145 |
| 8.6 SCOPE FOR FUTURE RESEARCH | 146 |
| BIBLIOGRAPHY | 147 |
| APPENDIX – PROTOTYPE IMPLEMENTATION DISK..... | 162 |

List of Figures

| | |
|--|-----|
| FIGURE 2.1 THE OFFICIAL BLUETOOTH LOGO..... | 32 |
| FIGURE 2.2 BLUETOOTH PROTOCOL STACK..... | 35 |
| FIGURE 2.3 BLUETOOTH PICONET (POINT-TO-POINT)..... | 42 |
| FIGURE 2.4 BLUETOOTH PICONET (POINT-TO MULTI POINT)..... | 42 |
| FIGURE 2.5 BLUETOOTH SCATTERNETS | 43 |
| FIGURE 3.1 BLUETOOTH SECURITY ARCHITECTURE | 54 |
| FIGURE 6.1 COMPLETE DESIGN OF BLA..... | 80 |
| FIGURE 6.2 BLUETOOTH MODULE | 85 |
| FIGURE 6.3 THE FLOW OF INFORMATION THROUGH CDM..... | 88 |
| FIGURE 6.4 THE FLOW OF INFORMATION THROUGH AM..... | 90 |
| FIGURE 6.5 THE FLOW OF INFORMATION THROUGH SM..... | 92 |
| FIGURE 6.6 THE FLOW OF INFORMATION THROUGH LM..... | 94 |
| FIGURE 6.7 COMMUNICATION BETWEEN BLA AND BLUETOOTH MODULE..... | 96 |
| FIGURE 7.1 BLA GRAPHICAL USER INTERFACE..... | 102 |
| FIGURE 7.2 BLA MENU OPTIONS..... | 103 |
| FIGURE 7.3 START BLA..... | 103 |
| FIGURE 7.4 ACCEPT REQUEST | 104 |
| FIGURE 7.5 DISCARD REQUEST | 105 |
| FIGURE 7.6 LOG PACKET | 105 |
| FIGURE 7.7 STOP BLA | 106 |
| FIGURE 7.8 POWER OFF BLUETOOTH..... | 107 |
| FIGURE 7.9 EXIT FROM BLA..... | 107 |
| FIGURE 7.10 BLA DATABASE..... | 108 |
| FIGURE 7.11 TDDB | 109 |
| FIGURE 7.12 NTDDB..... | 109 |
| FIGURE 7.13 SDMDB | 110 |
| FIGURE 7.14 CDB..... | 110 |
| FIGURE 7.15 LDB | 111 |
| FIGURE 7.16 BIS GRAPHICAL USER INTERFACE..... | 112 |
| FIGURE 7.17 BIS MENU OPTIONS..... | 112 |
| FIGURE 7.18 BLUETOOTH INTRUSION SIMULATOR STARTED..... | 113 |
| FIGURE 7.19 EXIT BLUETOOTH INTRUSION SIMULATOR..... | 113 |
| FIGURE 7.20 BIS SAFE REQUESTS..... | 114 |
| FIGURE 7.21 BIS INTRUSIONS..... | 115 |
| FIGURE 7.22 BIS RANDOM (SAFE/UNSAFE) REQUESTS..... | 116 |
| FIGURE 7.23 BLA RECEIVING CONNECT REQUEST FROM BIS | 117 |
| FIGURE 7.24 BLA CHECKING TDDB | 117 |
| FIGURE 7.25 BLA ALERTING MPUI OF A SAFE CONNECTION | 118 |
| FIGURE 7.26 BIS RECEIVING A SUCCESSFUL CONNECT RESPONSE | 119 |
| FIGURE 7.27 REMOTE DEVICE ADDRESS ADDED TO CDB DATABASE..... | 119 |
| FIGURE 7.28 BLA RECEIVING AUTHENTICATION REQUEST FROM BIS | 120 |
| FIGURE 7.29 BLA ALERTING MPUI OF A SAFE AUTHENTICATION REQUEST | 121 |
| FIGURE 7.30 BIS RECEIVING A SUCCESSFUL AUTHENTICATION RESPONSE | 121 |
| FIGURE 7.31 BLA RECEIVING SERVICE ACCESS REQUEST FROM BIS..... | 122 |

| | |
|--|-----|
| FIGURE 7.32 SM CHECKING SDB | 123 |
| FIGURE 7.33 BLA ALERTING MPUI OF A SAFE SERVICE ACCESS REQUEST..... | 123 |
| FIGURE 7.34 BIS RECEIVING A SUCCESSFUL SERVICE ACCESS RESPONSE | 124 |
| FIGURE 7.35 BLA CHECKING NTDDB..... | 125 |
| FIGURE 7.36 IDVM ALERTING MPUI OF THE INTRUSION | 125 |
| FIGURE 7.37 BIS GETTING A DISCONNECT REQUEST AND INDICATION THAT THE INTRUSION ATTEMPT IS DETECTED BY BLA | 126 |
| FIGURE 7.38 CONNECTION ATTACK LOGGING INFORMATION OBTAINED FROM LDB..... | 126 |
| FIGURE 7.39 IDVM ALERTING MPUI OF THE INTRUSION | 127 |
| FIGURE 7.40 AUTHENTICATION ATTACK LOGGING INFORMATION OBTAINED FROM LDB | 128 |
| FIGURE 7.41 IDVM ALERTING MPUI OF THE INTRUSION | 128 |
| FIGURE 7.42 SERVICE ACCESS ATTACK LOGGING INFORMATION OBTAINED FROM LDB | 129 |
| FIGURE 7.43 RANDOM CONNECT REQUEST AND RESPONSE (SAFE CONNECTION)..... | 129 |
| FIGURE 7.44 RULE MATCH REQUEST RECEIVED BY BIS FROM BLA..... | 130 |
| FIGURE 7.45 TDDb, AFTER A SAFE RULE MATCH REQUEST FOR CONNECTION FROM BIS | 131 |
| FIGURE 7.46 CDB SHOWING THE CONNECTION TO THE REMOTE DEVICE AFTER GETTING A POSITIVE RULE MATCH RESPONSE FROM BIS | 131 |
| FIGURE 7.47 LDB AFTER GETTING A RANDOM CONNECTION ATTACK FROM BIS..... | 132 |
| FIGURE 7.48 NTDDb AFTER GETTING A RANDOM CONNECTION ATTACK FROM BIS | 132 |
| FIGURE 7.49 RANDOM AUTHENTICATION REQUEST AND RESPONSE | 133 |
| FIGURE 7.50 LDB AFTER GETTING A RANDOM AUTHENTICATION ATTACK FROM BIS..... | 134 |
| FIGURE 7.51 RANDOM SERVICE ACCESS REQUEST AND RESPONSE..... | 135 |
| FIGURE 7.52 LDB AFTER GETTING A RANDOM SERVICE ACCESS ATTACK FROM BIS..... | 136 |
| FIGURE 7.53 SAFE REQUEST/RESPONSE SESSION BETWEEN BLA AND BIS | 137 |
| FIGURE 7.54 BIS GETTING THE INDICATION THAT REQUEST IS DISCARDED BY BLA..... | 138 |
| FIGURE 7.55 LDB AFTER SENDING A DISCARD REQUEST TO BIS..... | 138 |
| FIGURE 8.1 BLA TEST RESULT: LOG FILE SHOWING INTRUSION DETECTION..... | 144 |
| FIGURE 8.2 BLA TEST RESULT: INTRUSION DETECTION ALERT IN USER INTERFACE..... | 144 |

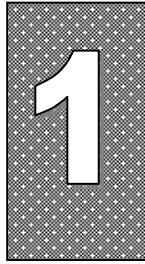
Acronyms and Abbreviations

The following is a list of acronyms and abbreviations that are used commonly throughout this dissertation.

| | |
|----------------|---|
| ACL | Asynchronous Connectionless Link |
| AM | Authentication Module |
| AM_ADDR | Active Member ADDRESS |
| API | Application Programming Interface |
| ARP | Address Resolution Protocol |
| BBMI | BLA - Bluetooth Module Interface |
| BD_ADDR | Bluetooth Device ADDRESS |
| BIS | Bluetooth Intrusion Simulator |
| BLA | Bluetooth Logging Agent |
| CDM | Connection and Disconnection Module |
| CDB | Connection Data Base |
| CF | Compact Framework |
| CPU | Central Processing Unit |
| CTP | Cordless Telephony Profile |
| DUN | Dial-up Networking |
| DoS | Denial-of-Service |
| EPROM | Entrepreneurial Programming And Research On Mobile phones |
| ETSI | European Telecommunications Standards Institute |
| FP | Fax Profile |
| FTP | File Transfer Profile |
| GAP | Generic Access Profile |
| GOEP | Generic Object Exchange Profile |
| GPS | Global Positioning System |

| | |
|----------------|---|
| GUI | Graphical User Interface |
| GSM | Global System for Mobile Communication |
| HCI | Host Controller Interface |
| HFP | Hands-Free Profile |
| HSP | Headset Profile |
| ID | Intrusion Detection |
| IDS | Intrusion Detection System |
| IDVM | Intrusion Detection and Verification Module |
| IEEE | Institute of Electrical and Electronics Engineers |
| IMEI | International Mobile Equipment Identity |
| IP | Intercom Profile |
| L2CAP | Logical Link Control and Adaptation Protocol |
| LAN | Local Area Network |
| LAP | LAN Access Profile |
| LMP | Link Management Protocol |
| LM | Logging Module |
| LDB | Logging Database |
| MAC | Media Access Control |
| MITM | Man-In-The-Middle |
| MMS | Multi Media Service |
| MPUI | Mobile Phone User Interface |
| NTDDB | Non Trusted Devices Database |
| OBEX | OBject Exchange Protocol |
| OPP | Object Push Profile |
| PC | Personal Computer |
| PIM | Personal Identification Module |
| PIN | Personal Identification Number |
| PDA | Personal Digital Assistant |
| PM_ADDR | Parked Member ADDRess |
| POS | Point-of-sale |
| PPP | Point to Point Protocol |

| | |
|---------------|---------------------------------------|
| RF | Radio Frequency |
| RFCOMM | Radio Frequency Communication |
| SCO | Synchronous Connection Oriented |
| SDP | Service Discovery Protocol |
| SDAP | Service Discovery Application Profile |
| SDMDB | Services and Device Mapping database |
| SIG | Special Interest Group |
| SM | Service Module |
| SMS | Short Message Service |
| SP | Synchronization Profile |
| SPP | Serial Port Profile |
| SSID | Service Set Identifier |
| TCP | Transmission Control Protocol |
| TCS | Telephony Control Protocol |
| TDD | Time Division Duplex |
| TDDB | Trusted Devices Database |
| UDP | User Datagram Protocol |
| WAP | Wireless Access Protocol |
| WAE | Wireless Application Environment |
| WEP | Wired Equivalent Privacy |
| WWWD | World Wide Wardrive |



Introduction

1.1 Introduction

Information technology has improved communication via the numerous services it provides today, with Internet in particular being the most used medium. The only predicament is that this type of communication started taking place with wires connecting the communication mediums. In other words, there was a physical channel connecting the two people who were communicating. A person using this type of communication had to be at a specific place to communicate, just like when using wired telephones. This was one of the limitations that wired communication faced. Wireless technology then overcame this restriction, and communication is now performed by sending electromagnetic signals through air. This means that two or more communication mediums can connect wirelessly.

Wireless technology, in its variety of forms, is a rapidly developing area of Electronics. This technology has become extremely popular because of its vast effectiveness, communication infrastructure enhancements and efficiency, greater mobility, and reduced costs [1]. Furthermore, wireless technology allows network managers to setup and enhance networks without having to install or move wires. It is used in a variety of new applications which includes, but is not limited to Point of Sale (POS) terminals, defense and access control applications to enhance security, data acquirement applications, Global Positioning

Systems (GPS) and Satellite communication systems. In addition, it is the ideal replacement for all the scenarios which can be accomplished using wired communication [2].

The mobile phone is the most used wireless device by far. This fact is not likely to change any time soon, if ever. Mobile phones are easy and appealing to use. They are also comfortable and equipped with more or less every latest feature the modern user desires. The research conducted by Entrepreneurial Programming and Research on Mobile phones (EPROM) shows the following statistics: There are at present more than 2.4 billion mobile phone users globally and more than 1,000 new mobile phone subscribers are added every minute. In 2005, the mobile phone consignment increased by 19 percent to 810 million units and was expected to rise by 15 percent to 930 million units in 2006 [3].

As according to Sir David Brown, Chairman of Motorola, Mobile phones on the market today have the same processing power of yesterday's Personal Computers (PCs) [4]. The Bluetooth integration in mobile phones changed the ways in which a mobile phone can be used. "Bluetooth wireless technology is a short-range communications system that takes the place of cables, connecting portable or fixed electronic devices" [18]. Bluetooth-enabled mobile phones are very powerful computing devices, not only useful for voice calls or text messaging, but also for a much wider variety of applications. The incorporation of Bluetooth in mobile phones has advanced the mobile communication technology to such an extent that mobile phone users no longer have to even touch their phone or take it out of their pocket to receive or make a call. If they choose to answer a call, they can simply answer it with their Bluetooth-enabled headset, leaving their phone completely untouched. This is possible through establishing a Bluetooth connection between headset and the mobile phone.

The recent development of Bluetooth watches from Fossil¹ and Sony Ericsson affirms that Bluetooth will make a big difference to our mobile lives. These watches enable users to see who is calling, and to silence or reject a call directly from the watch. Today's mobile phones

¹ Fossil [<http://www.fossil.com>], the company offers a wide variety of fashionable consumer products which mainly includes a series of fashion watches.

have increasingly advanced features that sometimes seem to get in the way of the basic task of making and receiving phone calls. When enabled to answer and place calls without having to hold the phone in our hands; we experience a dramatic improvement in the responsiveness of our communications [5].

In spite of all the above-mentioned advantages, security remains a big concern in mobile phones. Wireless technology is tremendously exposed to security attacks and eavesdropping. Bluetooth is not different in this [6]. The basic radio communication medium for wireless holds a serious exposure to attacks [7]. Inherent Bluetooth security performance in mobile phones is weak and a Bluetooth firewall is not available by default [6]. Intruders thus use Bluetooth as an outlet for launching serious intrusions in Bluetooth mobile phones. The idea that there needs to be an additional Bluetooth security mechanism in mobile phones lies behind this research, which is further motivated below.

1.2 Motivation for this Research

The following motivated this research:

1.2.1 Crime through Bluetooth-enabled mobile phones

There has been a massive increase of wireless equipments in the past few years and Bluetooth wireless technology is growing at a fast rate [22]. Although Bluetooth-enabled mobile phones are globally accepted, it also has a number of disadvantages. The most important disadvantage in particular is the crime committed through Bluetooth-enabled mobile phones.

Common criminal activities that intruders use Bluetooth security vulnerabilities for include, stealing valuable information from mobile phones, eavesdropping on confidential conversations and accessing mobile phone commands silently from the mobile phone. This enables intruders to use the attacked phone not only to make calls, but also to get access to the Internet. Security vulnerabilities have disastrous consequences for phone owners; they are often heavily charged and even prosecuted for criminals' anonymous activities.

Recent incidents from south Manchester re-affirm that high profile criminal activities are happening through Bluetooth. The intruders in south Manchester carry Bluetooth-enabled mobile phones as they walk near parked cars that contain expensive laptops or mobile phones [106]. The intruders' Bluetooth phones help them find what they are looking for. Once they find the devices, they try to compromise them through Bluetooth security vulnerabilities.

This incident is picked from the hundreds of sophisticated crimes that are happening daily through Bluetooth. The number of intrusions committed through Bluetooth-enabled mobile phones is increasing at a rapid rate and it is a high risk to neglect them. The major financial institutions and high profile business firms worldwide are an easy target of intrusions. The wireless technology and its vulnerability to cyber crime has become an acute sign of our times [8].

Crime forms the primary motivation of this study. The second motivation for the study follows below.

1.2.2 Propagation of viruses and Trojans into corporate networks via Bluetooth mobile phones

Intruders today are increasingly targeting Bluetooth mobile phones as a means for propagating viruses and Trojans into corporate networks. According to Greg Dey, a security analyst at McAfee, monetary theft is extremely latent in mobile phone payment systems. For this reason, a major virus targeting the systems is only a matter of time [20]. In 2004, the Cabir Worm SYMBOS_CABIR.A appeared on the Symbian stage as the first mobile threat [9]. Although the worm did not cause too much damage, it proved the concept of mobile worms. According to Vishal Dhupar, the Managing Director of Symantec India, there were 40 reported Symbian threats as of April 29, 2005. These hazards consisted of 20 variants of the Cabir virus, 8 variants of the Skulls Trojans and a significant number of others. "Eighty two percent of businesses worldwide agree that they consider the damage from virus attacks the same or greater on a mobile network than on a fixed network" [10, 11].

A virus or Trojan in a mobile phone can easily communicate to the corporate network and cause great damage. It can, for example, corrupt a full corporate network and delete or change valuable company information. Cardtrp is a mobile phone virus that is capable of infecting PCs. Trend Micro² reported this virus in September 24, 2005, and marked the beginning of the latest class of converged viruses. The Cardtrp virus spreads via Bluetooth and Multi Media Service (MMS) messages [12]. If the mobile phone is equipped with a memory card, then Cardtrp copies the Windows version of the virus onto the card. As soon as the user of the mobile phone inserts the memory card to his or her PC, the virus is installed. If this virus is installed on a PC which is in a corporate network then ultimately the full corporate network will be infected [12].

The second motivation for this research was inspired by propagation of viruses and Trojans into corporate networks. The third motivation for the study follows below.

1.2.3 The inefficiency of the existing Bluetooth protocol implementation and Bluetooth security manager in mobile phones

The inefficient implementation of the Bluetooth protocol stack in mobile phones is presently the primary cause for the existing security issues. The greater part of the Bluetooth mobile phones on the market are subject to one or another implementation issue [14]. For example, the Personal Identification Number (PIN) code used for authenticating a remote Bluetooth connection is too short or the default PIN is all zero in majority of Bluetooth mobile phones. Even though the Bluetooth security specification recommends a long PIN code (up to 16 bytes), many implementations limit the PIN length to only four digits. This procedure simply makes it easier for an intruder to crack the PINs and to attack the system [13]. The Bluetooth Object Exchange (OBEX) Protocol and Radio Frequency Communication (RFCOMM) services uncovered severe performance issues. Bluetooth security architecture also revealed

² Trend Micro Incorporated [<http://www.trendmicro.com>], offers a variety of antivirus products and services to protect the corporate network and to safeguard the security of the Internet content.

a shared Master key for all Bluetooth devices in the piconets and a number of other vulnerabilities [15].

Besides these vulnerabilities, the lack of proper Bluetooth knowledge among users is also responsible for many intrusions. This gives way to the next motivation, which follows below.

1.2.4 Bluetooth unawareness of mobile phone users

To a certain extent, many intrusions are a result of Bluetooth unawareness among mobile phone users. A large number of these intrusions are preventable if users turn Bluetooth to a non-discoverable mode when they find themselves in unknown locations. The same should apply when users are not using the Bluetooth feature. The users can also increase the security of their devices and prevent critical information leakage by not connecting with unknown devices. However, it remains unrealistic to create Bluetooth awareness in millions of mobile users before they start using Bluetooth-enabled mobile phones [16]. Mobile phones should be equipped with a solution to identify intrusions and to give alerts to user as and when it occurs.

The motivations explained thus far, makes it clear that it is highly important and necessary to conduct this research. The intention of the research is to come up with a solution to address the aforementioned problems.

1.3 Issues to be addressed

This research recognizes the significance of Bluetooth security in mobile phones. The key issues that are addressed in this research are put together in the questions below.

1.3.1 What is Bluetooth wireless technology and what is its significance in mobile phones?

Bluetooth wireless technology connects electronic devices and enables seamless data and voice communication by forming short range radio connections. The key traits of Bluetooth are its low price and minimal power usage. In addition, Bluetooth technology has gained global acceptance and any Bluetooth-enabled device from anywhere in the world, can connect to other nearby Bluetooth-enabled devices.

Within a short period, Bluetooth technology has become very popular. All major mobile phone manufacturers are now providing the Bluetooth feature in majority of their mobile phones. Data from the NPD Group³ reveals that nearly one in six mobile phones sold during the third quarter of 2005 was Bluetooth-enabled. Bluetooth Wireless Technology has greatly expanded in the variety of applications used in mobile phones and has played a significant role in producing new applications in mobile phones [17].

However, with the popularity of Bluetooth technology in mobile phones, intruders are inclined to find new ways to compromise mobile phones through Bluetooth technology. This has created the need to secure Bluetooth-enabled mobile phones.

1.3.2 What is Bluetooth Security, and how important is it in mobile phones?

Bluetooth security is a way to secure Bluetooth communication between various devices. The Bluetooth Special Interest Group (SIG) has categorized different security modes and security levels in its security specification [18, 19]. Bluetooth security is of the uttermost

³The NPD Group [<http://www.npd.com>], focuses in providing market research information for a wide variety of industries.

importance in mobile phones. Manufacturers of mobile phones do currently determine the level of Bluetooth security required and implement it. However, a large number of mobile phones on the market today have one or more Bluetooth vulnerabilities. The intruders target these vulnerabilities to access valuable information ranging from mobile phone address books to significant corporate data. Subsequently, such valuable information needs to be highly secured in mobile phones.

To protect the valuable information in mobile phones, there needs to be an additional Bluetooth Security mechanism. The next section addresses this issue.

1.3.3 The provision of additional Bluetooth Security mechanisms in mobile phones

Numerous Bluetooth security susceptibilities in mobile phones exist. This is either because of weak security implementation or due to weaknesses in the Bluetooth security specification. Intruders exploit these security vulnerabilities and compromise mobile phones. Current security mechanisms in mobile phones are not capable of fully securing mobile phones. As the number and usage of Bluetooth-enabled mobile phones increase, there needs to be additional security mechanisms in mobile phones.

1.4 Path to Bluetooth Logging Agent (BLA)

In this research, an attempt is made to conduct a detailed study; to analyse the existing Bluetooth security mechanisms, the Bluetooth security architecture and the current Bluetooth security vulnerabilities and limitations, which is elaborated in chapter 3. The study is extended to chapter 4 to identify the Bluetooth intrusions and the viruses and worms created as a result of flaws in the existing Bluetooth security. After analysing each of the Bluetooth intrusions, viruses and worms as identified in chapter 4, this research realizes that the Bluetooth security issues in mobile phones can be alleviated if an extra Bluetooth security mechanism exists at the mobile phone's user level. The existing Bluetooth security products

are then recognized and studied to see if they can resolve the current Bluetooth security issues and vulnerabilities in mobile phones and can be used as an additional security mechanism to protect the mobile phones from intrusions. A detailed examination of each of the existing Bluetooth security products are covered in chapter 5. The findings of this study reveals that, none of the existing Bluetooth security solutions are capable of resolving the issues addressed in this research and offers a user level protection in mobile phones. As a result the need to develop an extra Bluetooth security mechanism in mobile phones at the user level arises; that could trace all the Bluetooth activities happening in the device and instantaneously give alerts to the user as and when they occur. The security system proposed and prototyped in this research for this purpose is called the Bluetooth Logging agent (BLA) which is further addressed in the research goal which is as follows.

1.5 Research Goals

Existing Bluetooth enabled mobile phones do not have the facility to capture anonymous Bluetooth connections that are being targeted towards them. It is very important that the mobile phones should be equipped with a Bluetooth security solution such as BLA that could monitor and identify all Bluetooth activities and alert the user of intrusions as and when they occur. A security system at user's level such as BLA is needed to alleviate this problem so that intrusions and anonymous activities can be blocked by users. The main goal of this research is to prove that, if an additional Bluetooth security mechanism such as BLA is implemented in mobile phones, then the current Bluetooth security vulnerabilities and intrusions can be alleviated and as a result, the overall security in mobile phones can be improved.

This research will provide comprehensibility on using BLA in mobile phones by following a specific research methodology.

The following section explains the research methodology used to in this research.

1.6 Research Methodology

The research methodology used in this research is a combination of mainly three approaches that are typically used in the problem solving of software engineering projects. They are the waterfall model, the prototyping model and the qualitative model.

The next sections discuss this research in contour with the models.

The research begins, by adapting the process of water fall model. The waterfall model is a systematic and sequential approach, in which the development of the software is seen as flowing progressively downwards through the phases of analysis, design, implementation, testing and support [114]. The research starts with analyzing the feasibility of the research and identifying the problem statement in chapter 1. Analysis is further continued into chapter 2 and chapter 3 by giving a detailed explanation of Bluetooth and the existing Bluetooth security, its vulnerabilities and limitations respectively. The analysis of chapter 3 was led into chapter 4 by discussing the current intrusions in Bluetooth that were created from the existing security flaws. The research further progresses into chapter 5 by discussing the existing security solutions in Bluetooth and comparing these solutions in line with problem statement of the research to propose a solution to the problem statement. After a proper analysis has been carried out, the research adapts the next process of design in chapter 6 by designing the solution proposed for the research and each component in the design is extensively explained.

The research, after the design process follows a combination of the waterfall model and prototyping model. In the prototyping model, the functional prototype model is used in the research. This model attempts to simulate the design through a functioning prototype [114]. Chapter 7 explains the implementation of the design through a prototype, which is the BLA. Through the BLA, the research attempts to prove that if this proof of concept is extended to Bluetooth mobile phones and at a user level, then the current Bluetooth security issues can be alleviated. After the prototype was implemented, it was tested, thus coming back to the waterfall model to verify that the expected results were achieved.

The research then progresses into the last chapter by adapting the test strategy which is outlined in the next section for verifying and validating the test results.

1.7 Test Strategy

The test strategy used in this research is based on the qualitative research methodology. The qualitative research is defined as “a process of inquiry with the goal of understanding a social or human problem from multiple perspectives; conducted in a natural setting with a goal of building a complex and holistic picture of the phenomenon of interest” [115]. The qualitative research uses, direct observation as one of the techniques for data collection and analysis [116]. In this approach, photographs and artifacts are collected as one of the methods for data validation [117]. By following this approach, in this study, the screenshots and traces of the Bluetooth activities in BLA are collected as test data during the testing phase of the BLA Prototype for analysis, which is elaborated in chapter 7. The test data thus collected are further analysed, verified and validated against the expected conditions to see if the proof-of-concept implementation of the prototype is capable of resolving the research goals. The verification and validation of test data are further elaborated in chapter 8.

The following section explains terminology that will recur throughout this dissertation.

1.8 Terminology

The following terms are used frequently throughout the dissertation and their definitions are provided in sections below. These terms will be discussed in detail later in the dissertation, when they are encountered.

1.8.1 Bluetooth

Bluetooth is a wireless connectivity technology using short-range radio frequency waves. It is as an economical, wireless connection system for all classes of portable devices which includes but is not limited to laptops, mobile phones, Point Of Sale (POS) terminals and

Personal Digital Assistants (PDAs). In addition, it is also used to wirelessly inter connect Central Processing Unit (CPU), monitors, printers, keyboards and mouse of a PC [18].

1.8.2 Bluetooth Mobile Phone

The ‘Bluetooth mobile phone’ is a mobile phone with an inherent (built-in) Bluetooth functionality.

1.8.3 Bluetooth Protocol Stack

The ‘Bluetooth protocol stack’ is a group of protocol layers that can bring about Bluetooth wireless communication. A more precise definition explains Bluetooth protocol stack as a layered set of functional units, which communicates via a particular protocol. This communication ultimately depends on function. Therefore, each layer in a protocol stack has clearly defined duties and responsibilities. Each layer also has clearly defined interfaces to adjacent layers in the protocol stack [18].

1.8.4 Bluetooth Device Address

The ‘Bluetooth Device Address’ is basically an address of a Bluetooth device. It is termed the BD_ADDR and it is a 6 byte field which is used to recognize each Bluetooth device [18].

1.8.5 Piconet

Piconet refers to a group of Bluetooth devices joint together into a short-range network through Bluetooth connections [18].

1.8.6 Inquiry

‘Inquiry’ is a procedure whereby a Bluetooth device sends out its inquiry messages to other Bluetooth devices and waits for inquiry reply. The aim is to discover other Bluetooth devices that are within its area of coverage [18].

1.8.7 Discoverable Mode

‘Discoverable mode’ of a device refers to the mode when that device is discoverable. This means that a device communicating with another device can ‘see’ or locate that device. It is identifiable by any other device within a specific range of that device. Another definition is

as follows: A Bluetooth device is discoverable if it will respond to inquiries. This means that other Bluetooth devices in the area can discover its presence [18].

1.8.8 Non-discoverable Mode

Devices which are in this mode are not visible or identifiable to other Bluetooth devices and they will not reply to any inquiry messages [18].

1.8.9 Logical Link Control and Adaptation Protocol (L2CAP)

This protocol is implemented in the L2CAP layer of the Bluetooth and it makes available segmentation and re-assembly services which enables large packets to pass across Bluetooth links. It also allows multiplexing for higher layer protocols and services [18].

1.8.10 L2CAP Channel

An 'L2CAP Channel' is basically a logical connection at the L2CAP level between two Bluetooth devices and its purpose is to facilitate a single application per channel or a higher layer protocol [18].

1.8.11 Bluetooth Connection

'Bluetooth connection' fundamentally refers to the Bluetooth wireless connection between two Bluetooth devices. Another definition is as follows: Bluetooth connection is 'a connection between two peer applications or higher layer protocols mapped onto an L2CAP channel' [18].

1.8.12 Link key

A link key is a secret security key which is shared by two Bluetooth devices and is used to protect the communication between them. A link key authenticates one device to the other [19].

1.8.13 Pairing

Pairing is a security procedure used to generate the link key to safe guard the Bluetooth communication between two devices [19].

1.8.14 Personal Identification Number (PIN)

This refers to a user-friendly number that must be entered in the device to get the Bluetooth access to a remote device and is the start of the pairing process [18].

1.8.15 Trusted Device

This refers to a device that is trusted by the local device and is flagged as trusted in the security database [18].

1.8.16 Intrusion

In this dissertation, ‘intrusion’ is the most commonly used term. It is also known as ‘attack’, hence the terms intrusion and attack will be used interchangeably throughout the dissertation. Although the meaning of this term is quite clear, it is defined as an ‘attempt to compromise the confidentiality, integrity, and availability or to bypass the security mechanisms of a system’ [24].

1.8.17 Intrusion detection (ID)

ID is the process of capturing intrusion attempts by closely watching the activities occurring in a system [25].

1.8.18 Intruders

Intruders are also known as attackers and hence these two terms will be used interchangeably throughout this dissertation. Intruders are authorised or unauthorised users who may gain access to a system by anonymously obtaining access rights or by misusing the existing access rights allocated to them [26].

1.8.19 Intrusion Detection Systems (IDSs)

‘IDSs’ are used to detect intrusions by the use of various intrusion detection approaches [27].

1.8.20 Vulnerability

Vulnerability is basically defined as part of a system that is easily exposed to damage [28].

1.8.21 Virus

A ‘virus’ is essentially a program written with an intension to cause disastrous results to the system in which the virus program is running and to replicate itself to other systems [21].

1.8.22 Trojan

Trojans are analogous to viruses, with the exception that they are not powerful enough to replicate themselves [23].

The research plan and layout of this dissertation is presented next.

1.9 Dissertation layout

This dissertation is organized as eight chapters. *Chapter 1* introduces the dissertation, explains and motivates the research problem, proposes the BLA model, identifies the research goals, explains the research methodology, test strategy and clarifies the terminology used.

Chapter 2 provides the basic concepts of Bluetooth technology, explains Bluetooth protocol stack and gives a better idea of Bluetooth profiles. In addition, it discusses Bluetooth applications in mobile phones and other devices.

Chapter 3 gives a general idea of the current Bluetooth security architecture. It points out the issues in wireless communication, the limitations of the present security architecture of Bluetooth and the vulnerabilities and intrusions occurring in Bluetooth-enabled mobile phones. It also deals with Bluetooth security implementation issues in mobile phones.

Chapter 4 analyses each type of Bluetooth intrusion in detail. It also addresses the need for an additional Bluetooth security mechanism.

Chapter 5 proposes a solution to overcome the current vulnerabilities and intrusions. It also attempts to compare the proposed solution with the existing security products in its bid to prove the value of the research.

Chapter 6 explains the proposed solution in detail with an outline of the overall development process, the proposed design, explanation of individual modules and data flow diagrams.

Chapter 7 explains the prototype implementation for the proposed design. The prototype is also illustrated.

Chapter 8 concludes the dissertation by summarizing the importance of the study, verifies and validates the research results, analyses the feasibility of implementing the prototype in Bluetooth mobile phones and addresses the scope it leaves for future research.

2

Overview of Bluetooth

For many people who use wireless devices, a dream comes true because they are able to effortlessly communicate with others. In this scenario, different classes of wireless devices communicate simply by entering each other's proximity. This state of wireless communication enables one wireless device to fulfill the need of another. Although Bluetooth wireless technology started at the outset as a simple solution for cable replacement, it has now become an economic wireless solution, satisfying the dreams and requirements of many people. This chapter aims to provide an insight into the Bluetooth wireless technology.

2.1 What is Bluetooth?

Bluetooth is designed as a cable replacement technology using radio waves to improve wireless communication. It fulfills wireless interconnections in the form of ad hoc networks and synchronises the data and voice communication between various wireless devices. Bluetooth has become widely accepted due to its low cost, low power consumption, low complexity and robustness [29, 31].

In order to recognize Bluetooth technology and its features, one should first understand the basics of this technology. A good starting point is the history of Bluetooth, which is set out below.

2.2 The History of Bluetooth

Bluetooth wireless technology originated in 1994, when Ericsson Mobile Communications started a study to examine the alternatives to the cables that linked their mobile phones with accessories. The study looked at using radio links because of its naive advantages over infrared links, used previously to connect portable devices. The radio is not directional and does not need line-of-sight, so it has oblivious advantages over infrared links [29, 34, 35].

The name "Bluetooth" was coined from the King - Harald Blatand who ruled Denmark in the tenth-century. The name was adopted because; the Bluetooth wireless technology is expected to unify the telecommunications and computing industries. Although, the name Bluetooth was an informal name for the Bluetooth project, it became the trademark of this technology and the Bluetooth Special Interest Group (SIG) [29, 34, 35]. The next paragraph elaborates on this.

The Bluetooth SIG came in to existence in February 1998 as a result of the efforts from Ericsson Mobile Communications AB, Intel Corp., IBM Corp., Toshiba Corp. and Nokia Mobile Phones, who were the core promoters of this technology. The idea was to gain and endorse acceptance for Bluetooth technology and to define an open Bluetooth specification. The core promoters released Version 1.0 of the Bluetooth specification in the website, <http://www.bluetooth.com> in July 1999. The core promoters group was expanded with the addition of Microsoft, Lucent, 3Com and Motorola in December 1999 [29, 32]. These members have been a critical factor to the success of Bluetooth wireless technology as they had influenced its direction and development. The initial "HB" for Harald Blatand was an inspiration and became official logo for Bluetooth, which is represented in Figure 2.1.



FIGURE 2.1 THE OFFICIAL BLUETOOTH LOGO [32]
(Courtesy: <http://www.bluetooth.com>)

The next section explains the technical specifications of Bluetooth.

2.3 Bluetooth Technical Specifications

The following sub-sections discuss Bluetooth technical specifications.

2.3.1 Spectrum

Bluetooth devices operate in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz (Giga Hertz). In France it operates at 2.4465 to 2.4835 GHz frequency range whereas in the rest of the world it operates at 2.4 to 2.4835 GHz [29, 31]. The next section defines specification of range.

2.3.2 Range

The operating range of Bluetooth is determined by class of Bluetooth device used which falls into the following three classes [31]:

Class 3 devices – These devices operates within one meter.

Class 2 devices – These devices operate within ten meters, and are mainly used in mobile phones.

Class 1 devices – These devices operates within 100 meters.

2.3.3 Power

Bluetooth is designed with a view of minimal power consumption and Bluetooth radios are powered down when in inactive [31].

2.3.4 Data Rate

Bluetooth operates within 1 Mbps (Mega Bits per Second) data rate [31].

2.3.5 Connection Specifications

The Bluetooth connection setup procedures are as follows [31]:

- A Bluetooth device can take the role of either a slave or a master during the connection setup. The device that initiates the communication, usually takes on the master role and the slave device accepts the communication request.
- The master and slave device transmits or receives in even and odd time slots respectively.
- Bluetooth ad-hoc networks called piconets are formed to share the communication channel. A piconet has a master device which controls the communication and supports up to seven slave device.
- Bluetooth supports two data transfer modes. They are SCO (synchronous connection oriented) for voice transmissions and ACL (asynchronous connectionless) for data transmissions.

The next section analyses the Bluetooth protocol stack.

2.4 Bluetooth Protocol Stack

The Bluetooth protocol stack was developed with the aim of taking advantage of and re-using existing protocols for different purposes at the higher layers. The following figure illustrates the architecture of the Bluetooth protocol stack.

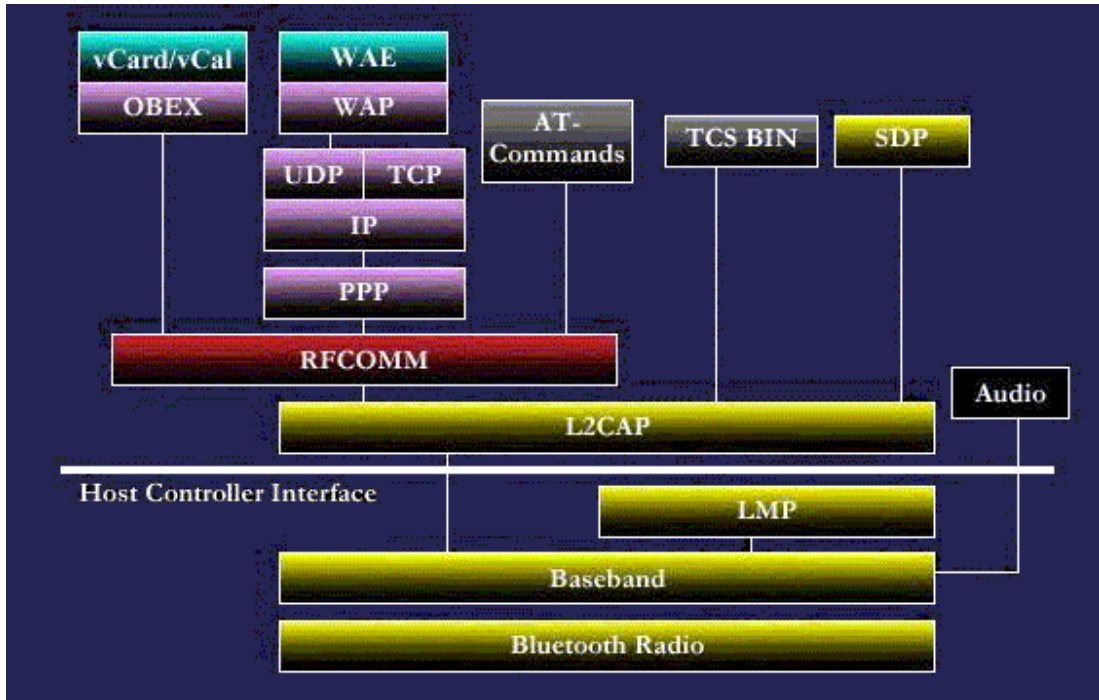


FIGURE 2.2 BLUETOOTH PROTOCOL STACK [38]
 (Courtesy: <http://www.tutorial-reports.com>)

As seen in Figure 2.2, the Bluetooth protocol stack consists of Bluetooth specific protocols combined with non Bluetooth specific protocols like User Datagram Protocol (UDP), Transmission Control Protocol (TCP), Internet Protocol (IP), Object Exchange Protocol (OBEX), vCard, vCal and Point to Point Protocol (PPP). The main advantage of this structural design or architecture is the modification of available applications to operate with the Bluetooth Technology. It also grants access to commonly used applications over Bluetooth specific protocols. This architecture, in effect, provides new applications and existing applications (developed by different vendors) to gain maximum benefit from Bluetooth [36].

The protocol stack is categorised into four core layers based on their functionality. The protocols belong to the layers as presented in Table 2.1.

| Protocol Layers | Protocols in Bluetooth stack |
|------------------------------------|--|
| Bluetooth Specific Protocol Layers | Baseband, LMP, L2CAP and SDP |
| Cable Replacement Protocol Layer | RFCOMM |
| Telephony Control Protocol Layers | TCS Binary and AT-Commands |
| Adopted Protocols | PPP, UDP/TCP/IP, OBEX, vCard, vCal, WAP and WAEA |

TABLE 2.1

Bluetooth Radio is at the bottom of the stack and its function is to transmit and receive data on the physical radio channel. The Bluetooth specification also recognizes a Host Controller Interface (HCI) in addition to the above protocol layers mentioned in Table 2.1. This layer provides an interface between the higher layers such as L2CAP and RFCOMM and lower layers such as Baseband and Link Management Protocol (LMP) of the protocol stack. In situations where the higher layers executes on a host device's processor and the lower layers on the Bluetooth device, HCI acts as interfacing mechanism between these two devices. A typical set-up is a Bluetooth card plugged into a PC. In this case, the higher layers will run in PC, the lower layers will be in the Bluetooth card, and the HCI component will provide the necessary interfacing functionality [31]. The next section gives an overview of the core Bluetooth protocols.

2.4.1 Bluetooth Core Protocols

The core Bluetooth protocols defined by SIG are Baseband, LMP, L2CAP and Service Discovery Protocol (SDP) and they are set out in the following sub-sections.

2.4.1.1 Baseband

The Baseband layer's functionality is to provide a physical Radio Frequency (RF) link between two Bluetooth devices. It carries out several operations at the link-level according to the higher-level commands from the Link Management Protocol. Baseband offers two different kinds of links between device, namely SCO and ACL links. ACL links are used for

transmitting data where as SCO links are used for data and audio transmissions [36, 37]. The following subsection clarifies the audio component.

2.4.1.1.1 Audio

A major function of Bluetooth is to be a carrier of audio information. SCO packets encapsulate the audio data and the Baseband directly routes these packets. It does not make use of L2CAP. The audio functionality enables the usage of built-in Bluetooth devices like wireless headsets [36, 37]. Above the Baseband protocol is the LMP protocol, which is explained in the next section.

2.4.1.2 Link Management Protocol

The LMP is responsible for creating, modifying, and releasing links between Bluetooth devices. LMP is also responsible for authenticating and encrypting logical links. It also helps to control the power modes and the connection states of the Bluetooth devices in piconets [36, 37]. Above the LMP protocol is the L2CAP protocol, which is described in the next section.

2.4.1.3 Logical Link Control and Adaptation Protocol

L2CAP operates over the Baseband, and it interfaces with SDP, RFCOMM and TCS. The main purpose of L2CAP is to offer data services to the upper layer protocols through protocol multiplexing capability, segmentation and reassembly operations and using group abstractions. L2CAP layer presents logical channels (called L2CAP channels), which permits the applications and protocols above L2CAP to exchange L2CAP data packets up to 64 kilobytes in length [31, 36, 37]. As explained earlier, SDP is one of the protocols that interface with L2CAP protocol. The next section elaborates on this.

2.4.1.4 Service Discovery Protocol

The SDP layer is responsible for querying the services offered by other Bluetooth devices. Its main functionality is to discover the services and their attributes that are available in other Bluetooth devices [36].

Besides SDP, another protocol that has interfaced with L2CAP is RFCOMM. The next section discusses this protocol.

2.4.2 Cable Replacement Protocol - RFCOMM

The cable replacement protocol-RFCOMM emulates the RS-232⁴ ports functionality used for transferring data and signaling. It operates over the Bluetooth Baseband and provides services for upper layer protocols that use serial line as a mechanism for transferring data [36, 37].

The last protocol that interfaces with L2CAP is the TCS Binary. The next section explains this further.

2.4.3 Telephony Control Protocols

The Bluetooth framework uses the TCS Binary and AT- Commands to achieve its telephony functions. The next sub-sections details these protocols.

2.4.3.1 TCS Binary

Telephony Control Protocol – Binary, TCS Binary outlines how telephone calls transmit across a Bluetooth link. It gives guidelines for the signaling to set up both point to point and point to a multipoint calls [36, 37].

2.4.3.2 AT- Commands

A number of AT- Commands transmit control signals for telephony and makes use of the RFCOMM for data transmission [36]. Besides the above Bluetooth specific protocols, Bluetooth protocol stack reuses the functionalities of certain adopted protocols. The next section explains these adopted protocols.

⁴RS-232 is an acronym for 'Recommended Standard no. 232'. This is the EIA (Electronic Industries Association) approved standard for communication via pc serial ports.

2.4.4 Adopted Protocols

The following sub-sections clarify the adopted protocols used by Bluetooth framework.

2.4.4.1 PPP

The Point-to-Point Protocol (PPP) runs over RFCOMM and is used to carry packets from the higher layers across RFCOMM [36].

2.4.4.2 UDP/TCP/IP

The UDP/TCP/IP standards are provided to enable the Bluetooth devices to communicate with other Bluetooth units connected and to use their UDP/TCP/IP services, such as the Internet. The Bluetooth unit in this case can work as a bridge to the Internet. Internet Bridge and OBEX use the TCP/IP/PPP protocol configuration and the UDP/IP/PPP configuration is used in WAP [36].

2.4.4.3 OBEX Protocol

Object Exchange Protocol (OBEX) is designed to allow devices to exchange arbitrary data objects. For example, a PDA might pull a file from a mobile phone, or a mobile phone synchronising an address book might push it into a laptop. OBEX primarily makes use of the vCard and vCal content formats to swap data [36, 37].

2.4.4.4 WAP

This protocol facilitates the mobile devices to access the Internet and to use telephony services. In WAP protocol, the Wireless Application Environment (WAE) forms the top layer of the architecture, and it provides an environment for developing WAP applications. The WAP is adopted as a part of the Bluetooth stack to assist in the reuse of these applications [36, 37].

Besides the Bluetooth protocol stack, Bluetooth devices are also equipped with Bluetooth profiles. Bluetooth profiles guarantee interoperability and prescribe the use of Bluetooth specification in applications. The next section gives an overview of Bluetooth profiles.

2.5 Bluetooth Profiles

Bluetooth profiles refer to a set of procedures that should be followed when developing applications over Bluetooth. The aim of the profiles is to make sure that different Bluetooth devices from different manufacturers will be able to interoperate [39, 40, 41].

The following sub-sections explain the major Bluetooth profiles.

2.5.1 Generic Access Profile (GAP)

GAP defines a basic set of procedures that all Bluetooth devices use both in handling connections and user interfaces [41].

2.5.2 Serial Port Profile (SPP)

SPP defines how the serial ports should be emulated in Bluetooth products. By adopting this profile, the applications that use serial ports can work over Bluetooth [41].

2.5.3 Service Discovery Application Profile (SDAP)

This profile specifies how a service discovery application should be supported in Bluetooth products [41].

2.5.4 Generic Object Exchange Profile (GOEP)

This profile defines how the Bluetooth devices implement the OBEX data models [41].

2.5.5 Object Push Profile (OPP)

This profile defines the Object push use case which involves the pushing, pulling and exchanging of data objects between Bluetooth devices [39].

2.5.6 File Transfer Profile (FTP)

This profile defines the wireless file transfer use case which involves the transferring and browsing of files in Bluetooth devices [40].

2.5.7 Synchronisation Profile (SP)

This profile defines how to facilitate the data synchronisation between Bluetooth devices [41].

2.5.8 Headset Profile (HSP)

This profile defines the requirements of the Bluetooth headset usage model between devices such as headsets, mobile phones and laptops [39].

2.5.9 Hands-Free Profile (HFP)

HFP defines how to provide the hand-free usage model between Bluetooth devices [40].

2.5.10 Cordless Telephony Profile (CTP)

This profile defines how to support cordless telephony in Bluetooth [40].

2.5.11 Intercom Profile (IP)

The IP defines the intercom functionality of Bluetooth [39].

2.5.12 Dial-up Networking Profile (DUN)

This profile defines how Bluetooth can be used to access a network by means of a Bluetooth device which can provide a dial-up connection for example by the use of a modem or a mobile phone [39, 40, 41].

2.5.13 Fax Profile (FP)

The Fax Profile defines the procedures for sending and receiving faxes without wires [39].

2.5.14 LAN (Local Area Network) Access Profile (LAP)

The LAN Access Profile defines how Bluetooth devices access a fixed network by the use of Bluetooth LAN Access Points [39, 40].

The next section explains the network topology used in Bluetooth.

2.6 Network Topology

The Bluetooth network topology is classified as a point-to-point connection or a point-to-multipoint connection [29, 31].

The following sub-sections explain Bluetooth network topologies.

2.6.1 Piconet

Piconet is defined as a collection of Slave devices operating together with one common Master. The simplest piconet is formed when there are only two devices to communicate, and this scheme is illustrated in Figure 2.3.

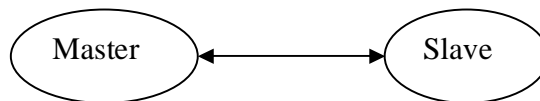


FIGURE 2.3 BLUETOOTH PICONET (POINT-TO-POINT)

Another Piconet scheme involves multiple devices. In this case, where multiple slaves connect to the master, the communication topology becomes point-to-multipoint and Figure 2.4 illustrates this [42].

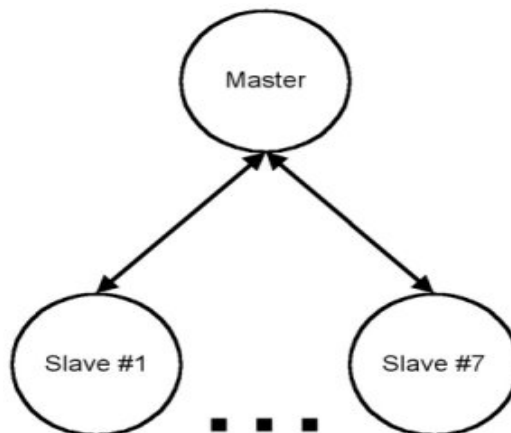


FIGURE 2.4 BLUETOOTH PICONET (POINT-TO MULTI POINT)
(Courtesy: <http://www.wirelessdevnet.com>)

In order to maximize the use of the available spectrum, several piconets can co-exist exist in the same area to form scatternets. The next section explains this.

2.6.2 Scatternet

A group of piconets that are joined together by common members is called a scatternet [29]. Figure 2.5 illustrates the scatternets. The members linking the piconets can be Slaves on both piconets and a Master of one piconet and a Slave on another.

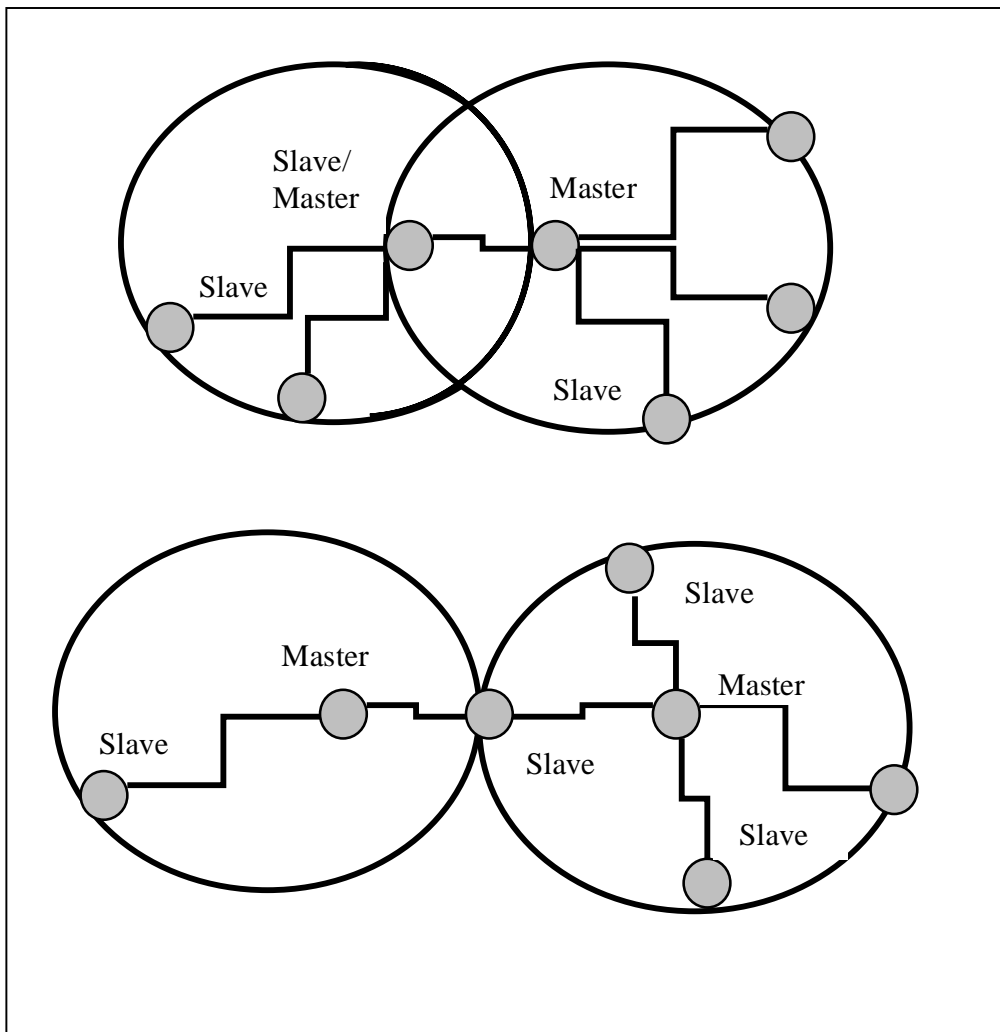


FIGURE 2.5 BLUETOOTH SCATTERNETS

Figure 2.5 depicts two different examples of scatternets. On the first scatternet, a device acts as a master in one piconet where as it acts as a slave in another. On the second scatternet, a device is a slave to two different masters.

The next section discusses Bluetooth operational procedures and modes.

2.7 Operational Procedures and Modes

Bluetooth devices operate by establishing connections and exchanging data with other devices in its range. A number of operational procedures form piconets to enable subsequent communications. The operational procedures and modes are relevant at different layers and device can be in multiple modes and procedures at the same time. The following sub-sections give an overview of the operational procedures and modes used by the Bluetooth devices.

2.7.1 Inquiry Procedure

This procedure is used by the Bluetooth devices to find out other Bluetooth devices in its range. The Bluetooth device that tries to find other nearby devices is called an inquiring device. An inquiring device sends inquiry messages actively; other Bluetooth devices listen for the inquiry requests and they respond to the inquiry messages and their by they will be discovered in the process [29, 31].

The next sub-section explains the procedure of paging.

2.7.2 Paging Procedure

The paging procedure is also known as connecting procedure. In this, the device which initiates the connection or page procedure sends page messages to other devices in its vicinity; other device stays in the page scanning mode. In page scanning, the Bluetooth device is waiting for paging or for a connection request from the other device and respond to the paging message [29, 31].

When the paging succeeds, the devices enter into the connected mode; this is described in the next sub-section.

2.7.3 Connected Mode

After a successful connection procedure, the devices are physically connected to each other. In connection mode, there is a physical link between the devices and there are logical links. When in the connected mode, it is possible to create and release additional logical links, and to change the modes of the physical and logical links while remaining connected to the piconet physical channel. It is also possible for the device to carry out inquiry, paging or scanning procedures or to connect to other piconet, without having to disconnect from the original piconet physical channel [29, 31].

Now that the operational procedures and modes of Bluetooth technology are explained, the next section will highlight the applications of Bluetooth technology.

2.8 Applications of Bluetooth Technology

Bluetooth has remarkable applications and a huge potential in information transfer and synchronization especially in confined settings. The following sub-sections are only a small representation from numerous Bluetooth applications. In the near future, a huge increase of more complex Bluetooth applications can be expected [42, 43, 44].

2.8.1 Infotainment

Bluetooth integrated infotainment systems can communicate with Bluetooth in mobile phones to access data. The Global System for Mobile Communication (GSM)⁵ modules may use this data, their by avoiding the need for an additional SIM card. A Bluetooth hands-free profile implemented in the car can establish Bluetooth connections with the mobile phone of the user, and it also allows the user to make use of the same mobile phone in different cars.

⁵ GSM is a mobile phone technology based on Time Division Multiple Access (TDMA).

2.8.2 Load Truck Management

Load trucks use PDAs as a user interface for navigation systems and fleet management. The PDA may connect to the system via Bluetooth; and vehicle related information might also be supplied to the PDA via Bluetooth.

2.8.3 Diagnostics

The replacement of cables with Bluetooth connections simplifies diagnostic equipment for vehicle repair. For example, serial cables are replaceable by Bluetooth links and the data can be exchanged from the vehicle and the diagnostics equipment

2.8.4 Medical

Bluetooth has noteworthy benefits in the medical field. Bluetooth is extensively used to monitor the activities of patients remotely, to capture the biometric data wirelessly and in medicine dispensers.

2.8.5 Automotive

Bluetooth can remotely control audio or video equipment of a car. However, the main usage of Bluetooth in a car is the hands-free telephony.

2.8.6 Point-of-sale payments

The Bluetooth-enabled mobile phones and PDAs are extensively used as a method of payment in point-of-sale (POS) terminals.

Apart from the above-mentioned applications, Bluetooth technology has a wide range of applications which are explained as follows.

- We can eliminate the involved and monotonous duty of establishing network connections between the computing devices in an enterprise if we setup the enterprise with a Bluetooth network installation.

- With the usage of Bluetooth device one is not constrained to work in fixed locations as the Bluetooth device can establish connections with other devices in its range and can make the computing very easy
- By using Bluetooth, the peripherals of a PC or laptop can be interconnected wirelessly.
- With Bluetooth, mobile phones and digital cameras can send still or video images to photo processing kiosks and get the prints instantaneously.
- Bluetooth phones support the three way phone use case. At home, it can be used as a portable phone, when the user moves between places it functions as a mobile phone and when the phone comes within the vicinity of another Bluetooth enabled phone it functions like a walkie-talkie.
- Bluetooth is very handy in business conferences and meetings in that it can send documents and exchange business cards instantaneously.
- The Bluetooth headset can be connected to the mobile phone or any Bluetooth computing device to keep us hands-free for doing other important tasks.
- Bluetooth offers automatic data synchronization between various computing devices.
- Bluetooth is also used in a wide variety of applications in the airline industry and hotel industry.

Now that the applications of Bluetooth technology have been explained, the next section summarises this chapter.

2.9 Summary

Although Bluetooth started as a cable replacement technology to improve the communication, it has become one of the most powerful technologies and a day-to day necessity. This chapter explained the technical side of Bluetooth, including the technical specifications, Bluetooth protocol stack, Bluetooth profiles and Bluetooth operations and procedures to get a better understanding of the fundamentals of this technology. Bluetooth is now extensively adapted in industries, including the medical, travel and hotel industries. Bluetooth is also used in pay-point sales, in our day-to day lives and in many real time operations. This chapter thus explained Bluetooth applications and the benefits in using Bluetooth.

Although Bluetooth has been slowly accepted in the market, it is now starting to become more and more prevalent. Since it satisfies the preliminary need of closer range connectivity, it has a very high potential. However, Bluetooth's high reputation is also linked to several security vulnerabilities, which are explained in the next chapter.

3

Bluetooth Security, its vulnerabilities & limitations

Wireless communications significantly improves the communication infrastructure in organisations and offers users many benefits. It covers a wide range of different capabilities for various uses and requirements. The four key benefits of wireless technology identified are as follows:

1. Increased efficiency – Improved communications lead to faster data-transfer and the result is in increased efficiency.
2. Portability – With wireless communication, there is no need to carry cables or adapters when moving from one place to another.
3. Greater flexibility and mobility for users – Wireless communication devices can be easily networked. As a result, people can work together, even if they are in remote places.
4. Reduced costs – Wireless communication is relatively cheaper to setup and maintain than wired communication.

Regardless of all these advantages, wireless devices are less secure than the wired devices and Bluetooth is not any different [29]. The main reason for this is that the underlying communication medium employed in wireless devices (the radio waves) is easily accessible

to intruders. However, as with any wireless technology, Bluetooth is also equipped with its own built-in security mechanism. This chapter is a study of the Bluetooth's built-in security mechanism, which is fundamentally in the form of frequency hopping, authentication and encryption. This chapter analyses wireless security vulnerabilities in general, as well as Bluetooth security vulnerabilities, the limitations of Bluetooth security and the current Bluetooth security implementation issues in mobile phones.

3.1 What is Bluetooth Security?

With the attractiveness of features that Bluetooth wireless technology today presents in various Bluetooth-devices, it is clear to see that organisations use Bluetooth devices extensively. Just like laptops and PCs, Bluetooth devices such as mobile phones, PDA's and other resource constrained devices are accomplishing important tasks. As a result, the information residing in these devices is very often confidential, highly sensitive and very valuable. This type of information thus needs to be highly secured. Bluetooth security essentially is a way of securing the communication between different Bluetooth devices and a way of protecting the information residing in the Bluetooth-enabled devices.

The three main security mechanisms used in Bluetooth are frequency hopping, authentication and encryption. These security mechanisms are discussed in detail in the following sub-sections.

3.1.1 Frequency hopping

The design of Bluetooth allows it to function in strident radio frequency settings. Bluetooth utilizes a speedy frequency hopping scheme to secure the Bluetooth link, and to make it robust during communication. Comparing to other wireless technologies using the same frequency band, the Bluetooth radio uses faster hops and shorter packets [49].

3.1.2 Authentication

Authentication in Bluetooth security is in the form of a 'challenge-response' scheme which uses the challenge-response protocol. The challenge-response protocol authenticates devices by verifying a secret key in the devices called the Bluetooth link key. There are two devices

in the authentication procedure. They are the claimant and the verifier. The claimant is the device trying to prove its identity, and the verifier is the device validating the identity of the claimant. The authentication procedure is uni-directional, in other words, the procedure repeats with the roles for verifier and claimant switched over to achieve mutual authentication [29].

3.1.3 Encryption

Besides authentication, Bluetooth uses the encryption security mechanism to obstruct eavesdropping on the air-interface. Encryption protects the payloads of the packets exchanged between two devices. The Bluetooth specification permits three different encryption modes. These modes are as follows:

- Encryption Mode 1 – There is no encryption on any traffic.
- Encryption Mode 2 – The broadcast transmission is not protected, that is not encrypted. Traffic is encrypted according to individual link keys.
- Encryption Mode 3 – All traffic is encrypted according to the master link key.

The next section gives an outline of the Bluetooth security architecture.

3.2 Bluetooth Security Architecture

With the purpose of providing usage protection and information confidentiality, Bluetooth is set with its security mechanism both at the application level and at the link level. At the base of Bluetooth's security features is a secret link key, which is shared by a pair of devices. When the two devices communicate for the first time, a pairing procedure generates this key. To keep transmissions secure and robust, Bluetooth makes use of frequency hopping. This not only improves transparency but it also reduces eavesdropping by permitting only synchronised devices to communicate with each other. All Bluetooth devices have individual addresses called the BD_ADDRESS, hence each device can identify the other device connecting to it.

The initialisation process in Bluetooth devices uses a Personal Identification Number (PIN). This PIN is known as the 'Bluetooth passkey'. The PIN length can be up to 128 bits (16 bytes) [29]. The following sections explain the Bluetooth security in more detail.

3.2.1 Bluetooth Security Modes

According to the Bluetooth specification, Bluetooth devices mainly have three security modes [19, 52, 53]. They are as follows:

Security Mode 1 - Non secure mode

Security mode 1 is the most insecure mode. Devices in this mode do not have any security procedure and the security functionality is entirely bypassed. The Bluetooth device in this mode is in a promiscuous state or in a discovery mode. This permits other devices to connect to it. This mode is mainly used by applications that do not need any security. An example of such an application is exchange of business cards.

Security Mode 2 - Service level enforced security mode

In this mode, security is imposed in devices after a L2CAP connection is established. Security is enforced in Mode 2 after L2CAP connection is established between the devices.

Security Mode 3 - Link level enforced security mode

Mode 3 enforces that devices commence security procedures before setting up an L2CAP connection. This security procedure is the inbuilt security mechanism in the device. This mode also supports encryption and authentication using a secret link key. A pairing procedure generates this key when the two devices communicate for the first time.

Apart from the above three security modes, Bluetooth also has security levels for services and devices. These are explained in the following sections.

3.2.2 Bluetooth Security Levels

The following sub-sections discuss Bluetooth security levels.

3.2.2.1 Authentication and Authorization

Authentication is the process of identifying the devices before a connection takes place. Authentication takes place via the secret link key or by pairing [19]. The next section explains pairing in detail.

Authorisation is the process of validating whether a particular device has access to a service on another device. Devices that are allowed access are known as the trusted devices, and will be indicated as trusted. Unknown devices will have to first acquire authorisation from the user before accessing a service. Authorisation can also be provided automatically by an application [19].

3.2.2.2 Pairing and Bonding

The Bluetooth Generic Access Profile (GAP) calls two devices that recognise that they share a link key as 'bonded'. Bonding refers to the step-by-step procedure to create a relationship based on a common link key. Bonding means there is a link created particularly for the purpose of creating and exchanging a common link key. For the period of bonding, the link managers verify that they share a secret key through authentication. After authentication, the link managers create and exchange a link key. The link level procedures of authentication and link key generation are collectively called pairing. Bonding may involve higher layer initialisation procedures as well as link level pairing. The term 'Bluetooth Bonding' is used at the user interface level, to refer collectively to bonding and pairing procedures [29].

3.2.3 Bluetooth Security Architecture

Bluetooth Security is typically implemented in devices according to Figure 3.1.

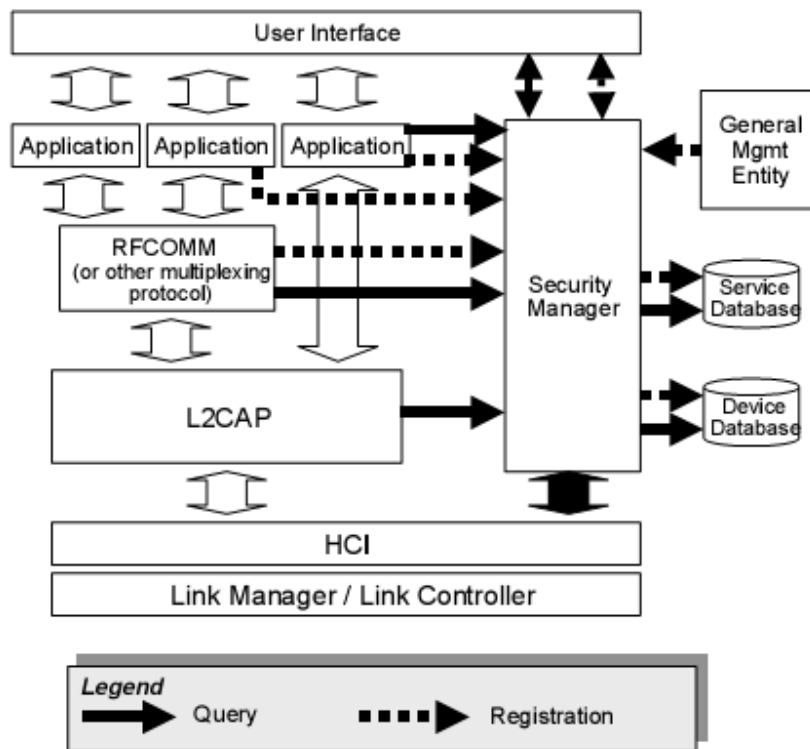


FIGURE 3.1 BLUETOOTH SECURITY ARCHITECTURE [19]
 (Courtesy: <http://www.bluetooth.com>)

The main component in the security architecture is the security manager. The functionalities performed by this component are given below.

- Store security related information in the service database for all the services.
- Stores security related information in the device database for all the devices in range.
- Grants or denies access requests using applications or by protocol implementations.
- Imposes encryption and authentication before a connection takes place.
- It initiates to set up a trusted relationship from a device by processing the inputs from a human operating device called the External Security Control Entity(ESCE)
- Starts the pairing process and obtains the PIN from ESCE or an application.

The next section discusses the vulnerabilities of wireless security.

3.3 Wireless Security Vulnerabilities

By entering even into the remotest parts of the world, wireless technology serves many convincing human purposes. The IEEE 802.11⁶ wireless standards have gained vast public acceptance and are becoming more widespread in the marketplace. The deployment of wireless networks gives customers, partners and employees the freedom of mobility from within and outside of an organisation. Wireless technology assists businesses in becoming more productive and effective. It decreases an organisation's costs, improves its relationships with its business partners, and attracts new customers. Conversely, wireless technology also brings many security vulnerabilities associated with traditional wired networks. The following section addresses these wireless security vulnerabilities.

3.3.1 WarDriving

The name 'wardriving' was adopted from 'war dialing'. As the name suggests war dialing is the method of using a modem connected to a computer to dial telephone numbers (often sequentially, for example dialing 011-2345844 followed by 011-2345845, and so forth) to locate other computers that are connected to modems [54]. Wardriving uses the same concept; the only difference is that, it is used in wireless networks. Using a Global Positioning System (GPS), a notebook computer with wireless functionalities and special software, an intruder can find other wireless access points. The special software stores latitude, longitude and configuration of the access points found along the driver's route [55]. Once the access points are discovered, the intruder uses a software program to map the results of the wardrive. Based on these results, a statistical analysis is carried out. This statistical analysis can be of one drive, one area, or a general overview of all wireless networks. The concept of driving around to find wireless networks probably began the day after the first wireless access point was set up. Wardriving became better known when Peter Shipley, a computer security consultant in Berkeley, California automated the process. In 2000, Shipley performed an 18 month survey in Berkeley. His results were presented at the

⁶ Institute of Electronic and Electrical Engineers (IEEE) is an organization that promotes electrical engineering world wide. IEEE has fostered many standards, including the IEEE 802.11 standard for wireless LANs.

DEFCON⁷ hacker conference in July 2001. His main intention was to make people aware of the insecurity of wireless networks. This laid the foundation for the 'true' wardriver [54, 55].

Reports by WorldWide Wardrive (WWWD) 4 in June 2004 revealed that 61.6 percent of all wireless access points put forward to the WWWD forum were broadcasting data with no encryption enabled. In other words, anyone listening in could easily view the data or packets sent by these wireless devices. Usernames, passwords, credit card numbers and other sensitive information could be included in the data. The study furthermore revealed that 31.4 percent of the logged access points were using default Service Set Identifiers (SSIDs)⁸ which made them easy to find and access. It showed that 27.5 percent were using no encryption with default SSIDs [54]. Wardriving is the first step performed prior to an intrusion or attack. The following sections explain various intrusions or attacks occurring in the wireless domain.

3.3.2 Denial of Service (DoS) attacks

DoS attacks are attacks that prevent users from accessing available services that they have. A DoS attack can be performed by flooding the network with faulty packets to group legitimate traffic and to cause systems not to respond [55]. Wireless networks are more susceptible to DoS attacks. The cause may be due to various factors, like limited bandwidth, communication medium (open radio waves), mobility and poor routing functionalities [56]. It is difficult to prevent DoS attacks in wireless networks. Protection against these attacks is also complex. Such attacks can cause a severe degradation in terms of the achieved throughput and latency.

DoS attacks fall into two types, those that are at the routing layer and those that are at the Media Access Control (MAC) layer. The side effects of a routing layer-DoS attack in the

⁷ DEFCON (<http://www.defcon.org>) is the world's largest annual hacker convention, held annually in Las Vegas.

⁸ SSID is unique identifier of length 32 characters, attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to the BSS (Base Station Subsystem). The SSID differentiates one WLAN from another.

wireless network are deterioration in the quality of the connection, frequent route failures, performance degradation and loss of packets. The primary side effect of a MAC layer DoS attack is battery drainage of the devices in the wireless network.

The next section explains man-in-the-middle attacks.

3.3.3 Man-In-The-Middle attacks

Similar to the DoS attacks, Man-In-The-Middle (MITM) attacks also occur more on wireless networks than wired networks. In an MITM, an intruder is able to modify or insert a message between two devices without both of the devices knowing [57]. The main two MITM attacks are eavesdropping and manipulation.

In eavesdropping, the intruder listens to the communication between different devices. The result of eavesdropping is an information leak, in which sensitive information can be provided to a third party without the consent of actual owner of the information. In ‘manipulation attack’, the unauthorised information received through eavesdropping is changed to suit the intruder. This information may be spoofing an IP address, change a MAC address or any other type of modification [55].

3.3.4 Address Resolution Protocol (ARP) poisoning

In ARP poisoning, objects that use TCP/IP as their communication protocol are allowed to identify the IP addresses of other hosts in the network. The ARP will first broadcast a request to a particular host to identify its IP address. The host will receive the request and acknowledge it. Then the source device will store the host’s MAC address and IP address in its cache memory, so that future connections can be made from the reference in the cache memory.

In ARP poisoning, the intruder sends illegitimate packets with a spoofed IP address claiming that the IP address belongs to the intruder. All transmissions from the host are routed to the intruder’s device and not to the actual source. This will then allow the intruder's device to eavesdrop on communications. Responses are even manipulated to intensify the intrusion.

3.3.5 Wired Equivalent Privacy (WEP) intrusions

A very well known security scheme in wireless networks is the Wired Equivalent Privacy or WEP authentication. The use of WEP implies that the network is more secure than a completely open wireless network. Nevertheless, WEP is particularly inadequate for a wireless network. The following paragraphs explain the reason for this.

In WEP, each encrypted frame uses an RC4⁹ stream cipher that is decrypted at the access point. The data is encrypted as follows: WEP uses a secret key called 'WEP key' and adds it with a 24-bit piece of data called the initialization vector, or IV. WEP key is added with IV because IV can be changed with each transmission, and this will increase the life of the WEP key. WEP uses this with a random number generator to create the stream. At the receiving end or access point this stream is recalculated and is compared with the received data to make sure of its integrity [55].

As WEP is vulnerable, intruders use various techniques to compromise WEP schemes. Essentially, WEP intrusions fall under three categories: brute-force intrusions, passive intrusions and active intrusions. In brute-force intrusion, determining the shared 'WEP key' will identify and exploit the key weaknesses within the WEP Algorithm. In passive intrusion, the intruder sniffs the packets and gathers valid information such as the Access Point (AP) configuration, the services running in the network, the encryption and authentication scheme employed and the length of the 'WEP key'. The active intrusion focuses on injecting packets into the current wireless stream. This is possible with the information collected from the brute-force intrusion and passive intrusion [58].

Now that the general wireless security vulnerabilities are clearer, the next section focuses specifically on Bluetooth security vulnerabilities.

⁹ In cryptography, RC4 (also known as ARC4) is the most widely used and popular software stream cipher. It is used in popular protocols such as Secure Sockets Layer (SSL) and WEP.

3.4 Bluetooth Security Vulnerabilities

Bluetooth, together with other wireless networks, can form ad hoc network that has different security mechanisms and vulnerabilities [62]. In an ad hoc network, there are no fixed infrastructures. As a result, security in the wireless networks is also complicated. In securing ad hoc networks, the role of authorisation and key management is significant. The most vulnerable points of attack are trusted third party and identity-based schemes for key agreement. However, it is possible to build a good authentication mechanism for ad hoc networks in most cases [62]. The use of proper authentication and encryption controls are necessary when one refers to confidentiality. With regard to wireless communications, attackers are able to sniff messages on the air without using these controls. Integrity attacks are similar to confidentiality attacks. They occur through unintentional and intentional radio interference propagation.

A large number of the mobile phones and other Bluetooth devices on the market today have critical vulnerabilities in terms of Bluetooth security. These Bluetooth security susceptibilities are classified in to fundamental vulnerabilities and implementation vulnerabilities. The following sub-sections explain these vulnerabilities.

3.4.1 Fundamental vulnerabilities

Bluetooth is no different from all the broadcast technologies that disclose some information. Despite Bluetooth's use of the encryption scheme to hide the contents of its message traffic, it is still vulnerable to traffic analysis [51]. A single connection may not have much sensitive information, but the possibility of sensitive information in a large number of connections cannot be ignored. Although Bluetooth devices have a limited range, sensitive Bluetooth receivers can span across a greater distance than the operational distance.

Bluetooth is exposed to DoS attack [51]. In order to form ad hoc connections with other Bluetooth devices in its proximity, a Bluetooth device continually broadcasts its identity and presence. This broadcast contains information such as the Bluetooth Device Address and the device name. It may also contain sensitive information such as the International Mobile

Equipment Identity (IMEI). The device broadcasts constantly until another device recognises it. An intruder can therefore easily make use of this security vulnerability to track and monitor the device. The next section explains implementation-induced vulnerabilities.

3.4.2 Implementation-induced vulnerabilities

Most of Bluetooth's security implementations on devices rarely attain the security embedded in the Bluetooth security standard or protocol. This is partially due to the difficulty in implementing the Bluetooth security standard and partly due to the improper Bluetooth security implementations [51, 59, 60]. The following paragraphs address some implementation-induced vulnerability.

The Bluetooth security standard necessitates that security implementations include (a) random inputs to key generation routines and (b) initialisation vectors for performing encryption. These values are either selected randomly or from the available sample space. If this is not the case, the Bluetooth security implementation may be less secure than what the sample space might suggest. The majority of the Bluetooth devices do not tackle this issue, and hence they are vulnerable [51, 59, 60].

When Bluetooth applications are implemented developers are prone to include extra generality and flexibility. Intruders exploit this extra generality and flexibility to their own benefits [51, 59, 60].

Bluetooth security PINs are of 1 to 16 octets (8 bits to 128 bits) in length, depending on the degree of security required in applications. Although the Bluetooth security standard emphasises the use of long PIN codes, many Bluetooth security implementations use PIN lengths only up to four. Bluetooth devices that do not have any user interface for entering PIN codes such as headsets, car-kits and modems have fixed pre-defined PIN codes that are values like '0000' or '1111'. These PIN codes can be easily guessed and hence these devices are indeed vulnerable [51, 59, 60].

Based on the Bluetooth security specification, a Bluetooth device that uses a unit key¹⁰ for authentication and encryption can only use one unit key for all its secure connections at any given time. The above requirement in using the unit key is a Bluetooth security vulnerability and it opens the door for possible intrusions. In the unit key scheme, all the trusted devices participating in the group communication know the unit key. Hence, any device can eavesdrop on any communication between the devices in the group. In a Bluetooth group communication, the master devices distribute the unit key to all the devices. Due to this security vulnerability, any trusted device can compromise any other trusted device, even the master device. Intruders exploit the above vulnerabilities and compromise Bluetooth devices. The next section addresses the intrusions occurring in Bluetooth devices, especially in mobile phones.

3.5 Bluetooth Security limitations

Bluetooth security implementations are not at all satisfactory, and have some crucial limitations [63]. The following scenarios demonstrate the limitations of the Bluetooth security architecture.

- Scenario 1: Two Bluetooth devices (for example two mobile phones) communicate with each other to carry out a task such as file synchronisation [19, 61].
- Scenario 2: Two or more Bluetooth phones communicate with each other to carry out tasks for which security is not mandatory, such as exchanging business cards [19, 61].
- Scenario 3: This would be in scenarios such as a mobile phone requiring access to connect to a banking environment through a Bluetooth link. It will first connect to a Local Area Network (LAN) Access Point. The LAN Access Point will connect to

¹⁰ A unit key labeled as K_A , is basically a link key which is a 128 bit random number. The unit key is created once at installation of the Bluetooth unit. Thereafter, it is very rarely changed.

the banking services via a wired or wireless LAN. This is a 3-tier configuration: Tier 1 is the mobile device, Tier 2 is the LAN Access Point, and Tier 3 is the banking Services [19, 61].

Based on the three scenarios above, the following Bluetooth security architecture limitations emerge:

- Support for ‘legacy applications’¹¹: In all the scenarios, the legacy application will not communicate with the Bluetooth security manager. There is no security support identified for legacy applications in Bluetooth. Therefore, Bluetooth specific security application must be implemented to set up security procedures with the Bluetooth security manager on behalf of the legacy application. [19, 61, 63]
- It is not the user but only the device that is authenticated. If the user needs to be authenticated, other security features will be necessary [19, 61, 63].
- Scenario 1 defines no mechanism to cater for separate authorisation of each service. A more flexible security policy should be put into practice for this architecture. This can be done by modifying the security manager and the registration processes, without changing the Bluetooth protocol stack [19, 61, 63].
- The approach will only allow access controls when a connection takes place. The access check can be asymmetric, but once a connection takes place, the data will flow bi-directionally. Bluetooth security architecture does not permit one direction flow on the L2CAP channel. Bluetooth security implementations should therefore also cater for options to enforce unidirectional traffic. Such enforcement should occur at the application level [19, 61, 63].

¹¹ When referring to legacy applications and data in information technology, we refer to those that have been inherited from languages, platforms, and techniques earlier than current technology.

- The Bluetooth reference security architecture is based on the Bluetooth baseband security procedure. Hence it only deals with the Bluetooth link security and device authentication. To ensure an end-to-end security as in scenario 3, the security architecture proposes an end-to-end solution. With Bluetooth devices access services such as those in Scenario 3, it is important to ascertain that there is appropriate enforcement of security at both ends of the link [19]. If not, several passwords may be required before the link is complete. This would inevitably increase user frustration [61].

3.6 Summary

A strong security mechanism should be in place for any technology that sends and receives critical data. With the development of wireless technologies, the difficulty of implementing a secure communication link is greatly increased. Bluetooth has become one of a number of 'hot and hyped' technologies of the day [51]. Notwithstanding substantial investment in the Bluetooth security specification, there are still large security holes in Bluetooth security. For example, Bluetooth devices can easily leak sensitive information. Despite the fact that Bluetooth-enabled mobile phones are set with in-built Bluetooth security mechanisms, as explained in this chapter, it has serious security defects. The next chapter elaborates on the current vulnerabilities and intrusions in Bluetooth-enabled mobile phones.

4

Bluetooth Intrusions

Chapter 3 discussed Bluetooth's built-in security, as well as the limitations and vulnerabilities of the built-in security mechanism. This chapter offers an insight into the intrusions occurring in Bluetooth devices. The chapter is organised into two major sections: The first section focuses on the security vulnerabilities, threats and intrusions occurring in Bluetooth devices, especially in mobile phones. The second section addresses the need for an additional Bluetooth security mechanism. The terms 'intruder' and 'attacker' or 'intrusion' and 'attack' act interchangeably throughout this chapter.

4.1 Bluetooth Intrusions

Bluetooth-enabled mobile phones are extensively used by the public and they are definitely making communication easier. Yet these phones are extremely vulnerable to various intrusions [64]. Serious Bluetooth security flaws occurred in the mobile phones of various vendors [14]. The following section covers each Bluetooth security attack in detail, focusing mainly on the attacks occurring in Bluetooth mobile phones.

4.1.1 BlueBug

BlueBug is a Bluetooth security vulnerability found in certain models of Nokia, Sony Ericsson and Motorola phones [65]. Intruders take advantage of this vulnerability and ultimately take control of the mobile phone under intrusion. This security flaw is a serious vulnerability, as it allows intruders to perform the following activities in the affected mobile phone:

▪ **Initiating phone calls**

The BlueBug security vulnerability permits an intruder to initiate phone calls from a vulnerable mobile phone. This means that an intruder can ask a target phone to make a call from that phone to the intruder's phone. The compromised phone can make a call silently to the intruder's phone and once connected to the intruder's phone; it provides a channel for the intruder to listen to conversations on the compromised phone. The intruder can also make calls from the compromised phone [66, 67].

▪ **Sending Short Message Service (SMS) to any number and reading SMS from the phone**

The intruder may manipulate SMSs in the following ways:

- The victim's phone number may be obtained by sending an SMS to the intruder's phone from the victim's phone.
- SMSs may be sent to premium rate numbers via the victim's phone. This will result in a great deal of financial loss to the victim.
- Reading SMSs from the compromised phone will lead the intruder to obtain secret information of the victim.
- By sending SMSs from the victim's phone to the service provider, which offers the location tracking service, the location of the victim may be tracked.

▪ **Reading and writing phonebook entries**

The intruder can manipulate this in the following ways:

- The intruder may analyse the phonebook of the victim to find out the latest missed calls and received calls.
- The phonebook entries may be changed to entries like 'Honey' with an emergency number 100.

- After a list of phone calls have been made from the compromised phone, the list of dialed numbers may be overwritten.

▪ **Setting call forwards**

The intruder may change the call forward numbers on the compromised phone.

▪ **Internet Connection**

An internet connection can be established by using the BlueBug loophole. The illegal injection of mail worms could take place from here.

▪ **Forcing the phone to use a certain service provider**

In busy places such as airports, service providers can make use of the BlueBug loophole to register these phones to their network.

4.1.2 Bluejacking

Bluejacking permits the transfer of business cards (vCards) anonymously to Bluetooth-enabled devices. It takes place without informing the user [68]. Bluejacking is a harmless attack and the purpose of the attack is not to steal or manipulate information, but to make the user react or to ping the phone. The business cards have a clever or flirtatious message in the name field instead of a phone number [69]. The intruders would then send personal or interesting messages to the phone. Bluejacking can only be carried out if the sending and receiving device is within 10 meters. In order to avoid Bluejacking, phone owners should avoid adding an unknown receiver's details to their contacts. By doing so, the intrusion attempt will fail. If a device is set in non-discoverable mode, it will also not be vulnerable to Bluejacking.

Bluejacking originated as a gimmick and the purpose was to simply send anonymous messages to other devices around the neighborhood. Soon marketing companies took on the idea and started using it as an advertising tool. Through Bluejacking, advertisers could set up Bluetooth devices next to advertising hoardings or in shops. It started being a useful medium

to broadcast messages to passers-by. Although Bluejacking seems to be an undamaging attack, there always remains the possibility in advertising that one shop can send messages to tamper the image of other shops. A similar form of intrusion, namely BlueSnarf, is explained next.

4.1.3 BlueSnarf

BlueSnarf is different from Bluejacking, in that it allows data, such as telephone numbers, calendars and diary entries, stored in a vulnerable mobile phone to be stolen by the intruder. For an intruder to execute a BlueSnarf intrusion, the intruder needs to connect first to the OBEX Push Profile (OPP). Bluetooth SIG specifies OPP for the easy exchange of business cards and other objects between Bluetooth devices. Because authentication is not obligatory for the implementation of OBEX service, the majority of Bluetooth mobile devices require sufficient authentication. The BlueSnarf attack connects to an OBEX Push target. It then sends an OBEX GET request for known filenames such as 'telcom/pb.vcf' for the device's phone book [70]. If an improper Bluetooth implementation is present in the device, an intruder would be able to recover all files where the name is either known or guessed correctly.

4.1.4 BlueSnarf++

BlueSnarf++ is a variation of the BlueSnarf intrusion [71]. The primary distinguishing factor is that; in BlueSnarf++ the intruder has full read or write access to the device's file system when connecting to the OBEX Push Profile. Devices that are vulnerable to this intrusion usually have a full-fledged OBEX Push service implemented through an OBEX FTP server rather than a simple server that only supports a subset of the OBEX protocol. This permits the intruder to connect to the device using an OBEX FTP client. The attacker will then issue commands that are used to communicate with a regular FTP server. Through this intrusion, the intruder may browse the full file system of the device, modify the files and also remove them [72].

4.1.5 BlueSmack

BlueSmack is a critical DoS attack and powerful enough to hang Bluetooth-enabled mobile phones with instant effect. The Bluetooth L2CAP layer can request an echo from another Bluetooth peer. This type of attack manipulates the above feature of the L2CAP layer. It also considerably compromises the device.

4.1.6 BlueBump

A BlueBump attack entails pairing with another device for a simple service. Thereafter, the pairing is used to attack other services. To carry out this attack, the attacker would have to get the victim to accept a connection for a trivial data exchange. It could be receiving a business card, calendar entry, or a picture. After the data has been sent, the attacker will still keep the connection open. This will enable the attacker to request a link key regeneration after the victim has deleted the pairing. After a new link key has been produced, the attacker would then have access to the victim's device at any time. The attacker thus would now have full access to any of the services provided by the victim's device [73, 74].

4.1.7 BlueDump

For an attacker to perform the BlueDump attack, the BD_ADDR of a set of paired devices needs to be revealed. The attacker then spoofs one of the device addresses and connects to the other. Since the attacker has no link key, the attacker's device will respond with an 'HCI_Link_Key_Request_Negative_Reply' when the victim's device requests authentication. In some instances this might cause the compromised device to delete its own link key and go into pairing mode [75].

4.1.8 BlueChop

The intention of this attack is to disturb a piconet using a device that is not in the piconet. The attacker spoofs one of the device addresses in the piconet and links it to the master unit disturbing the piconet. This is only possible if the master unit supports more than one connection to a scatternet [76].

4.1.9 HeloMoto

HeloMoto is a vulnerability that is only found in some of the Motorola phones (hence the vulnerability is called HeloMoto). During this attack, the attacker manipulates the incorrect implementation of the trusted device. This is achieved by first connecting to the unauthenticated OBEX Push Profile, pretending to send a vCard. The attacker then begins sending a vCard, but the process is interrupted. By doing this, the attacker's device is stored in the 'list of trusted devices' on the compromised phone. Once the attacker's device is in the list of trusted devices, the attacker can connect to the headset profile without authentication. Hence, this way, the attacker can control the compromised phone [77].

4.1.10 Car Whisperer

The Car Whisperer attack compromises the car-kits, headsets, hands-free devices and other Bluetooth devices inside a car. These devices lack user interfaces to key in passkeys but are equipped with a set of known passkeys that are required during the pairing process. In majority of these cases, the passkey on these devices is '0000' or '1234', so the Car Whisperer can easily guess these passkeys [78]. The attacker can easily connect to these devices from a long distance by using sophisticated antennas and special purpose software programs. Once a connection is established, the attacker can insert audio data into the car. The attacker can also record audio from the car kit or other devices, and may eavesdrop conversations from people sitting in the car.

4.1.11 Warnibbling

Warnibbling refers to a hacking technique similar to the War driving attack. In Warnibbling, the intruder maps the Bluetooth devices in the proximity of the intruding device. The intruder then extracts corporate or personal sensitive information from these devices [88]. According to Mr. Ollie Whitehouse, director of Security Architecture @stake, Inc [88, 89]; Warnibbling can be carried out on a PC which is equipped with the Linux Operating System and a Bluez supported Bluetooth device [90, 91]. Warnibbling was successfully performed by Mr. Ollie Whitehouse using VMWare on an IBM T30 with an additional TDK USB based Bluetooth transceiver [92, 93, 94]. Redfang is an example of popular software used for Warnibbling. Redfang permits intruders to find Bluetooth devices in the area, and permits

intruders to access any data on the compromised device. It is also capable of finding devices in its proximity, even when such devices are in non-discoverable mode [79].

4.1.12 Bluetooth viruses and worms

In addition to the above intrusions, virus writers are finding Bluetooth devices (especially Bluetooth mobile phones) the perfect platform for launching viruses and worms. They take advantage of Bluetooth security vulnerabilities to spread the viruses and worms through Bluetooth. The following sub-sections investigate Bluetooth viruses and worms separately.

4.1.12.1 Cabir

The Cabir worm infects Bluetooth mobile phones based on the Symbian Operating System. This system supports the Series 60 User Interface Platform [80]. This worm emerged on 14th of June 2004. It can only gain access to devices that have Bluetooth and are in discoverable mode [81]. The Cabir worm propagates into mobile phone as an installation file. If the victim installs the file, the mobile phone is infected with the worm. Once a Cabir worm gets into its first mobile phone, it will immediately take control of the Bluetooth functionality of the phone. It will also start looking for other Bluetooth mobile phones. When it finds one, it will replicate itself and tunnel into the new mobile phone, which in turn will begin its own Bluetooth scanning process to replicate to other phones.

The Cabir worm has many variants, which are more dangerous than the original. The most dangerous among them are the Cabir.H and Cabir.I. The Cabir worm is able to spread to only one mobile phone on every reboot, while the variants Cabir.H and Cabir.I can propagate to any number of Bluetooth mobile phones in its proximity [82]. Although these worms do not destroy the data in infected phones, they can block Bluetooth connections to other devices. They can also rapidly drain the phone's battery [83].

4.1.12.2 Mabir.A

The Mabir.A worm is similar to the Cabir worm. It attacks mobile phones on the Symbian Operating System, which supports the Series 60 User Interface Platform. The Mabir.A worm gets into mobile phones through Multimedia Service messages and via Bluetooth. Once this

worm gets into the phone, it will also spread to other phones in the vicinity through Bluetooth. Apart from the above procedure, this worm will capture SMS and MMS messages in the infected phone and send itself to the message senders in reply to original messages [84].

4.1.12.3 Lasco.A

The Lasco.A worm infects only mobile phones on the Symbian Operating System. These phones must support the Series 60 User Interface Platform. The Lasco.A is very similar to Cabir.H and is embedded on the same source code as Cabir.H. The main distinctive feature between Cabir.H and Lasco.A is the infection routine. The Lasco.A worm reaches the mobile phone messaging inbox as an installation file, called `velasco.sis`. When the user clicks the `velasco.sis` and chooses to install the `velasco.sis` file, the worm is activated. It then infects new devices over Bluetooth. In addition, this worm will search for installation files in the device and duplicate itself by infiltrating those files. This worm will spread if the infected files are manually copied to other devices or when it is installed [85].

4.1.12.4 Commwarrior

The Commwarrior is a worm that is quite similar to the Cabir, Mibir.A and Lasco.A worms. It can only infect mobile phones that are based on the Symbian Operating System and are running the Series 60 User Interface Platform. This worm spreads through Bluetooth, MMS or by an infected memory card inserted into a device. When the worm gets in the phone, it reads the address book and then sends itself as an MMS message to the addresses obtained, thereby also spreading to other phones. The installation files that Commwarrior sends each time are randomly named. As a result, users cannot be warned to avoid installation files with any particular name [86].

The Commwarrior worm has some variants, which are slightly more advanced than the original worm. Among these is Commwarrior.Q, which is by far the most popular and dangerous. When it gets into a phone, Commwarrior.Q sends MMS messages from midnight to 7 am to all the numbers in the infected phone's contact list. It uses a sent message to be part of the MMS, so that the MMS looks genuine. However, Commwarrior.Q stops infection

after 7am, as it becomes noticeable to the user [87]. It then begins scanning other phones to infect via Bluetooth. Even though this worm does not damage the phone's data, it is classified as highly dangerous, mainly because it can cause high phone charges by sending off multiple messages.

The next section motivates the need for an additional Bluetooth security mechanism to safeguard devices from the existing vulnerabilities.

4.2 The need for an additional Bluetooth Security mechanism

The users of the Bluetooth devices realise the security issues of Bluetooth only when they fall victim to an attack. Bluetooth-enabled cars have become very popular now; if a car's on-board computer is compromised, this could put the lives of passengers and the driver at risk. Similarly, insecure mobile devices enable anomalous code to spread extremely quickly via Bluetooth. Nevertheless, some of the intrusions that were discussed in the previous sections can be avoided by either switching off the Bluetooth functionality in the device, or by keeping the device in non-discoverable mode. This solution is unappealing since it prevents devices from using Bluetooth for legitimate applications. As a result, there is a need for a permanent solution to improve Bluetooth Security. Devices should be equipped with an additional Bluetooth security mechanism, which would be capable of defending against possible intrusions and safeguarding devices against existing Bluetooth security vulnerabilities.

4.3 Summary

This chapter presented wireless security vulnerabilities in general, Bluetooth security vulnerabilities and Bluetooth intrusions. From Section 4.2, it has become clear that Bluetooth faces a number of security issues in the form of intrusions and viruses. A serious problem in Bluetooth which has no defense is the DoS attacks. Although Bluetooth SIG is finding solutions to this problem, the initial design to develop Bluetooth may make this a difficult problem to defend against. One can conclude here by saying that Bluetooth in its current

state is incompatible for the transfer of sensitive data. There needs to be an additional Bluetooth security mechanism to guard against existing vulnerabilities and intrusions. The next chapter proposes a solution to improve the existing Bluetooth security mechanisms.

5

Existing Bluetooth security solutions

With the popularity and advancement of the wireless technology, mobile phones are becoming more connected and subsequently more exposed to intrusions on a daily basis. Mobile devices form part of a large wireless network that links together millions of wireless devices. Considering the growth in Bluetooth-enabled mobile phone adoption in enterprises as part of the workforce, there are mobile commerce initiatives emerging from the financial services industries, as mobile computing power increases. There are also faster 3G mobile download speeds and a much wider availability of mobile phones. At the same time, there is also a rapid increase in serious security intrusions, viruses and malwares.

Bluetooth mobile phones are becoming more business-enabled and have been widely used by the public network. Because of the wireless nature of these phones, it will become easy for intruders to cause intrusions and for viruses to spread.

Bluetooth enabled devices are becoming the next generation Internet security threat because of the broad number of unprotected, mobile phones. This scenario is becoming more of a reality each day, with the addition of each new vulnerable Bluetooth enabled device. As the mobile channel continues its phenomenal growth, complexities of security such as identity theft, consumer privacy and fraud are also increasing rapidly.

The mass adoption of wireless technology is losing speed because of security concerns and Bluetooth is no exception. Because of its development and use, it is critical to resolve

Bluetooth security issues and Bluetooth is still inadequate for the transfer of high-security data. The number of intrusions and the extent of data loss clearly demonstrate the need for improved security [95]. Even though mobile phones are equipped with Bluetooth's built-in security mechanisms, various critical security vulnerabilities exist in the majority of mobile phones. For this reason, these phones are easily compromised. Consequently, there is loss of precious information, resources, time and financial loss, to name only a few. This fact confirms the high need and the significance of Bluetooth security.

Intrusion risks may be reduced to a certain extent if proper security policies are implemented in mobile phones. In spite of that, it is not always possible to stick to security policies consistently. This is due to the lack of basic security awareness and an understanding of Bluetooth technology among mobile phone users [9, 96, 97]. Therefore, there is a need for an additional security mechanism to tackle the Bluetooth security vulnerabilities and to keep the Bluetooth communication safe. This chapter firstly explains the existing Bluetooth security solutions to avoid intrusions in mobile phones. Secondly, it discusses the proposed solution.

5.1 Existing Bluetooth Security Solutions

This section focuses on Bluetooth security products to enhance the security in Bluetooth-enabled devices. These products are explained in detail below.

5.1.1 AirDefense BlueWatch™

AirDefense BlueWatch™ is a security solution which monitors and identifies all Bluetooth enabled devices and the communication between them within a specified range. This product is ideal to be set up in organisations to detect the Bluetooth related security threats. In addition, it can take up a proactive approach in the prevention of intrusion into a network. AirDefense BlueWatch also detects Bluetooth devices with no authentication or encryption. It furthermore also takes steps to close any security loop holes that may cause any security breaches. It runs only on PCs and PDAs installed with Windows 2000, XP or Windows CE

and a Bluetooth adapter [98]. The next section explains another Bluetooth Intrusion Detection System (IDS) known as Red-Detect.

5.1.2 Red-Detect™

Red-Detect is an enterprise class wireless and Bluetooth intrusion detection and prevention tool from Red-M wireless security solutions. It secures the wireless network and checks whether an intrusion attempt has occurred in the network. If so, it takes counter measures. Red-Detect comprises of the following three components: a group of Red-Alert PRO probes, a central server and a Windows management console [99]. The Red-Alert PRO probes capture all the wireless events on a 24X7 basis. It then stores the data in a central server. The central server then compares the captured data to its internal knowledge base to correlate intrusions. The purpose of the Windows management console is to present an interface to manage all the aspects of the wireless traffic in the network. Since Red-Detect take care of the security in a full wireless network, its usage is ideal for companies that use wireless networks. It also works effectively in companies that are moving from wired to wireless communications [100].

5.1.3 BlueAuditor

BlueAuditor is a network-auditing tool used to detect and monitor Bluetooth devices in a wireless network. It detects, monitors and displays key information of any device within a distance of 100 meters. BlueAuditor also permits network administrators to review their wireless networks against security vulnerabilities associated with the use of Bluetooth devices. BlueAuditor runs only on PCs or laptops installed with Windows 2000, Windows XP Service Pack2, Windows Server 2003 or Windows Vista and a Windows XP-compatible Bluetooth adapter. BlueAuditor runs only on top of Microsoft Windows supported Bluetooth drivers [101].

5.1.4 AirMagnet BlueSweep™

The AirMagnet BlueSweep is a Bluetooth security tool which is very analogous to AirDefence BlueWatch and BlueAuditor. This is a simple, user-friendly, Windows-based

utility that can detect and monitor Bluetooth devices in a wireless network environment, within a range of 100 meters. It enables network administrators to effortlessly discover and track Bluetooth devices that are active in the network. This then authorises them to act proactively to guard their network against potential vulnerabilities posed by those Bluetooth devices. Network administrators are thus also enabled to quickly and easily find the service or services that any detected Bluetooth device is providing or is able to provide. From this they will know exactly what is going on in the airspace over the network. At the moment, the AirMagnet BlueSweep can only be deployed on PCs or laptops installed with Windows XP Service Pack2 and a Windows XP-compatible Bluetooth adapter. It runs only on top of Microsoft Windows supported Bluetooth drivers [102].

The next section sets out issues with the above security solutions and puts forward a new Bluetooth security solution.

5.2 Proposed Bluetooth Security Solution

The previous section discussed the existing Bluetooth IDSs used to improve the security in Bluetooth devices. These IDSs mainly focus on detecting devices within a certain range. They demand extensive human intervention in order to find out what intrusions are occurring in the network (using the data captured from the user interface). The intrusions are only be detected once they have occurred.

All the IDSs are available either as a complete hardware or software solution or as a software only solution. IDSs such as Red-Detect (www.red-m.com) and AirDefense (www.airdefense.net) are very expensive and lack critical configuration abilities. Hence, they fail to present important alerts to administrators [100]. Even though they provide greater technical support along with a more user-friendly interface for configuration, monitoring, and reporting, one of the biggest disadvantages of these IDSs is their inability to change the antenna [103]. Instead of just changing to a higher gain antenna, there is always the need to buy more sensors to get more coverage. This can result in an increase in the cost of equipment, as well as an increase in the time needed to setup and maintain additional devices.

Existing security solutions are only suitable to monitor and detect vulnerabilities that take place in a full Bluetooth network. They are not capable of detecting intrusions that are targeted towards a particular device. In other words, these security solutions are only network based intrusion detection systems. The biggest shortcoming is that none of the existing Bluetooth IDSs can be deployed in mobile phones as they can only be used in PCs or laptops.

A large number of mobile phones from different mobile phone vendors on the market are having one or another Bluetooth security limitation. [14, 104, 105]. Even though vendors are aware of these issues, they are not considering it as critical. As a result, patches or fixes for security issues are not made available regularly. Until recently, the intrusions in mobile phones have been proof-of-concept attacks, restricted by weak transmission methods and a reserved target device population. However, according to Bob Egan, chief analyst at TowerGroup, mobile phones will gradually become the target of fraud and identity theft [106]. Some of the security issues may be corrected by installing the latest firmware released by mobile phone vendors. However, majority of mobile phone owners do not upgrade firmware from time to time. An upgrade in the firmware is inherently a complicated process in some of the mobile phone models. The majority of mobile phone users also do not have sufficient knowledge to upgrade firmware [107].

Even though numerous file scanners and malware blockers are available on the market for use in mobile phones; they are not particularly suitable for detecting the Bluetooth intrusions at the precise moment when an intrusion attempt takes place. Examples of those on the market include Trend Micro Mobile Security [108], Symantec Mobile Security [109], F-Secure Mobile Security™ [110], McAfee Mobile Security [111], Gold Lock™ [112] and Sophos Mobile Security™ [113]. Many intrusions in mobile phones occur without the user's knowledge during the establishment of Bluetooth connections. Present mobile phones do not have a solution for users to identify intruders or intrusions that occur while a Bluetooth connection takes place from a remote device. Existing Bluetooth IDSs are also not addressing this concept. If a mobile user is able to identify an anomalous connection that is taking place, then the user can be safe from many of these attacks. The importance of

alerting the user of incoming connections is hereby underlined. The proposed solution revolves around this concept.

The proposed solution to detect intrusion in Bluetooth-enabled mobile phones is to incorporate a Bluetooth Logging Agent (BLA) in mobile phones. The BLA is efficient and unique since it keeps track of all Bluetooth activities in the mobile phone. The BLA will identify and alert the user of any intrusion and make it easy for the user to identify any intrusion or unidentifiable Bluetooth connections.

5.3 Summary

As the prevalent use and recognition of Bluetooth continues, there are concerns of security vulnerabilities and privacy issues inherent in the use of this technology, especially in the mobile phone spectrum. Inadequate device resources and lack of user awareness has complicated this issue where the emphasis on design constraints, functionality and ease of use sometimes overshadow security concerns. This chapter discussed the existing Bluetooth IDSs. Although there are some Bluetooth IDSs, the field is still only developing and so are the products. Many products mainly concentrate on finding devices within a specific range and detecting where they communicate. As mentioned above, this brings about an increased cost in equipment and an increase in the time to setup and maintain additional devices. The proposed solution is simple, cost effective and will be highly useful, since it provides mobile phone users with the capacity to protect their phones. The following chapter discusses the proposed solution in detail.

6

Bluetooth Logging Agent (BLA)

Bluetooth is an open specification for short-range wireless ad-hoc communication. As an inter connective and new technology, Bluetooth faces traditional security problems, well known from the distributed networks. Bluetooth however has to cope with these issues on a new level because security issues in ad-hoc networks are much more complex, compared to traditional distributed networks. Moreover, Bluetooth networks are formed by radio links, which suggest that additional security aspects have to be considered when implementing Bluetooth applications.

The focus of this research is on suggesting ways to improve Bluetooth security in mobile phones. This chapter puts forward the Bluetooth Logging Agent (BLA) model as a way to improve the effectiveness of Bluetooth security in mobile phones. The information is organised into three sections. The first section explains the overall BLA development process, the second section explains the proposed design created for the BLA, individual modules of BLA and inter-communication between each module. The last section covers the communication between the BLA and the embedded Bluetooth module in mobile phones.

6.1 BLA Development Process

The BLA development process is organized as according to the BLA architecture illustrated in section 6.2. The core logic of BLA lies in the Intrusion Detection and Verification Module (IDVM) and Logging Modue (LM). The IDVM was first designed and developed, which involved the identification and development of Connection and Disconnection Module

(CDM), Authentication Module (AM) and Service Module (SM). These modules were then interfaced through the appropriate request and response mechanisms. The LM was developed further to monitor and trace the Bluetooth activities happening in the mobile phone. The BLA Database module was then designed and developed to store and filter the Bluetooth activities and to facilitate the intrusion detection of BLA. The Mobile Phone User Interface (MPUI) module was further incorporated and populated with the BLA user interface to facilitate the communication between the mobile phone user and BLA.

The IDVM, the LM, the BLA Database and the MPUI were then integrated and interfaced with the appropriate request and response mechanisms to develop the final BLA. Each of the modules in the BLA Architecture is analysed in detail in the sections that follow.

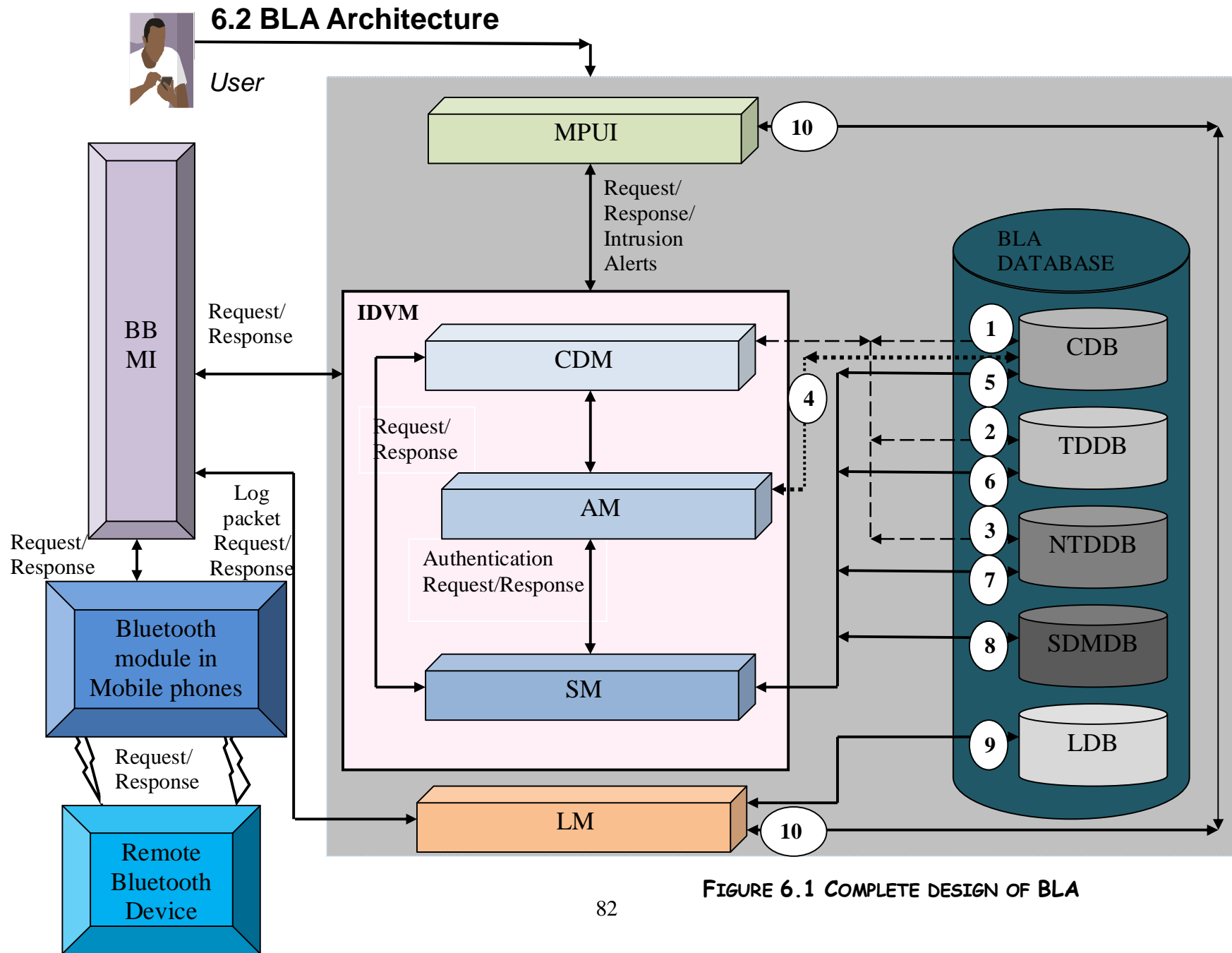


FIGURE 6.1 COMPLETE DESIGN OF BLA

The numbers in the circles in Figure 6.1 represent the message exchanges between the different modules. The number to message mapping is as follows:

1. Update CDB
2. CDM /TDDB handshakes; Database update requests and responses
3. CDM/NTDDB handshakes; Database update requests and responses
4. AM/CDB handshakes; Database update requests and responses
5. SM /CDB handshakes; Database update requests and responses
6. SM/TDDB handshakes; Database update requests and responses
7. SM/NTDDB handshake; Database update requests and responses
8. SM/SDMDB handshakes; Database update requests and responses
9. LM/LDB handshakes; Database update requests and responses
10. Communication between the MPUI and LM

The core functionalities that the BLA is intended to perform are as follows:

1. The BLA should work closely and communicate with the mobile phone's embedded Bluetooth module's stack and profiles like OBEX Profile, Serial Port Profile, Hands Free Profile and Headset Profile. The Bluetooth Module will indicate to the BLA what Bluetooth activities are occurring in the mobile phone. The principal Bluetooth module should distinguish the requests from BLA.
2. The BLA will be presented with a preset of trusted devices and their particular parameters, such as the device name and the Bluetooth Device Address. The BLA should only permit a connection from its pool of trusted devices after it has obtained permission from the user. When an incoming request is arriving in the mobile phone from a remote Bluetooth device, the BLA should authenticate the authenticity of the connection with the required parameter checks and via looking up the database. Parameter checks are carried out by subsequent handshakes with the remote device.

3. The BLA should cater for remote Bluetooth device connections, which are not in the trusted device list. These connections should be restrictive, and the mobile phone user should have the freedom to accept or reject such connections, upon further handshakes with the remote device.

4. The user should be able to stipulate access rights to mobile phone's services in BLA. If the remote device attempts to access a service which is not allowed, the BLA will alert the user. The Bluetooth connection with that device will then be terminated. The BLA should also signal the user to turn off Bluetooth on the instant that it picks up an unauthorised operation.

5. The BLA should only accept Personal Identification Number (PIN codes) with lengths that are greater than or equal to 8. For the duration of the authentication step, the BLA should not accept any connection from a Bluetooth device that does not meet this condition.

6. Upon request from the user, the BLA should provide the feature of logging all Bluetooth activities.

As represented in the complete design of the BLA in Figure 6.2; the BLA consists of various modules, where each module fulfills a specific role in the intrusion detection. The following sub-sections explain the purpose of each module.

6.2.1 Bluetooth Module in Mobile phones

The Bluetooth Module in Mobile phones is represented in Figure 6.3. As shown in the figure, the Bluetooth module consists of the Bluetooth Hardware, Bluetooth protocol stack, Bluetooth profiles and Bluetooth applications. The Bluetooth module is the core module that handles the Bluetooth activities happening in the device. This is the module that sends and receives the Bluetooth messages with other Bluetooth devices in its proximity. It communicates with the 'BLA - Bluetooth Module Interface' (BBMI) to deal with the requests from BLA and to alert BBMI with any message from the remote Bluetooth device.

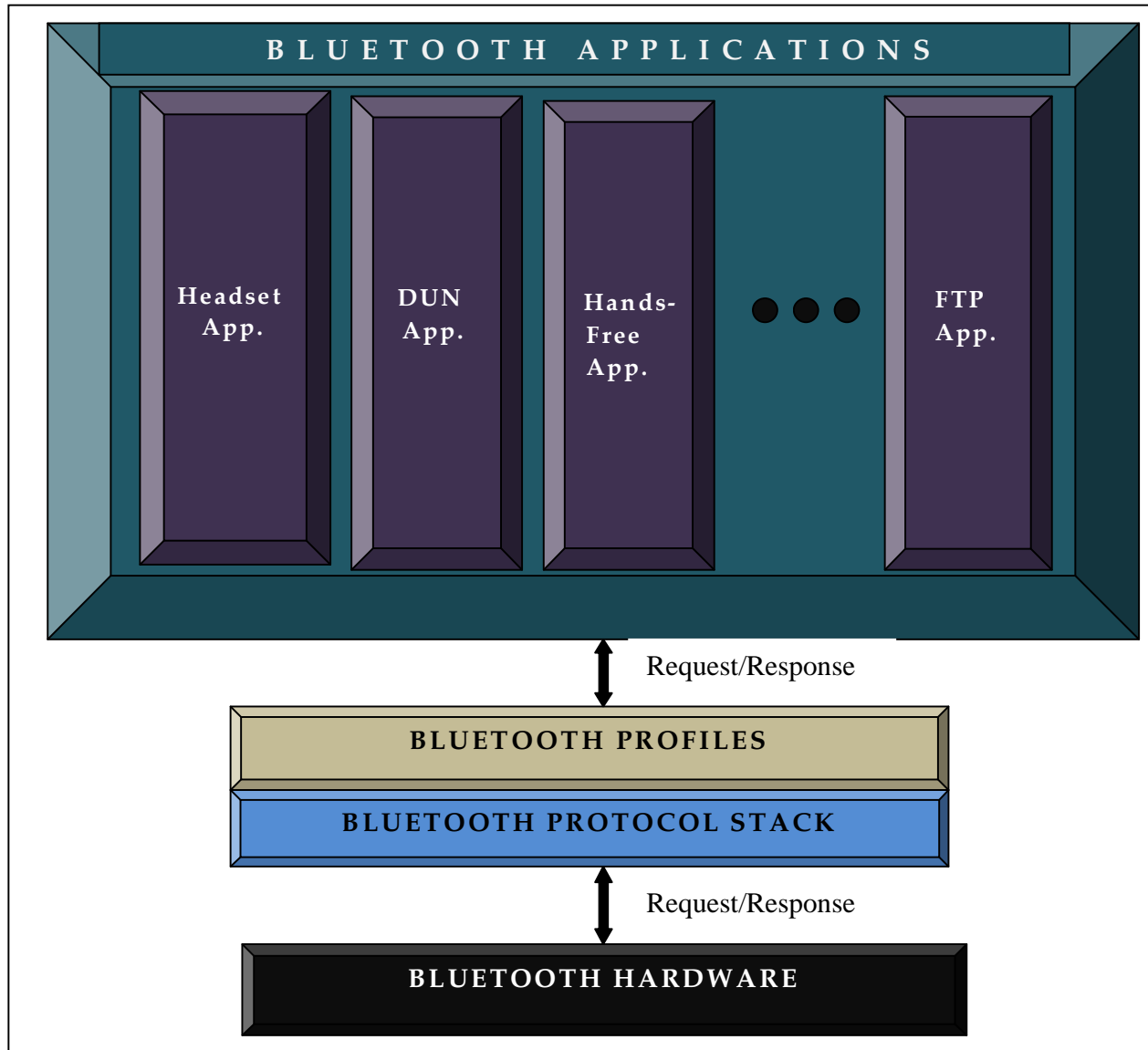


FIGURE 6.2 BLUETOOTH MODULE

6.2.2 BLA - Bluetooth Module Interface (BBMI)

The BBMI is responsible for the communication between the BLA and the embedded Bluetooth Module in the mobile device. Section 6.3 further explains this module.

6.2.3 Intrusion Detection and Verification Module (IDVM)

The IDVM is the core module of the BLA. It sends and processes the messages to and from the BBMI, mobile phone user interface (MPUI) and BLA Database. It consists of three sub-modules, which the following sub-sections discuss in detail.

6.2.3.1 Connection and Disconnection Module (CDM)

As the name implies, this module is responsible for the connection and disconnection of Bluetooth connection. When BLA gets a connection request indication, the request is sent to the CDM. At this stage, it becomes the responsibility of the CDM to check if the request is genuine or an intrusion attempt. The CDM performs various steps to see if the request is from a reliable source or if it is an intrusion attempt.

As the first step, CDM checks the Trusted Devices Database (TDDB) to determine whether the device that is attempting to connect is listed in the database. If the device is indeed listed, the CDM will assume that the remote device can be trusted. From there it will then perform further security checks to affirm that the remote device is from a valid source. If the connection request is genuine, the connection response will be sent and the new connection will be added to the Connection Data Base (CDB).

If the device that is attempting to connect is not listed in the TDDB, then CDM will check the Non Trusted Devices Database (NTDDB). If the device is listed in the NTDDB, then the CDM will classify this as an intrusion. An alert will then be sent to the MPUI. The CDM will furthermore send a disconnect response to BBMI. If a device is neither in the TDDB nor in the NTDDB, then the process becomes a bit more complicated. The CDM in such situations will have to determine

whether the connection is from a valid source or whether it is an intrusion attempt.

Under such circumstances, the CDM follows certain predefined rules. The list of valid rules includes the following:

1. 'Accept connections from mobile phones only from a list of models of a particular manufacturer'. Models excluded from the list have some Bluetooth security vulnerability and for this reason, BLA assumes that it is unsafe to accept connections from those devices.
2. If the connect request originates not from a mobile phone but from another class of devices (for example a laptop or PC), it is vital to ensure that the Bluetooth Device Address (BD_ADDRESS) falls within the trusted range of BD_ADDRESS's (marked by the BLA). The BLA can, for example, choose to accept connect requests only if the BD_ADDRESS is within the range of 00:AA:10:EE:21:01 to 00:AA:10:EE:21:0F.

On subsequent handshakes with the remote device, the CDM collects the information and correlates against the rules. If CDM at any stage finds that the request from the remote device does not match the rules, CDM will then mark it as an intrusion and alert this to the MPUI. The CDM will update the NTDDDB with the newly marked device.

In the event that CDM finds that the remote device is from a valid source, the connection is accepted and a connection response will be sent. The CDM then updates the CDB to reflect the new connection; and the new remote device is also added to the TDDDB. Figure 6.3 represents the flow of information through CDM.

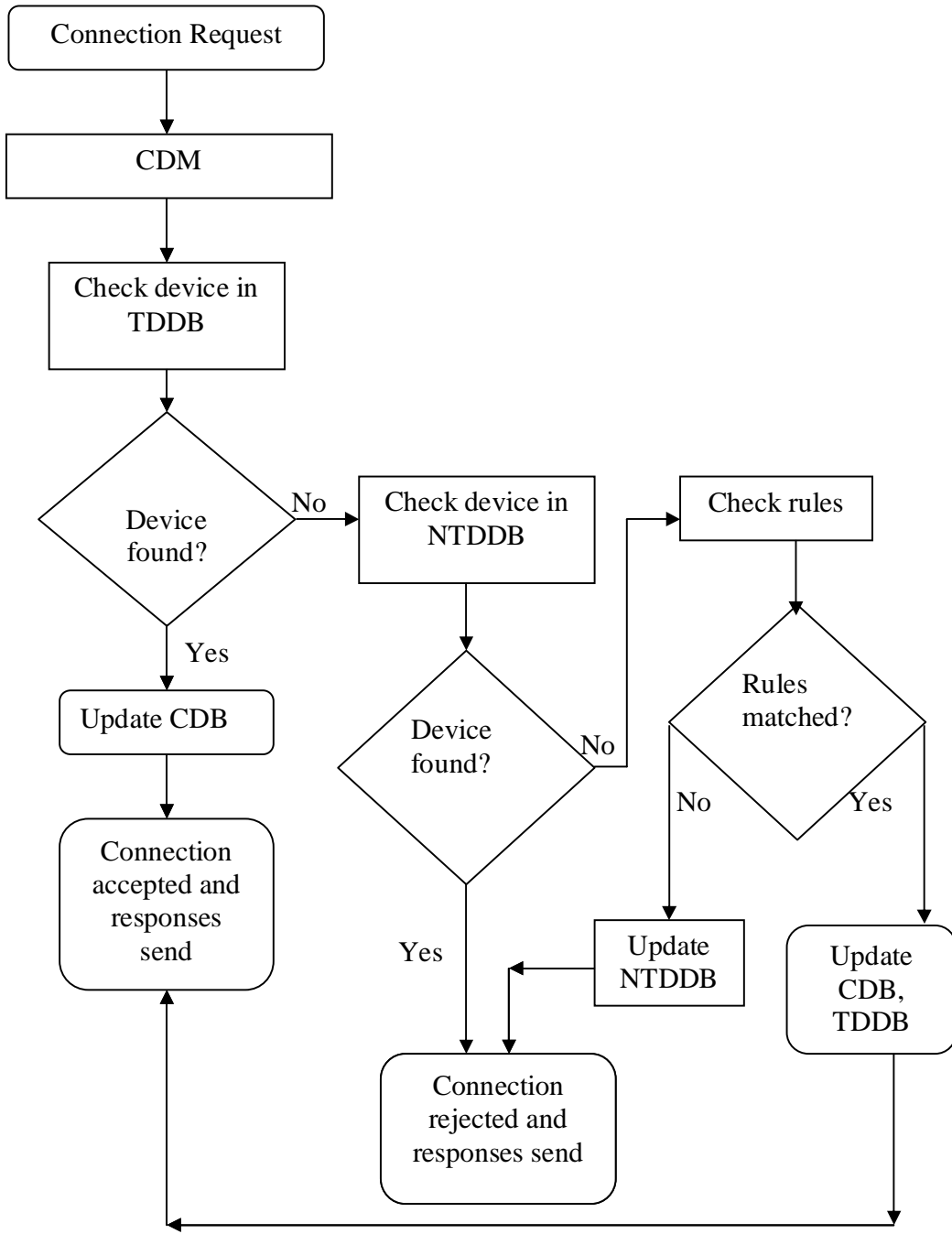


FIGURE 6.3 THE FLOW OF INFORMATION THROUGH CDM

6.2.3.2 Authentication Module (AM)

The Authentication Module (AM) handles the authenticity of the requests received by the Service Module (SM). The AM authenticates the request only if the device is already in the CDB and on condition that the PIN code length in the request is at least 8. If the device is not in CDB, AM classifies the received request as an intrusion attempt which possibly gained access through an anomalous Bluetooth connection. The MPUI is then alerted and an authentication-failed response is sent to SM. As explained in the earlier chapters, PIN codes of which the length is less than eight are classified as a security threat. The reason for this is that special algorithms can easily crack PIN codes with a short length [53, 96]. If the device is found in CDB and the PIN code length in the request is less than eight, the AM informs the SM that the authentication has failed. The AM then classifies the received request as an intrusion attempt and the MPUI is alerted of this. The NTDDB is subsequently updated with the remote device if it is not already in the database. The AM also checks the TDDB and if the device is listed, it is removed from the database. The disconnect request is then sent to the CDM to close the Bluetooth connection. The CDB is updated.

Figure 6.4 represents the flow of information through AM.

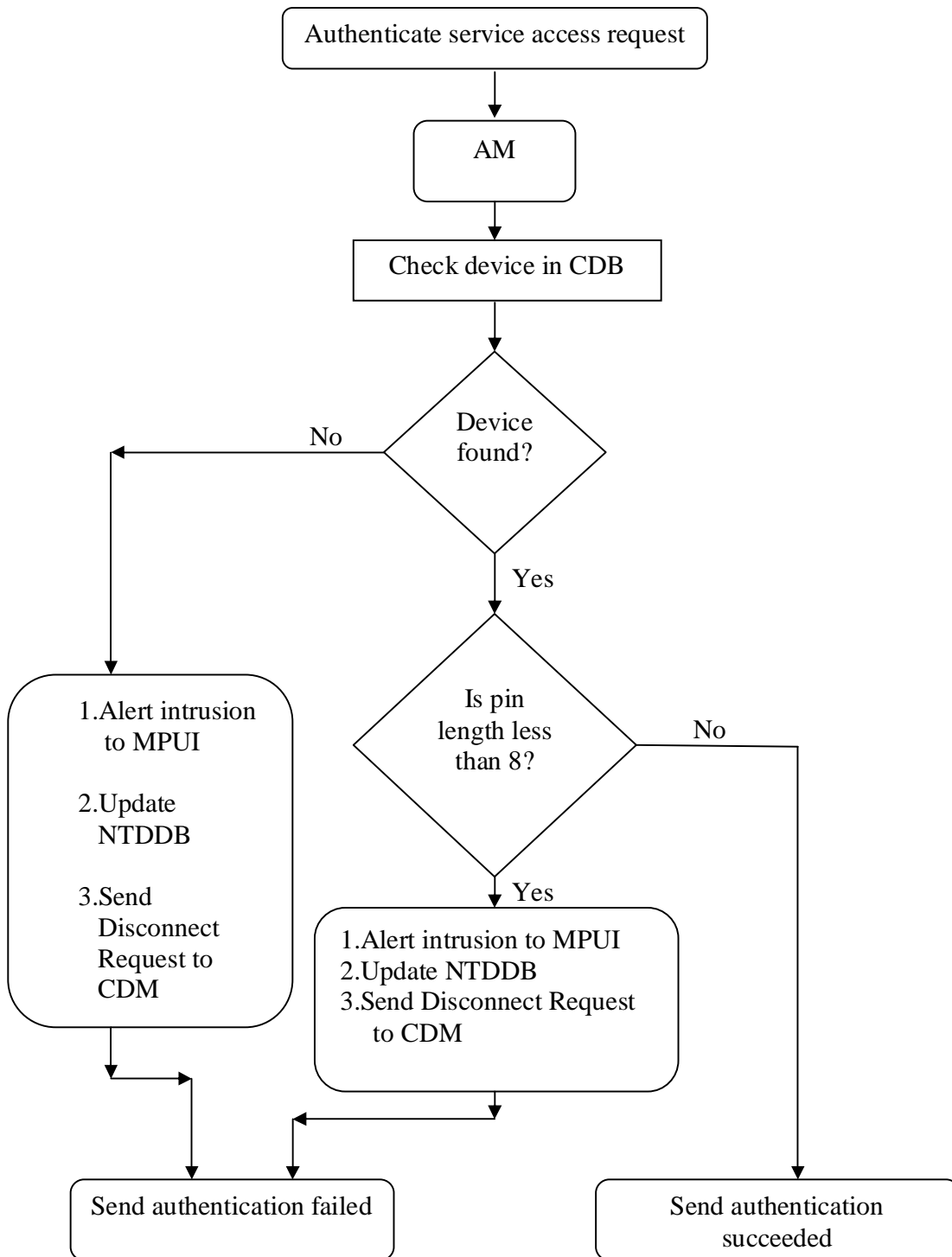


FIGURE 6.4 THE FLOW OF INFORMATION THROUGH AM

6.2.3.3 Service Module (SM)

The Service Module is in command of offering controlled access to the Bluetooth applications or services offered by the mobile phone to other devices. It does this by using the AM and the Services and Device Mapping database (SDMDB). When SM receives a service request; for example if remote device A sends a request to access the Internet through our current device (our current device in this case will act as a modem using the Bluetooth 'Dial Up Networking' application), the SM will trigger the AM to check the authenticity of the request. If the authentication fails, AM will take further action and an authentication failure status will be sent to SM.

If AM returns a successful authentication status, SM will check the SDMDB to see if device A is allowed to use the Internet Service. If it is listed, a positive response will be sent and device A will be granted permission to use the Internet service. If the device is not listed in the SDMDB, then SM will mark it as an intrusion attempt and the MPUI will be alerted. The NTDDB will be updated with the remote device and the disconnect request will be sent to the CDM to close the Bluetooth connection. In such a case, the remote device will also be removed from the CDDB and TDDB. The SM will send a positive or negative response to the BBMI, depending on the success or failure of the service access request.

Figure 6.5 represents the flow of information through SM.

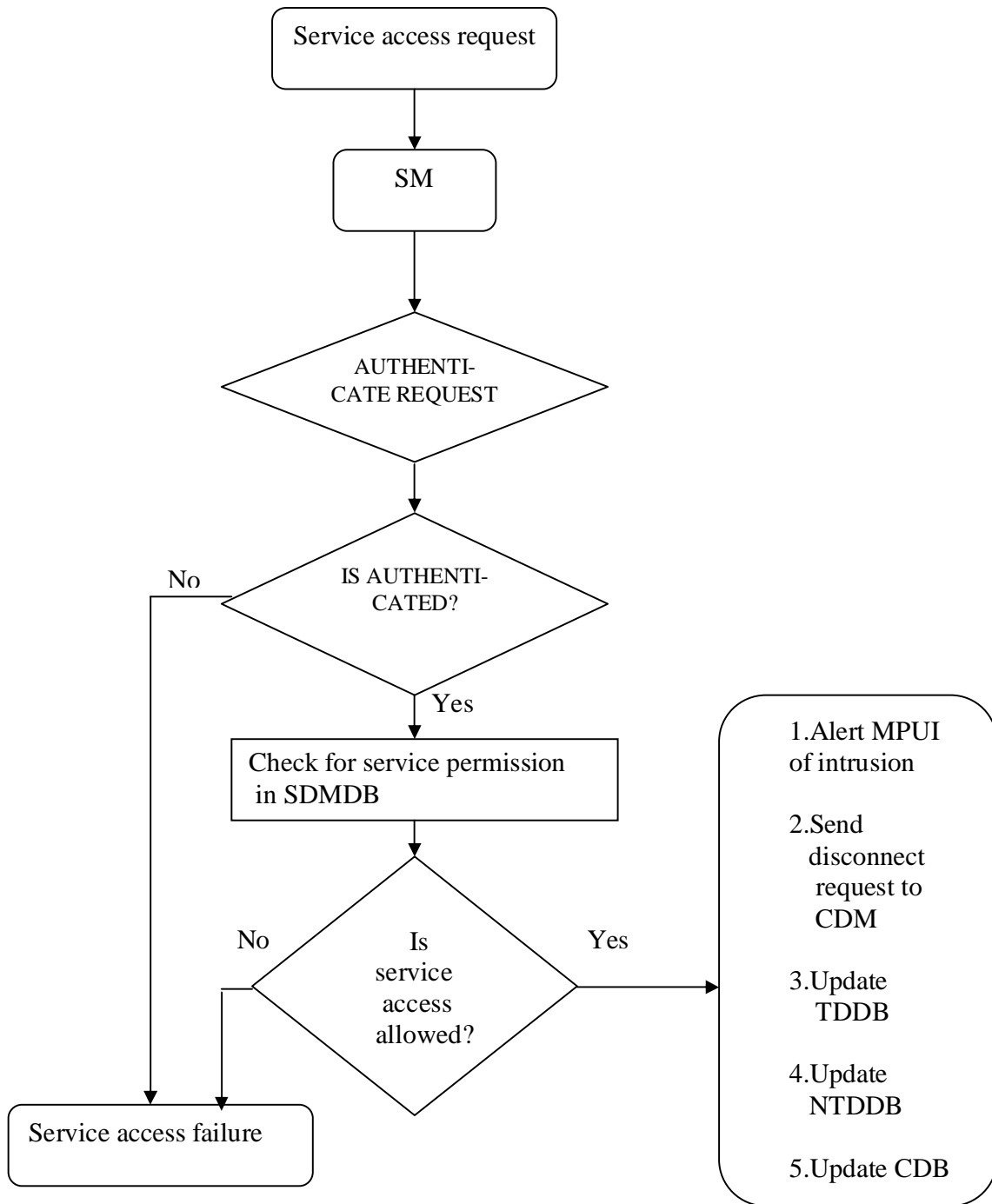


FIGURE 6.5 THE FLOW OF INFORMATION THROUGH SM

6.2.4 Logging Module (LM)

The LM is in command of logging all Bluetooth activities occurring in the device, upon request from the user. The user, if suspicious of any Bluetooth session, sends a request to the LM through the MPUI. When the LM receives the Log Packet Request, it transfers this request to the BBMI and then all transactions in that particular Bluetooth session is logged.

The LM updates the Logging Database (LDB) with the log file attained in the requested Bluetooth session. The LDB is very useful for storing and retrieving logs of sessions that are of suspicious nature to the user. Logged files can thus be used as references for tracing all Bluetooth activities that occurred in the respective Bluetooth sessions.

All logged files in the LDB share some common information apart from the message exchanges in that session. This includes the time in which the session started, the time in which the session ended and the Bluetooth connections active in that session. Figure 6.6 represents the flow of information through LM.

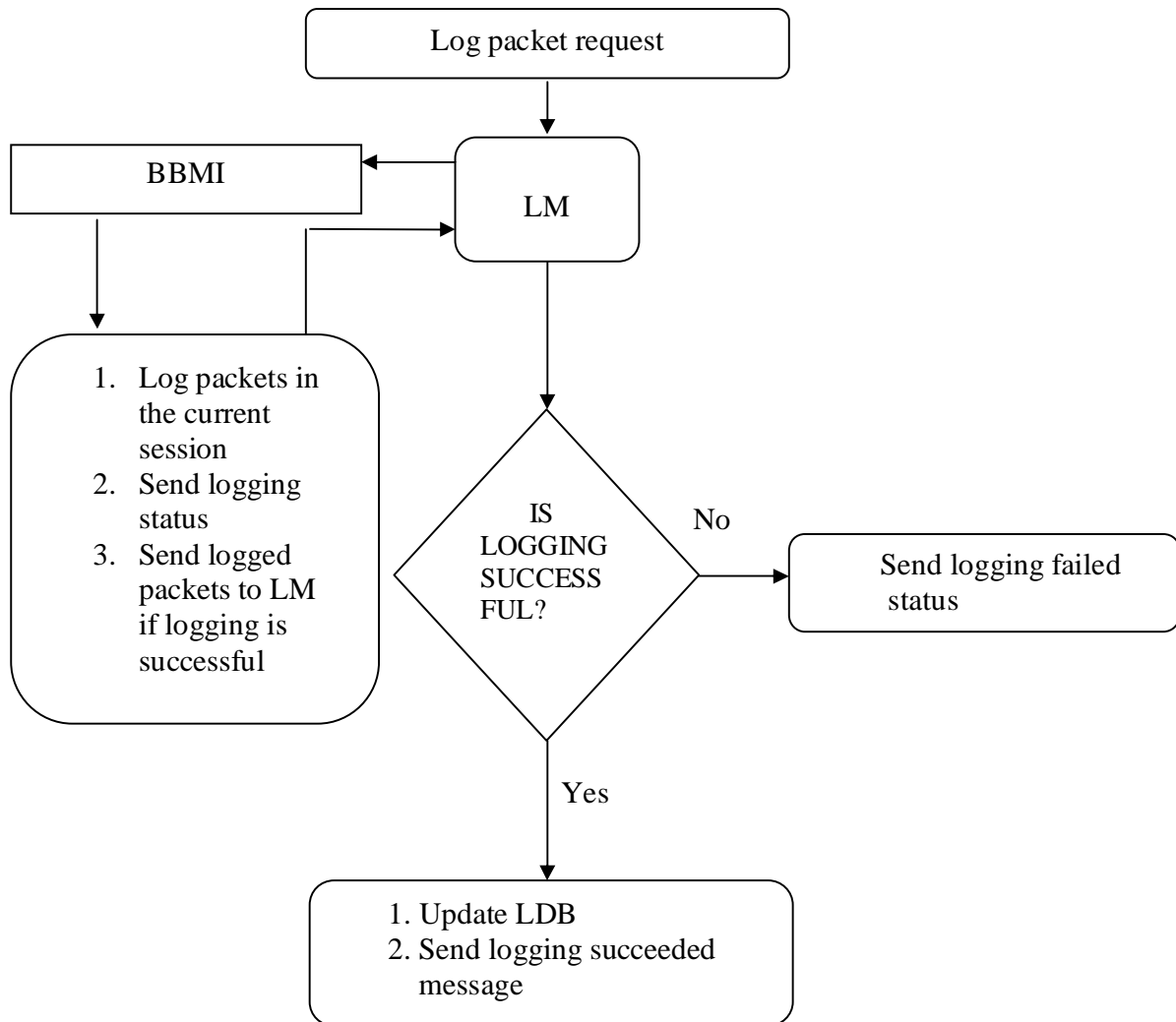


FIGURE 6.6 THE FLOW OF INFORMATION THROUGH LM

6.2.5 BLA database

The BLA database consists of five databases, which store key information about other Bluetooth devices that have either communicated with BLA, or are classified by BLA because of certain criteria.

6.2.5.1 Connection Database (CDB)

The BLA logs the `BD_ADDRESS` of the devices that have obtained a Bluetooth connection with BLA in CDB. The CDB maintains a list of currently active Bluetooth connections with BLA.

6.2.5.2 Trusted Devices Database (TDDB)

As the name implies, the TDDB is the storage base of a list of devices trusted by BLA. The `BD_ADDRESS` of the trusted devices are stored in this database. The BLA only accepts connections from a remote Bluetooth device if such a device is listed in the TDDB Database.

6.2.5.3 Non trusted Devices Database (NTDDB)

The BLA also stores the `BD_ADDRESS` of devices in NTDDB that have attempted intrusion or devices that are of suspicious nature to BLA and are blacklisted by the IDVM. The BLA will not accept a connection from a remote Bluetooth device if it is listed in the NTDDB.

6.2.5.4 Services and Devices Mapping Database (SDMDB)

The BLA stores the device to application mapping information in SDMDB. In SDMDB, the BLA stores information that is accessible to all trusted devices (services or applications) in the mobile phone.

6.2.5.5 Logging Database (LDB)

All communication message exchanges between BLA and remote Bluetooth devices are stored in the LDB. The messages are logged in LDB between the start time and end time of the communication session.

6.2.6 Mobile Phone User Interface (MPUI)

MPUI is the module that directly interacts with the mobile phone user. On receiving the intrusion detection alert from IDVM, this module immediately alerts the user so that the user can power off Bluetooth through the mobile phone UI. The MPUI exchanges requests and responses with IDVM and LM and is responsible for sending user inputs to these modules. The MPUI should facilitate the following functions:

1. 'Start BLA': As the name suggests, when the user selects this option, the BLA is started.
2. 'Accept Request': This option is to acknowledge requests. The requests may include requests of connection, service or application access.
3. 'Discard Request': This option enables the user to decline a request.
4. 'Log Packet': This option in the MPUI is to enable transaction logging.
5. 'Stop BLA': As the name suggests, the BLA stops when the user selects this option.
6. 'Power off Bluetooth': This option enables the user to turn Bluetooth off directly from MPUI. This is to safeguard the device against intrusions, when IDVM detects an intrusion.

6.3 BLA and Bluetooth Module Interface

The following figure represents the communication between BLA and the Bluetooth Module.

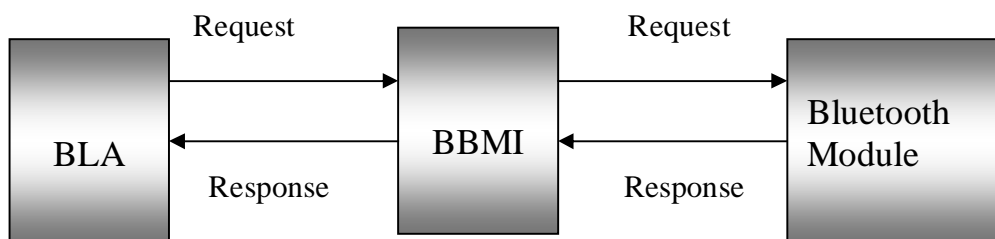


FIGURE 6.7 COMMUNICATION BETWEEN BLA AND BLUETOOTH MODULE

As depicted in Figure 6.7, the BBMI controls the communication between BLA and Bluetooth Module. BBMI sends and receives a series of messages before it successfully interfaces with the

Bluetooth Module. For example, when the user selects 'Start BLA' from MPUI, a 'Start Request' will be sent to the BBMI. On receiving this request, the BBMI will start the process of interfacing with the Bluetooth Module.

The BBMI will first send a request to power on the Bluetooth Module. If the Bluetooth Module is on, a positive response will be sent, otherwise a negative response will be sent to BBMI. The BBMI will proceed to the second step only if the first step is successful. On the second step, BBMI will register with the Bluetooth Module to send and receive the messages and to receive notifications. If everything goes well in the first and second step, BLA will receive a positive response from BBMI. If not, BLA will receive a negative response. Depending on the message from BBMI, the BLA will then inform the user that the BLA has started or has 'failed to start'. The BBMI takes actions based on the indications from BLA and the Bluetooth Module. The core functionality of the BBMI is to convert the message received from BLA to a format that is understandable to the Bluetooth Module and vice versa.

6.4 Summary

The BLA model shows potential to detect intrusions by enhancing the Bluetooth Security in Bluetooth mobile phones. This chapter gave a detailed overview of the design of the BLA model, the communication and interfacing between the various modules of BLA, and the flow of information through each module. This chapter was thus an attempt to produce an efficient design of BLA to remove vulnerabilities through which Bluetooth Security is compromised. The next chapter discusses the prototype that was developed on the design proposed in this chapter.



BLA Prototype Implementation

The last chapter discussed a prototype for the proposed BLA design. The purpose of this prototype is to establish that the BLA will enhance the built-in Bluetooth Security mechanism. The purpose in particular is to establish that the BLA, if deployed in mobile phones, will rectify the existing Bluetooth Security vulnerabilities and safeguard the mobile phone against Bluetooth intrusions.

7.1 Prototype Components, Assumptions

The research prototype consists of two components, namely the Bluetooth Logging Agent (BLA) and the Bluetooth Intrusion Simulator (BIS). The BLA is the component which detects the intrusions, alerts the mobile phone user and protects the mobile phone from Bluetooth Security vulnerabilities. As the name implies, the BIS is the component which generates Bluetooth intrusions and requests from remote devices. The BIS is thus a simulator for generating the Bluetooth intrusions. In essence, the BIS exactly replicate the behaviour of remote Bluetooth devices.

The BLA and BIS communication is implemented through socket communication. It simulates the Bluetooth link level connection between Bluetooth devices. A connect request in this prototype corresponds to the Bluetooth Logical Link Control and Adaptation Protocol (L2CAP) connect request. This is a data link level connection used on top of the Bluetooth link level connection and it is simulated as a socket connection in the prototype.

7.2 BLA/BIS Specifications and Pre-requisites for deployment

The BLA is implemented in Microsoft .NET Compact Framework (CF). The coding is in C#. The Microsoft Smartphone 2003 Emulator is selected as the simulator, which replicates the Bluetooth mobile phone and becomes the platform from where the BLA Prototype is implemented.

The pre-requisite for deploying BLA prototype is as follows:

Operating System: Microsoft Windows XP

Main Memory: at least 1 GB

Processor: Intel(R) Pentium (R) 4 CPU 3.06 GHz Processor (recommended)

Software Requirements: Microsoft Visual Studio 2005,

Microsoft .NET Compact Framework version 1.0,

Microsoft Smartphone 2003 Software Development Kit (SDK),

Microsoft Active Sync version 4.2

The BIS is implemented in Microsoft .NET Framework. The coding is in C#. The BIS is implemented as a Microsoft Windows project with a Windows Forms Graphical User Interface (GUI). It corresponds to intrusion devices, which compromise Bluetooth mobile phones. Internet access is a pre-requisite for the BLA and BIS communication. The research prototype is implemented and tested on top of a Microsoft Windows XP Operating System, with 1 GB main memory and on an Intel(R) Pentium (R) 4 CPU 3.06 GHz Processor.

The next section provides an insight into the communication between the BLA and BIS.

7.3 BLA/BIS communication message types

Communication between BLA and BIS takes place through a structured message exchange format, which simulates the communication between two Bluetooth devices. The message types are defined as follows:

| Message Type | Value in Header | Description |
|---------------------|-----------------|--|
| Connect Request | 1 | Request to establish a Bluetooth connection with the mobile phone. |
| Connect Response | 2 | Connect Response from BLA. The response can be positive or negative. If the request is safe, a positive connect response is sent, otherwise the connect request is classified as an intrusion attempt and instead of sending a Connect Response, the BLA sends a Disconnect Request. |
| Disconnect Request | 3 | Request to disconnect BLA and BIS communication. |
| Disconnect Response | 4 | Disconnect Response from BLA. |
| Rule Match Request | 5 | Rule Match Request sent by BLA to BIS to obtain more details of the remote device. The aim is to decide whether the device is from a reliable source or whether it is an intruder. |

| | | |
|-------------------------|----|---|
| Rule Match Response | 6 | Rule Match Response from the BIS to BLA. If the rules match, a positive rule match response is sent, otherwise, the request from the remote device is classified as an intrusion and instead of sending a rule match response, BLA then sends a Disconnect Request. |
| Authentication Request | 7 | Authentication Request received by the BLA from the BIS. |
| Authentication Response | 8 | Authentication Response from the BLA to BIS. If the authentication phase succeeds, a positive authentication response is sent, otherwise, an intrusion is detected and, instead of sending an authentication response, BLA then sends a Disconnect Request. |
| Service Access Request | 9 | Request from the BIS to get access to the Bluetooth services offered by the BLA. |
| Service Access Response | 10 | Service Access Response is sent by the BLA to BIS if the request is safe; otherwise, a Disconnect Request is sent by the BLA as response. |
| Request Failed | 11 | Request Failed message is sent |

| | | |
|--|--|--|
| | | <p>by the BLA to BIS on conditions where the mobile phone user discards the request under consideration. This happens when the user selects the 'Discard Request' option of the BLA.</p> |
|--|--|--|

TABLE 7.1

The next section provides a detailed discussion of the BLA.

7.4 BLA

When BLA is started, the first step is the initialisation of databases. The Connection Database (CDB), Trusted Devices Database (TDDB), Non Trusted Devices Database (NTDDDB), Services and Devices Mapping Database (SDMDB), and Logging Database (LDB) are initialised. On successful initialisation of databases, the BLA proceeds to the second step, which is the connection to the Bluetooth module. As explained in section 6.3 of Chapter 6, the BLA connects to the Bluetooth Module through the 'BLA - Bluetooth Module Interface' (BBMI). The BLA GUI is put into practice as in the following screenshot.



FIGURE 7.1 BLA GRAPHICAL USER INTERFACE

The BLA is equipped with six menu options to cater for the various user interface requirements, which are described in the following subsection.

7.4.1 BLA Menu Options

The following screenshot shows the menu options provided by the BLA. When the user clicks on the 'BLA – Options' the menu options are popped as represented in Figure 7.2.



FIGURE 7.2 BLA MENU OPTIONS

The next sub-sections analyses the BLA menu options one by one.

7.4.1.1 Start BLA

When the user selects 'Start BLA' option, the BLA is started and the Mobile Phone User Interface (MPUI) is alerted as represented in the following screenshot.



FIGURE 7.3 START BLA

7.4.1.2 Accept Request

The purpose of the 'Accept Request' menu option is to provide the mobile phone user the freedom to accept one of the following from a remote Bluetooth device: A safe connect request, an authentication request, or a service access request. In this prototype, a request from the BIS is accepted and the corresponding response is sent only if the user selects the 'Accept Request'. When the user selects the 'Accept Request', the MPUI is alerted of this as in the following screenshot.



FIGURE 7.4 ACCEPT REQUEST

7.4.1.3 Discard Request

The purpose of the 'Discard Request' menu option is to provide the mobile phone user the freedom to reject any request from a remote Bluetooth device. When the user selects 'Discard Request', the MPUI is alerted of this as in the following screenshot and a 'Request Failed' response is sent to the BIS.



FIGURE 7.5 DISCARD REQUEST

7.4.1.4 Log Packet

This option is provided to enable the logging of the information exchange between the communicating devices. The user has the option to enable the logging of the information exchange with the suspicious devices or with any devices. When the user chooses the 'Log Packet' option, the MPUI is alerted of this as in the following screenshot.

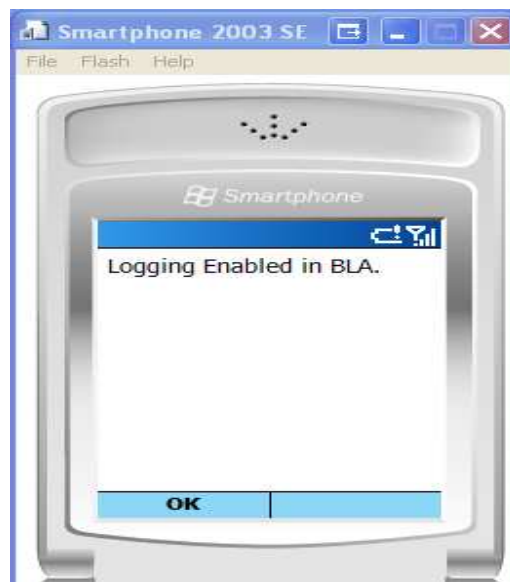


FIGURE 7.6 LOG PACKET

7.4.1.5 Stop BLA

As the name implies, when this option is selected, the BLA is stopped. When 'Stop BLA' is clicked, a 'Disconnect Request' is sent to the BIS and the BLA is disconnected from the BBMI. The MPUI receives a stopping alert as represented in the screenshot.



FIGURE 7.7 STOP BLA

7.4.1.6 Power off Bluetooth

This option is provided to enable the user to switch off Bluetooth directly from the MPUI to safeguard the device against intrusions in cases where the BLA has detected an intrusion attempt. When this option is selected, the Bluetooth is switched off and the MPUI receives an alert as in the following screenshot.



FIGURE 7.8 POWER OFF BLUETOOTH

7.4.2 Exit

Apart from the above Menu Options, an exit option is also provided in the main menu to exit from BLA application. When the 'Exit' option is clicked, the following events take place: All the databases are de-initialised; all the resources held by BLA are released; the BIS at the remote side gets an indication that BLA is closed through a 'Disconnect Request'; the MPUI gets the alert shown in the following screenshot and the BLA exits.



FIGURE 7.9 EXIT FROM BLA

The next sub-section explains the BLA Database layout used in the implementation of the prototype.

7.4.3 BLA Database Layout in Smartphone

The BLA Database screenshot is represented below. Each folder shown in the screenshot corresponds to a respective database. The databases are stored in the Smartphone's file system in the '\storage\Application Data\BLADatabase' folder. Each database is stored as a custom database in the form of a text file. This is attributable to Smartphone emulator's limitations in supporting third party databases.

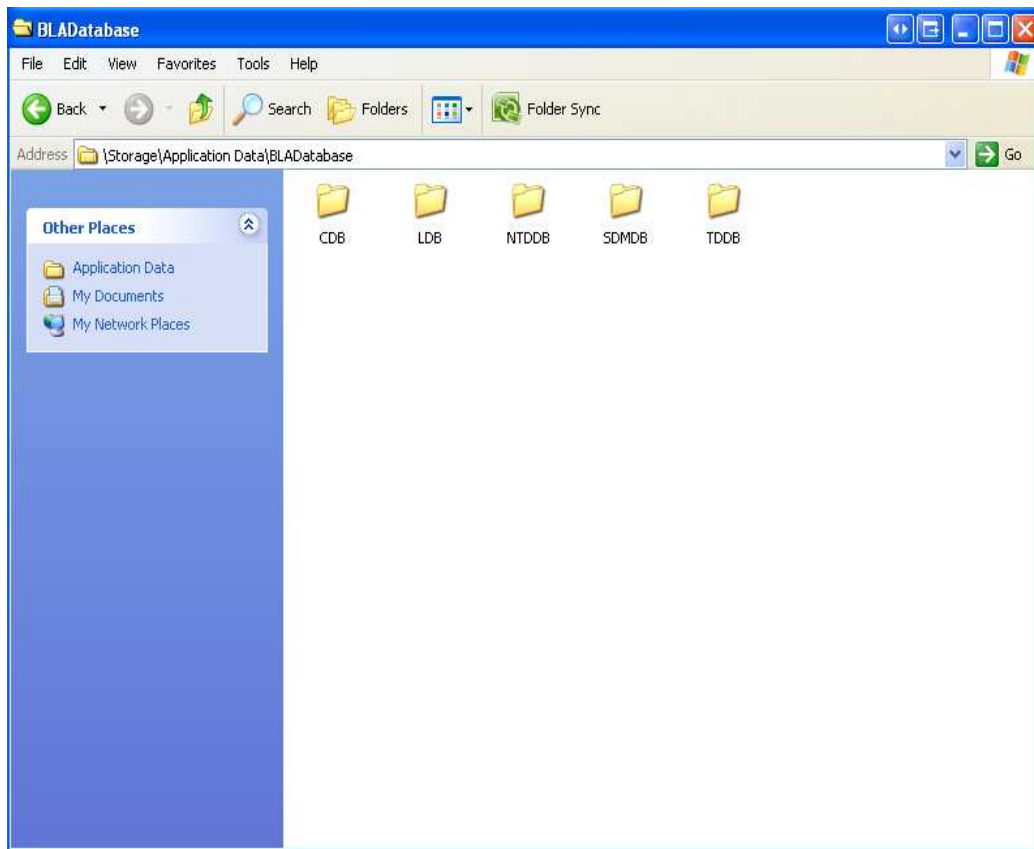


FIGURE 7.10 BLA DATABASE

Figure 7.11 to Figure 7.15 represent the status of each BLA database after a successful BLA and BIS session.

In the representation of the TDDb below, the Bluetooth Device Addresses (BD_ADDR) of the devices trusted by the BLA can be seen. The BLA classifies these devices as safe and accepts 'Connect Requests' from these devices. BLA adds a new trusted device to TDDb when it gets a

new safe device. Likewise, it removes a device from the TDDDB when it encounters an intrusion attempt from a device in the trusted device list.

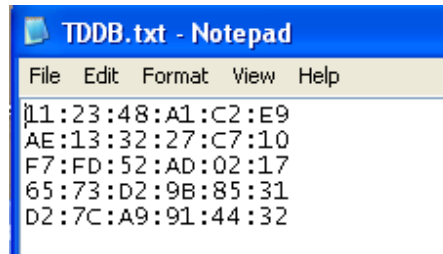


FIGURE 7.11 TDDB

The NTDDDB represented below shows the BD_ADDR of devices that are not trusted or are blacklisted by the BLA. The BLA classifies these devices as intruders and does not accept any request from these devices. This list is updated when BLA finds a new non trusted device or when BLA detects that a device in the trusted list has become non-trusted.

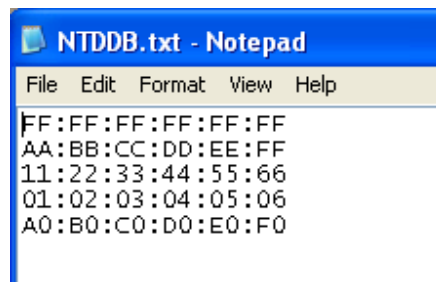


FIGURE 7.12 NTDDDB

The SDMDB represented below shows the BD_ADDR to service mapping generated by the BLA. According to the mapping in SDMDB, Bluetooth device '11:23:48:A1:C2:E9' has been granted access to the Dial Up Networking (DUN), Object Push Profile (OPP), Headset Profile (HSP), Hands Free Profile (HFP) and Serial Port Profile (SPP) service offered by the BLA. Bluetooth device 'AE:13:32:27:C7:10' is restricted to gain access only to the DUN and OPP service. Similarly, device 'F7:FD:52:AD:02:17' can only access the OPP and HSP service, device '65:73:D2:9B:85:31' can only access the HSP and HFP service, and device 'D2:7C:A9:9144:32' can only access the SPP and DUN service. The BLA grants access to a particular service as per the SDMDB database.

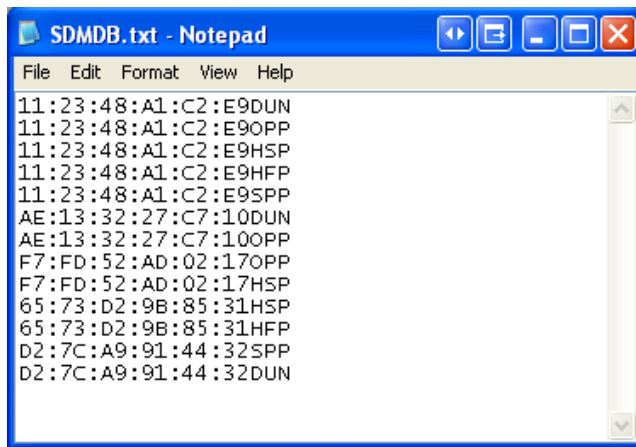


FIGURE 7.13 SDMDB

The CDB represented below shows the BD_ADDR of the remote device that is connected with the BLA after a successful connect request and connect response. This list is updated in accordance to the new successful connections with BLA.

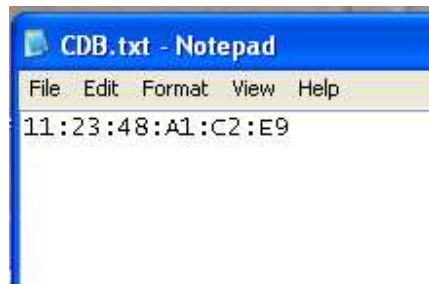
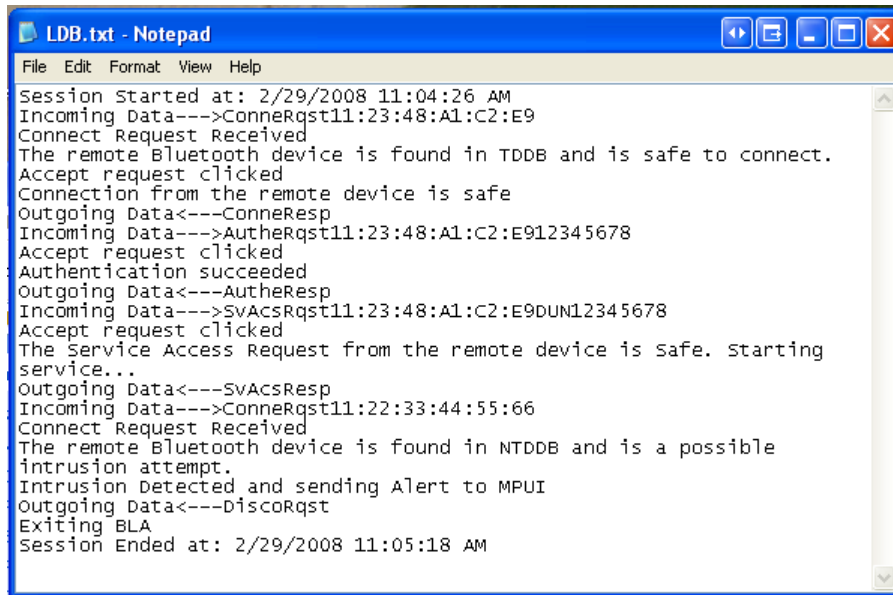


FIGURE 7.14 CDB

The LDB illustrated below shows the logging of a session between the BLA and BIS. The LDB starts logging data when the user clicks on 'Log Packet'. All the incoming and outgoing requests to and from BLA to the BIS are logged into the LDB between the start time of the session and the end time of the session. The LDB is very significant in that it can be used as future evidence to track intrusions and communication sessions between the BLA and BIS. The LDB data is especially useful in situations where the device gets compromised as a result of an intrusion.



```
File Edit Format View Help
Session Started at: 2/29/2008 11:04:26 AM
Incoming Data--->ConneRqst11:23:48:A1:C2:E9
Connect Request Received
The remote Bluetooth device is found in TDDb and is safe to connect.
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConneResp
Incoming Data--->AuthRqst11:23:48:A1:C2:E912345678
Accept request clicked
Authentication succeeded
Outgoing Data<---AuthResp
Incoming Data--->SvAcsRqst11:23:48:A1:C2:E9DUN12345678
Accept request clicked
The Service Access Request from the remote device is Safe. Starting
service...
Outgoing Data<---SvAcsResp
Incoming Data--->ConneRqst11:22:33:44:55:66
Connect Request Received
The remote Bluetooth device is found in NTDDb and is a possible
intrusion attempt.
Intrusion Detected and sending Alert to MPUI
Outgoing Data<---Discorqst
Exiting BLA
Session Ended at: 2/29/2008 11:05:18 AM
```

FIGURE 7.15 LDB

The next section describes the BIS implementation in detail.

7.5 BIS

The BIS component simulates the remote Bluetooth devices connecting to the device, which is equipped with the BLA Prototype implementation. The BIS generates safe requests, intrusions and random requests in order to test, analyse and emulate the power of the BLA. The BIS is explained in more detail in the following sub-sections.

The BIS GUI is implemented as in the screenshot that follows.



FIGURE 7.16 BIS GRAPHICAL USER INTERFACE

7.5.1 BIS General Menu Options

The BIS general Menu options are represented in the following screenshot.



FIGURE 7.17 BIS MENU OPTIONS

When the 'Start Bluetooth Simulator' option is selected, the BIS starts as shown in the following screenshot.



FIGURE 7.18 BLUETOOTH INTRUSION SIMULATOR STARTED

When the 'exit' option is selected, the BIS sends a Disconnect Request' to the BLA at the remote side. It then frees all the resources and exits the BIS. The following screenshot gives an example of how the BIS exits.



FIGURE 7.19 EXIT BLUETOOTH INTRUSION SIMULATOR

The following three sub-sections sets out the various requests that are generated by the BIS and sent to the BLA.

7.5.2 BIS Safe Requests Menu Options

The BIS Safe Requests Menu consists of options to send a ‘Safe ConnectRequest’, a ‘Safe AuthenticationRequest’ and a ‘Safe ServiceAccessRequest’ to BLA. As the name implies, each of these options are provided to generate safe requests to the remote Bluetooth device. The following screenshot represents the BIS Safe Requests menu options.



FIGURE 7.20 BIS SAFE REQUESTS

7.5.3 BIS Intrusions Menu Options

The BIS Intrusions Menu consists of options to send a ‘Connection Attack’, an ‘Authentication Attack’ and a ‘ServiceAccess Attack’ to BLA. As the name implies, each of these options are provided to generate attacks or intrusions to compromise the remote Bluetooth device. The following screenshot represents the BIS Intrusions menu options.



FIGURE 7.21 BIS INTRUSIONS

7.5.4 BIS Random Safe/Unsafe Requests Menu Options

The BIS Random Safe/Unsafe Requests Menu consists of options to send a 'Random ConnectRequest', a 'Random AuthenticationRequest' and a 'Random ServiceAccessRequest' to BLA. As the name implies each of these options are provided to generate random requests to the remote Bluetooth device. The Random requests are based on random number generation scheme in the BIS implementation and there is an equal probability of random request becoming a safe request or an intrusion attempt based on the random number value. The following screenshot illustrates the BIS Random Safe/Unsafe Requests menu options.



FIGURE 7.22 BIS RANDOM (SAFE/UNSAFE) REQUESTS

The next section explains the communication between the BLA and BIS.

7.6 Communication between the BIS and BLA

The communication between the BIS and the BLA is in the form of request and response format as shown in Table 7.1 of section 7.2. The BLA and the BIS must be started and be connected successfully before any request/response exchange can take place. The following sub-sections investigate each request/response scheme and the respective message processing in the BIS and BLA.

7.6.1 Safe Connect Request and Response

In this, a genuine connect request from a Bluetooth Device whose `BD_ADDR` is '11:23:48:A1:C2:E9' is sent from the BIS to BLA and the response is simulated. The BIS sends this request when the 'Safe ConnectRequest' option is selected from 'Safe Requests' option in the BIS's GUI. The systematic process of the request is explained below with the corresponding screenshots.

On receiving the request, the BLA calls the Intrusion Detection and Verification Module (IDVM) to process the request. The IDVM alerts the MPUI of an incoming connect request as represented in the following screenshot.



FIGURE 7.23 BLA RECEIVING CONNECT REQUEST FROM BIS

After indicating to the MPUI, the IDVM also indicates the request to Connection and Disconnection Module (CDM). The CDM processes the requests and determines whether the incoming device's BD_ADDR is listed in its TDDB. The TDDB that CDM is verifying is represented in the following screenshot.

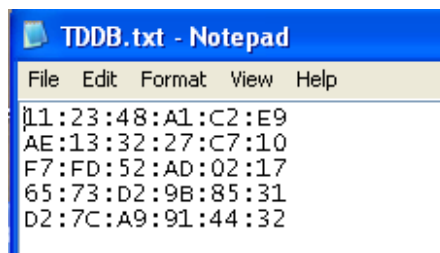


FIGURE 7.24 BLA CHECKING TDDB

Since the device '11:23:48:A1:C2:E9' is listed in the database, CDM decides that it is safe to connect with the remote device. It then passes this information back to IDVM. The IDVM alerts the MPUI, as represented in the following screenshot.



FIGURE 7.25 BLA ALERTING MPUI OF A SAFE CONNECTION

The connect request is accepted and the connect response is sent only if the user accepts the connection by clicking the 'Accept Request' menu option. If the user chooses 'Accept Request', the MPUI is alerted (see Figure 7.4) and a positive connect response is sent. The following screenshot represents the successful connect response received by the BIS when the connect request is accepted by the BLA. The user has the freedom to discard the connect request (or any request) by choosing 'Discard Request'. This is covered in detail under section 7.6.12.



FIGURE 7.26 BIS RECEIVING A SUCCESSFUL CONNECT RESPONSE

When the connection phase is successful, the device address '11:23:48:A1:C2:E9' is added to the CDB as represented in the following screenshot.

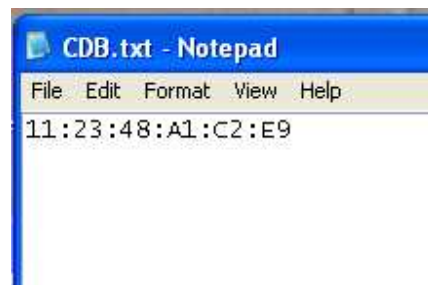


FIGURE 7.27 REMOTE DEVICE ADDRESS ADDED TO CDB DATABASE

7.6.2 Safe Authentication Request and Response

In this request and response scheme, a legitimate authentication request is sent from a Bluetooth device with BD_ADDR '11:23:48:A1:C2:E9' and with a PIN Code length of eight. The request is sent to BLA and the response is simulated. The BIS sends this request when the 'Safe Authentication Request' is selected from the 'Safe Requests' option in the BIS's GUI. As explained in Chapter 6, a legitimate authentication request is considered by the BLA as one, which

originates from a device that is already connected to the BLA, is in the CDB, and has a PIN Code length that is equal to or greater than eight. The systematic process of the request is explained below by means of the screenshots. On receiving the request, the BLA calls the IDVM to process the request. The IDVM alerts the MPUI of an incoming authentication request as represented in the following screenshot.



FIGURE 7.28 BLA RECEIVING AUTHENTICATION REQUEST FROM BIS

After indicating to the MPUI, the IDVM also indicates the request to the Authentication Module (AM). The AM then processes the request and determines whether the incoming device's BD_ADDR is listed in its CDB. Since the device '11:23:48:A1:C2:E9' is listed in the CDB and the PIN Code length is eight, the AM determines that it is safe to authenticate the device and passes this information back to IDVM. The IDVM alerts the MPUI as represented in the following screenshot.



FIGURE 7.29 BLA ALERTING MPUI OF A SAFE AUTHENTICATION REQUEST

The authentication request is accepted and the authentication response is sent only if the user accepts the request by clicking the 'Accept Request' menu option. If the user chooses 'Accept Request', then the MPUI is alerted of this, as represented in Figure 7.4. Consequently, a positive authentication response is sent. The successful authentication response that BIS receives, when the authentication request is accepted by BLA, is represented in the following screenshot.



FIGURE 7.30 BIS RECEIVING A SUCCESSFUL AUTHENTICATION RESPONSE

7.6.3 Safe Service Access Request and Response

In this request and response scheme, a Dial Up Networking (DUN) service access request is sent from a Bluetooth Device with BD_ADDR '11:23:48:A1:C2:E9' and with a PIN Code length of eight. The request is sent to BLA and the response is simulated. The BIS sends this request when 'Safe ServiceAccessRequest' is selected from 'Safe Requests' option in the BIS's GUI. As explained in Chapter 6, a valid service access request is considered by BLA as one that originates from a device that is already connected to the BLA, and is in the CDB and has a PIN Code length equal to or greater than eight.

A constraint is that the service access requested by the device should be listed or mapped in the Services and Devices Mapping Database (SDMDB) against the requesting device's BD_ADDR. The systematic process of the request is explained below by means of the screenshots.

On receiving the request, the BLA calls the IDVM to process the request. The IDVM alerts the MPUI of an incoming service access request as represented in the following screenshot.



FIGURE 7.31 BLA RECEIVING SERVICE ACCESS REQUEST FROM BIS

After indicating to the MPUI, the IDVM also indicates the request to Service Module (SM). The SM then processes the request and determines whether the incoming device's BD_ADDR is listed in its CDB. Since the device '11:23:48:A1:C2:E9' is listed in the CDB and the PIN Code length is eight, the SM then proceeds to the next step. The SM checks the SDMDB to determine whether the device has access to the requested service. In this particular request, SM then confirms that the device '11:23:48:A1:C2:E9' has access to DUN service. The SDMDB that SM verifies is represented in the following screenshot.

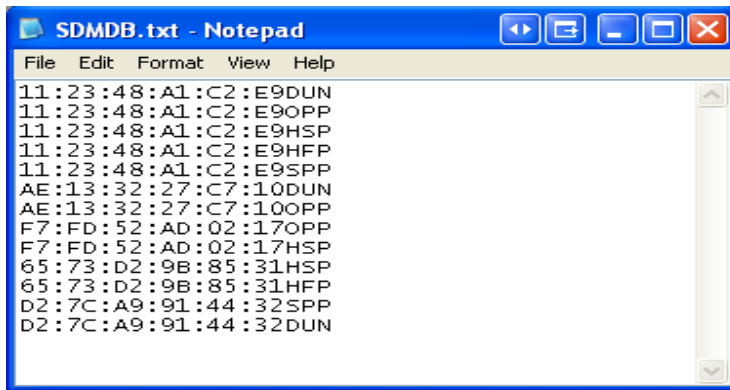


FIGURE 7.32 SM CHECKING SDB

Since the service access request is legitimate, the IDVM alerts the MPUI, as represented in the following screenshot.



FIGURE 7.33 BLA ALERTING MPUI OF A SAFE SERVICE ACCESS REQUEST

The service access request is accepted and the service access response is sent only if the user accepts the request by clicking the 'Accept Request' menu option. If the user chooses 'Accept Request', the MPUI is alerted of this (see Figure 7.4) and a positive service access response is sent. The following screenshot represents the successful service access response received by the BIS when the service access request is accepted by BLA.



FIGURE 7.34 BIS RECEIVING A SUCCESSFUL SERVICE ACCESS RESPONSE

7.6.4 Connection Attack from BIS and response from BLA

In this case, the BIS attempts to compromise the remote Bluetooth device through a connection attack. A connection attack from a Bluetooth Device of which the BD_ADDR is 'AA:BB:CC:DD:EE:FF' is sent to BLA and the response is simulated. The BIS attempts the connection attack when 'Connection Attack' is selected from the 'Intrusions' option in the BIS's GUI. On receiving the request, the BLA then calls the IDVM to process the request. The IDVM alerts the MPUI of an incoming connect request. This is represented in Figure 7.23.

After indicating to the MPUI, the IDVM also indicates the request to CDM. The CDM then processes the request and determines whether the incoming device's BD_ADDR is listed in its

TDDDB. The CDM determines that the device is not listed in the TDDDB and it proceeds to the next step of verifying the NTDDDB. The NTDDDB, as being verified by the CDM, is represented in the following screenshot.

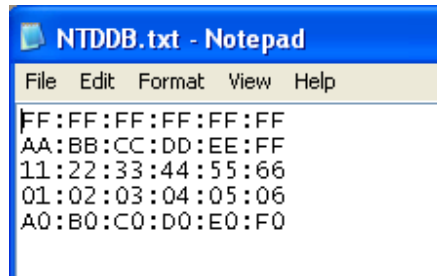


FIGURE 7.35 BLA CHECKING NTDDDB

Since the device from which the connection request originated is listed in the NTDDDB, the CDM concludes that it is a possible intrusion attempt and passes the information back to the IDVM. If the device is found neither in the TDDDB nor in the NTDDDB, the IDVM then sends a ‘Rule Match Request’ to the BIS (explained in section 7.6.7). After getting the intrusion attempt indication, the IDVM alerts the MPUI. This is represented in the following screenshot.



FIGURE 7.36 IDVM ALERTING MPUI OF THE INTRUSION

After alerting the MPUI of the intrusion attempt, the IDVM then sends a disconnect request and informs the BIS of the intrusion detection. This is represented in the following screenshot. The BLA is subsequently disconnected from Bluetooth and all the resources are released.



FIGURE 7.37 BIS GETTING A DISCONNECT REQUEST AND INDICATION THAT THE INTRUSION ATTEMPT IS DETECTED BY BLA

The following screenshot represents the logging information concerning this connection attack. It is obtained from the LDB database.

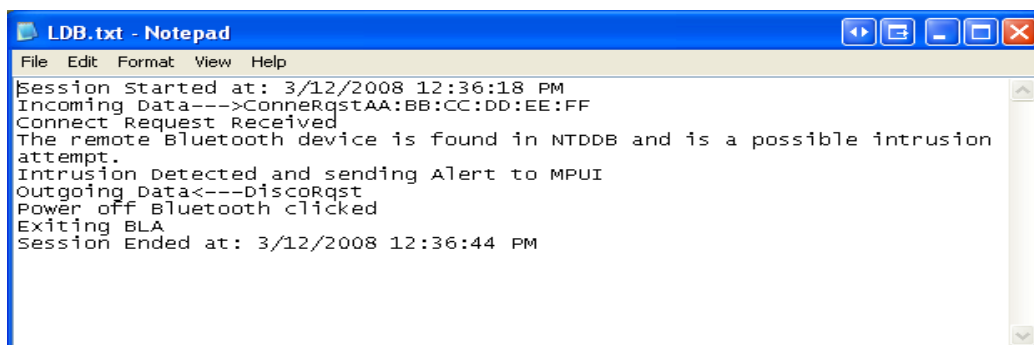


FIGURE 7.38 CONNECTION ATTACK LOGGING INFORMATION OBTAINED FROM LDB

7.6.5 Authentication Attack from BIS and Response from BLA

In this case, the BIS tries to compromise the remote Bluetooth device through an authentication attack. The BIS sends an authentication request from a device with BD_ADDR 'FF:FF:FF:FF:FF:FF' and with 'PIN 123'. The BIS attempts the authentication attack when 'Authentication Attack' is selected from the 'Intrusions' option in the BIS's GUI. On receiving the request, the BLA calls the IDVM to process the request. The IDVM indicates the request to AM. The AM then processes the request and determines if the request is genuine or an intrusion attempt. The AM then concludes that it is a possible intrusion attempt and passes this information back to IDVM. The IDVM subsequently alerts the MPUI of the authentication attack. This is represented in the following screenshot.



FIGURE 7.39 IDVM ALERTING MPUI OF THE INTRUSION

After alerting the MPUI of the intrusion attempt, the IDVM sends a disconnect request and informs the BIS of the intrusion detection as represented in Figure 7.37. The BLA is then disconnected from Bluetooth and all the resources are released.

The following screenshot represents the logging information obtained from the LDB database concerning this authentication attack.

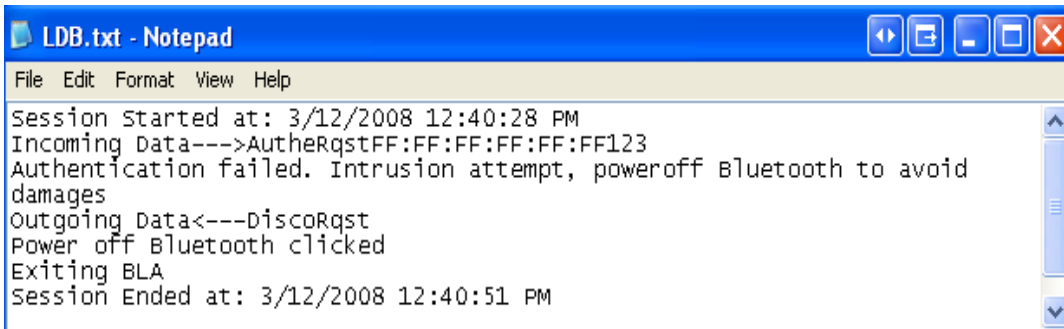


FIGURE 7.40 AUTHENTICATION ATTACK LOGGING INFORMATION OBTAINED FROM LDB

7.6.6 Service Access Attack from BIS and Response from BLA

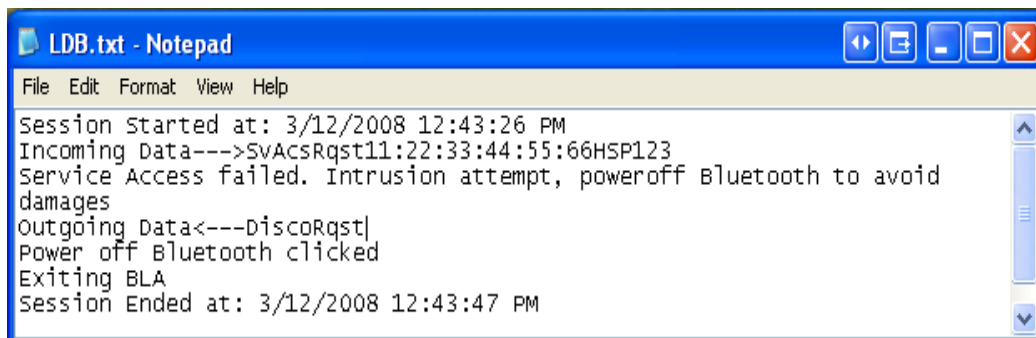
The BIS tries to compromise the remote Bluetooth device through a service access attack. The BIS sends a service access request to access Headset Profile (HSP) service from a device with BD_ADDR '11:22:33:44:55:66' and with 'PIN 123'. The BIS attempts the service access attack when 'ServiceAccess Attack' is selected from the 'Intrusions' option in the BIS's GUI. On receiving the request, the BLA calls the IDVM to process the request. The IDVM then indicates the request to SM. The SM processes the request and determines if the request is genuine or an intrusion attempt. The SM then finds that it is a possible intrusion attempt and passes this information back to IDVM. The IDVM subsequently alerts the MPUI of the service access attack. This is represented in the following screenshot.



FIGURE 7.41 IDVM ALERTING MPUI OF THE INTRUSION

After alerting the MPUI of the intrusion attempt, the IDVM then sends a disconnect request and informs the BIS of the intrusion detection as represented in Figure 7.37. The BLA is subsequently disconnected from Bluetooth and all the resources are released.

The following screenshot represents the logging information obtained from the LDB database concerning this service access attack.

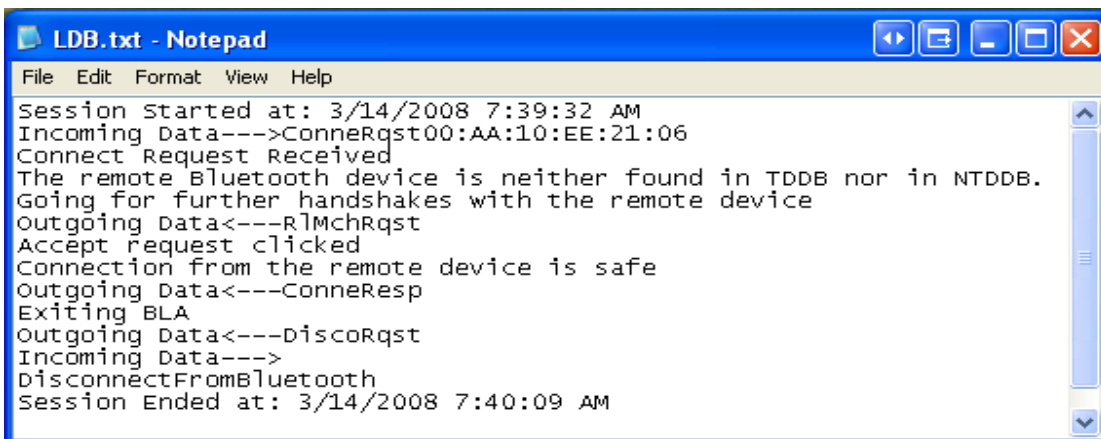


```
LDB.txt - Notepad
File Edit Format View Help
Session Started at: 3/12/2008 12:43:26 PM
Incoming Data--->SvAcsRqst11:22:33:44:55:66H5P123
Service Access failed. Intrusion attempt, poweroff Bluetooth to avoid
damages
Outgoing Data<---DiscoRqst|
Power off Bluetooth clicked
Exiting BLA
Session Ended at: 3/12/2008 12:43:47 PM
```

FIGURE 7.42 SERVICE ACCESS ATTACK LOGGING INFORMATION OBTAINED FROM LDB

7.6.7 Random Connect Request and Response from BLA

The purpose of this request response scheme is to generate a random connect request from the BIS and to send it to the BLA. The following screenshot represents the log file obtained from the LDB after a safe random connect request and response session.



```
LDB.txt - Notepad
File Edit Format View Help
Session Started at: 3/14/2008 7:39:32 AM
Incoming Data--->Connerqst00:AA:10:EE:21:06
Connect Request Received
The remote Bluetooth device is neither found in TDDb nor in NTDDb.
Going for further handshakes with the remote device
Outgoing Data<---R1Mchrqst
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConnerResp
Exiting BLA
Outgoing Data<---DiscoRqst
Incoming Data--->
DisconnectFromBluetooth
Session Ended at: 3/14/2008 7:40:09 AM
```

FIGURE 7.43 RANDOM CONNECT REQUEST AND RESPONSE (SAFE CONNECTION)

As represented in Figure 7.43, the BLA receives a connect request from a device with BD_ADDR '00:AA:10:EE:21:06'. The BLA then checks the TDDB to verify that the request is from a reliable source (see Figure 7.11). The BLA then finds that the device is not in the TDDB and proceeds to the next step of verifying the NTDDDB to determine whether the device is an intruder (see Figure 7.12). After verifying the TDDB and NTDDDB, the BLA concludes that the request is from a new device, since it is not listed in TDDB and NTDDDB. The possibility now arises that the request can be a safe connect request or a possible intrusion attempt. The BLA sends a rule match request to the BIS to retrieve more information about the remote device (as explained in section 6.2.3.1 of Chapter 6). The following screenshot represents the rule match request received by the BIS.



FIGURE 7.44 RULE MATCH REQUEST RECEIVED BY BIS FROM BLA

After sending the rule match request, the BLA waits for the rule match response from the BIS. When the BLA receives the rule match response from the BIS, it processes it to see if the rules are matching with the rules that are defined by the BLA. After the processing phase, the BLA concludes that the request is from a reliable source. Figure 7.45 and 7.46 demonstrate how the TDDB and CDB are updated respectively.

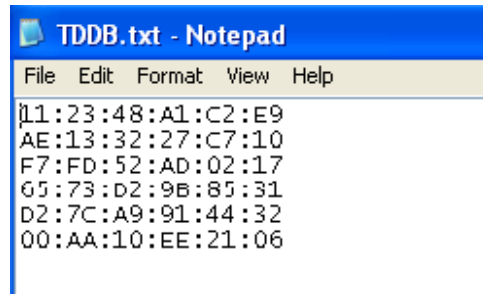


FIGURE 7.45 TDDB, AFTER A SAFE RULE MATCH REQUEST FOR CONNECTION FROM BIS

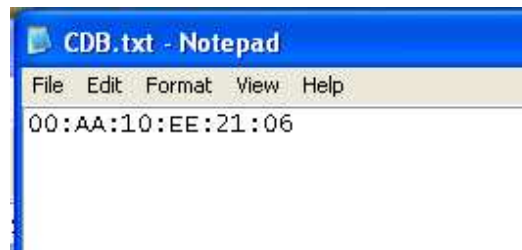
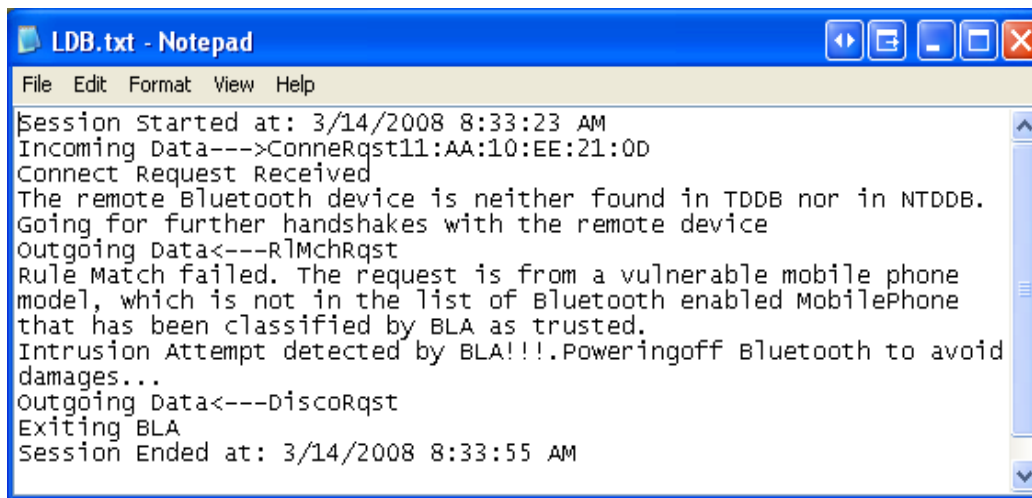


FIGURE 7.46 CDB SHOWING THE CONNECTION TO THE REMOTE DEVICE AFTER GETTING A POSITIVE RULE MATCH RESPONSE FROM BIS

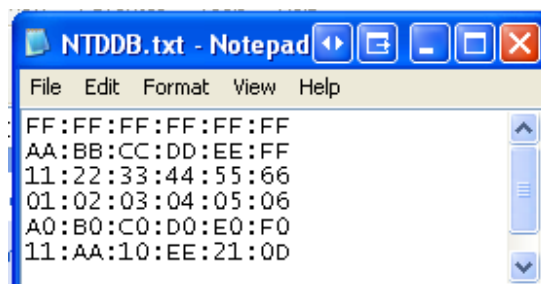
This section discusses a case where the random connect request received by the BLA from the BIS is a connection attack. The following screenshot represents the log file obtained from the LDB after the random connect request and the response session (classified as an intrusion attempt by BLA). In this case the attempt is to simulate a connect request from a Nokia 7650, which is classified by BLA as a vulnerable Bluetooth mobile phone. It is categorised as vulnerable because of inherent Bluetooth security issues and due to the actions taken by BLA on a connect request.



```
LDB.txt - Notepad
File Edit Format View Help
Session started at: 3/14/2008 8:33:23 AM
Incoming Data--->ConnerQst11:AA:10:EE:21:0D
Connect Request Received
The remote Bluetooth device is neither found in TDDB nor in NTDDB.
Going for further handshakes with the remote device
Outgoing Data<---R1MchRqst
Rule Match failed. The request is from a vulnerable mobile phone
model, which is not in the list of Bluetooth enabled MobilePhone
that has been classified by BLA as trusted.
Intrusion Attempt detected by BLA!!!.Poweringoff Bluetooth to avoid
damages...
Outgoing Data<---DiscoRqst
Exiting BLA
Session Ended at: 3/14/2008 8:33:55 AM
```

FIGURE 7.47 LDB AFTER GETTING A RANDOM CONNECTION ATTACK FROM BIS

As shown in the LDB, the BLA gets a connect request from a device with BD_ADDR '11:AA:10:EE:21:0D'. On detecting that, the device is not in TDDB and NTDDB; BLA goes for a rule match request and waits for the response. The BLA processes a rule match response and finds that the request is from a vulnerable mobile phone that is categorised by BLA as an unsafe connection device. The NTDDB is updated with the new device as depicted in the following screenshot.

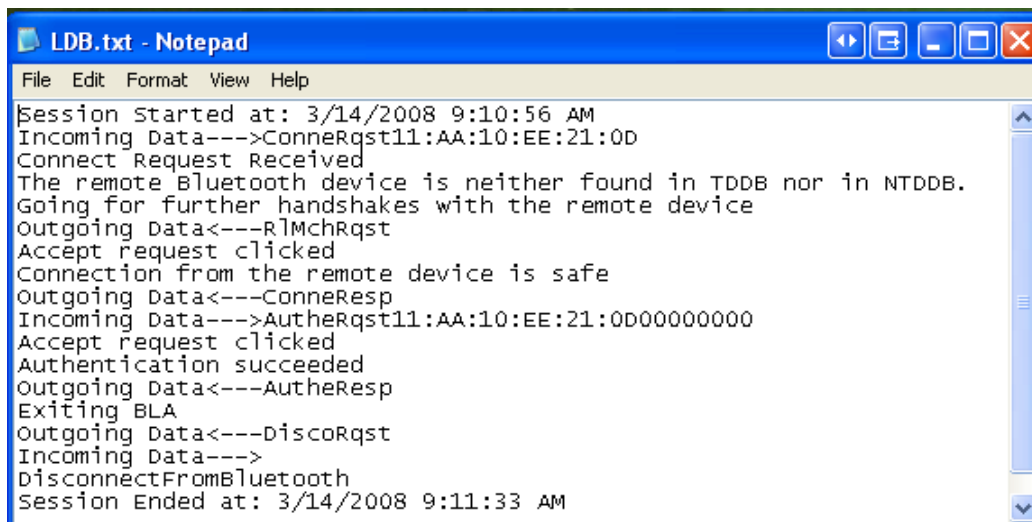


```
NTDDB.txt - Notepad
File Edit Format View Help
FF:FF:FF:FF:FF:FF
AA:BB:CC:DD:EE:FF
11:22:33:44:55:66
01:02:03:04:05:06
A0:B0:C0:D0:E0:F0
11:AA:10:EE:21:0D
```

FIGURE 7.48 NTDDB AFTER GETTING A RANDOM CONNECTION ATTACK FROM BIS

7.6.8 Random Authentication Request and Response from BLA

The purpose of this request response scheme is to generate a random authentication request from the BIS and send it to the BLA. The following screenshot represents the log file obtained from the LDB after a safe random authentication request and response session. As depicted in the screenshot, the BLA gets an authentication request from a device with BD_ADDR '11:AA:10:EE:21:0D' and PIN '00000000'. The BLA then calls the CM to check the CDB in verifying that the request is from a reliable source. When the BLA finds that the device is in CDB, it then goes to the next step of calling the AM to verify the authenticity of the request. When the AM concludes that it is safe to authenticate the remote device, a positive response is sent to the BIS.

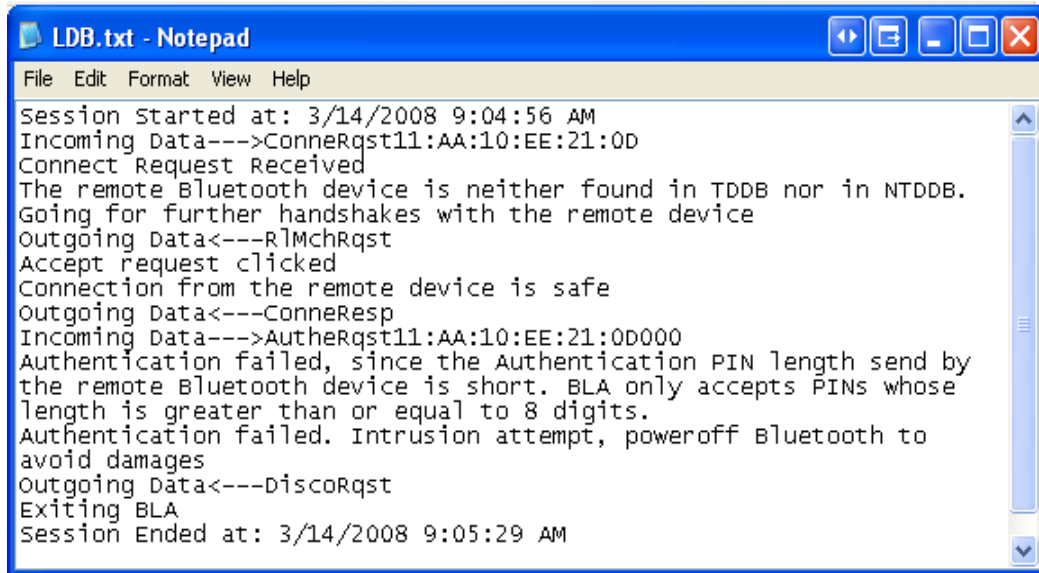


```
LDB.txt - Notepad
File Edit Format View Help
Session started at: 3/14/2008 9:10:56 AM
Incoming Data--->ConneRqst11:AA:10:EE:21:0D
Connect Request Received
The remote Bluetooth device is neither found in TDDB nor in NTDDB.
Going for further handshakes with the remote device
Outgoing Data<---R1MchRqst
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConneResp
Incoming Data--->AuthRqst11:AA:10:EE:21:0D00000000
Accept request clicked
Authentication succeeded
Outgoing Data<---AuthResp
Exiting BLA
Outgoing Data<---DiscoRqst
Incoming Data--->
DisconnectFromBluetooth
Session Ended at: 3/14/2008 9:11:33 AM
```

FIGURE 7.49 RANDOM AUTHENTICATION REQUEST AND RESPONSE (SAFE AUTHENTICATION)

Discussed here is the case when the random authentication request received from the BIS is an authentication attack. The following screenshot represents the log file obtained from the LDB after a random authentication request and response session (classified as an intrusion attempt by the BLA). As depicted in the screenshot, BLA gets an authentication request from a device with BD_ADDR '11:AA:10:EE:21:0D' and PIN '000'. The BLA then calls CM to check the CDB in verifying that the request is from a reliable source. When the BLA finds that the device is in CDB, it then goes to the next step of calling the AM to verify the authenticity of the request. The AM

then concludes that it is unsafe to authenticate the remote device, as the PIN length is only three. As explained in section 6.2 of Chapter 6, the AM will reject an authentication request with a PIN length shorter than eight.



```
LDB.txt - Notepad
File Edit Format View Help
Session Started at: 3/14/2008 9:04:56 AM
Incoming Data--->ConneRqst11:AA:10:EE:21:0D
Connect Request Received
The remote Bluetooth device is neither found in TDDB nor in NTDDB.
Going for further handshakes with the remote device
Outgoing Data<---R1MchRqst
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConneResp
Incoming Data--->AutherRqst11:AA:10:EE:21:0D000
Authentication failed, since the Authentication PIN length send by
the remote Bluetooth device is short. BLA only accepts PINs whose
length is greater than or equal to 8 digits.
Authentication failed. Intrusion attempt, poweroff Bluetooth to
avoid damages
Outgoing Data<---DiscoRqst
Exiting BLA
Session Ended at: 3/14/2008 9:05:29 AM
```

FIGURE 7.50 LDB AFTER GETTING A RANDOM AUTHENTICATION ATTACK FROM BIS

7.6.9 Random Service Access Request and Response from BLA

The purpose of this request response scheme is to generate a random service access request from the BIS and send it to the BLA. The following screenshot represents the log file obtained from the LDB after a safe random service access request and response session. As depicted in the screenshot, the BLA gets a service access request from a device with BD_ADDR 'AE:13:32:27:C7:10' and PIN '12345678' with the request to access DUN. The BLA calls the CM to check the CDB in verification that the request is from a reliable source. The BLA then finds that the device is in CDB and proceeds to the next step of calling the SM to verify that device 'AE:13:32:27:C7:10' has been granted access to the requested 'DUN' service. The SM then checks the SDMDB as demonstrated in Figure 7.13. On concluding that it is safe to access the requested service, the SM then sends a positive service access response to the BIS.

```
LDB.txt - Notepad
File Edit Format View Help
Session Started at: 3/14/2008 9:26:58 AM
Incoming Data--->ConneRqstAE:13:32:27:C7:10
Connect Request Received
The remote Bluetooth device is found in TDDb and is safe to connect.
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConneResp
Incoming Data--->SvAcsRqstAE:13:32:27:C7:10DUN123456789
Accept request clicked
The Service Access Request from the remote device is safe. Starting
service...
Outgoing Data<---SvAcsResp
Exiting BLA
Outgoing Data<---DiscoRqst
Incoming Data--->
DisconnectFromBluetooth
Session Ended at: 3/14/2008 9:27:39 AM
```

**FIGURE 7.51 RANDOM SERVICE ACCESS REQUEST AND RESPONSE
(SAFE SERVICE ACCESS REQUEST)**

Discussed here is the case when a random service access request received from the BIS is a service access attack. The following screenshot represents the log file obtained from the LDB after a service access request and response session (classified as an intrusion attempt by the BLA). As depicted in the screenshot, the BLA gets a service access request from a device with BD_ADDR 'AE:13:32:27:C7:10' and PIN '12345678' to access 'HFP' service. The BLA then calls the respective modules in verification of the CDB to determine whether the request is from a reliable source. On finding that the device is in the CDB, the BLA then proceeds to the next step of calling the SM to verify if the device 'AE:13:32:27:C7:10' has been granted access to the requested 'HFP' service. As depicted in the SDMDB (in Figure 13 in section 7.4.3) device 'AE:13:32:27:C7:10' is allowed to access the DUN and OPP service. From the log file obtained, it is evident that the remote device attempted access to the HFP. As this is not allowed, the BLA classified it as an intrusion attempt and a negative response was sent.

```
LDB.txt - Notepad
File Edit Format View Help
Session Started at: 3/14/2008 10:22:44 AM
Incoming Data--->ConnerQstAE:13:32:27:C7:10
Connect Request Received
The remote Bluetooth device is found in TDDb and is safe to connect.
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConnerResp
Incoming Data--->SvAcsRqstAE:13:32:27:C7:10HFP123456789
Service Access failed... The remote Bluetooth device doesn't have
the permission to access this Service.
Outgoing Data<---DiscoRqst
Exiting BLA
Session Ended at: 3/14/2008 10:23:21 AM
```

FIGURE 7.52 LDB AFTER GETTING A RANDOM SERVICE ACCESS ATTACK FROM BIS

7.6.10 Safe Request/Response session between BLA and BIS

The following screenshot represents the log file of the safe request and response message exchanges between the BIS and BLA. As demonstrated in the log, the BLA first receives a connect request from a device with BD_ADDR '11:23:48:A1:C2:E9'. The BLA consequently finds that the connect request is safe from the CDM. The MPUI is then alerted of the safe connect request. When the 'Accept Request' is selected from the MPUI, the connect request is accepted, the databases are updated and a positive connect response is sent to the BIS. The BLA then receives an authentication request from device '11:23:48:A1:C2:E9' with authentication PIN '12345678'. The BLA finds that the authentication request is safe from the AM and consequently the MPUI is alerted of the safe authentication request. When the 'Accept Request' is selected from the MPUI, the authentication request is accepted and a positive authentication response is sent to the BIS. The BLA now receives a request to access the DUN service from device '11:23:48:A1:C2:E9' with authentication PIN '12345678'. The BLA finds that the service access request is safe from the SM and the MPUI is alerted of the safe service access request. When the 'Accept Request' is selected from the MPUI, the service access request is accepted and a positive service access response is sent to the BIS.


```
LDB.txt - Notepad
File Edit Format View Help
Session Started at: 2/29/2008 9:22:26 AM
Incoming Data--->ConneRqst11:23:48:A1:C2:E9
Connect Request Received
Accept request clicked
Connection from the remote device is safe
Outgoing Data<---ConneResp
Incoming Data--->AutherQst11:23:48:A1:C2:E912345678
Accept request clicked
Authentication succeeded
Outgoing Data<---AutherResp
Incoming Data--->SvAcsRqst11:23:48:A1:C2:E9DUN12345678
Accept request clicked
The Service Access Request from the remote device is safe. Starting
service...
Outgoing Data<---SvAcsResp
Power off Bluetooth clicked
Outgoing Data<---DiscoRqst
Incoming Data--->
Exiting BLA
Session Ended at: 2/29/2008 9:23:14 AM
```

FIGURE 7.53 SAFE REQUEST/RESPONSE SESSION BETWEEN BLA AND BIS

7.6.11 BLA Discarding a Request from BIS

The BLA is equipped with the option of discarding any request from BIS by selecting the ‘Discard Request’ as shown in Figure 7.54. The requests received by the BLA may include a Connect Request, Authentication Request or Service Access Request. When this option is selected from the MPUI for discarding any request from the BIS, the MPUI is alerted as represented in Figure 7.5.

When BLA discards a request from the BIS, the BIS gets the indication as shown in the following screenshot.



FIGURE 7.54 BIS GETTING THE INDICATION THAT REQUEST IS DISCARDED BY BLA

The following screenshot shows the log file obtained from the LDB after a request is discarded from BLA.

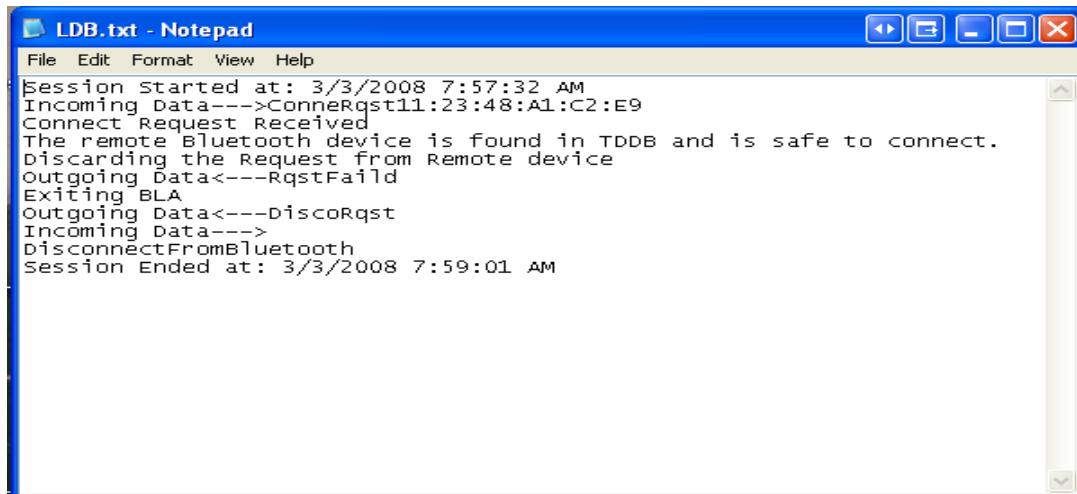


FIGURE 7.55 LDB AFTER SENDING A DISCARD REQUEST TO BIS

7.7 Summary

This chapter presented the implementation of the BLA Prototype and the BIS Prototype. The aim was to test and simulate the power of BLA in detecting Bluetooth intrusions and vulnerabilities. Section 7.1 addressed the prototype components and assumptions. Section 7.2 explained the BLA/BIS specifications and pre-requisites for deploying the prototype. Section 7.3 defined the communication message infrastructure between the BLA and the BIS. Sections 7.4 and 7.5 explained the BLA and the BIS GUIs in detail. Section 7.6 illustrated the communication between the BLA and the BIS and demonstrated how the BLA detects intrusions and safeguards the Bluetooth mobile phone. The next chapter concludes this research.



Conclusion

Bluetooth technology is becoming very popular and is becoming ubiquitous in modern society. According to the Bluetooth SIG, Bluetooth shipments have increased tremendously, particularly over the last few years. In fact, majority of the mobile phones are now equipped with Bluetooth. In high-end business phones, the penetration rate is even higher, and many business-class phones include Bluetooth [104,105].

While Bluetooth technology has gained significant development in current business world solutions, security issues have also increased exponentially. The emergence of a variety of mobile threats has heightened the concerns of mobile users and enterprises regarding the maturity of the technology, especially in terms of its overall lack of comprehensive security. The current Bluetooth security implementations in mobile phones are vulnerable and raise serious security concerns. It is clear that further steps have to be taken to alleviate the security issues in mobile phones. It is important for all Bluetooth mobile phone manufacturers to take a proactive approach to mitigate potential security breaches before it is too late [104,105]. This research has attempted to alleviate Bluetooth security vulnerabilities and limitations by devising a prototype for improving built-in Bluetooth security mechanism in mobile phones.

8.1 Research Synopsis

This research begins with the analysis of the current Bluetooth security issues and arriving at the motivation and problem statement of the research. An outline of how the problem is going to be dealt with was also addressed in detail.

The research continued to give an outline of the applications and fundamental concepts of Bluetooth technology, such as the Bluetooth protocol stack and Bluetooth profiles.

This was followed by a detailed explanation of the existing Bluetooth Security Architecture, its limitations, vulnerabilities and Bluetooth security implementation issues in mobile phones. During this analysis, it was discovered that currently there is no existing security at user's level. The research then continued to analyse the various intrusions caused by these vulnerabilities and the risks that users are involved in. This study of security vulnerabilities and intrusions actually developed the idea of developing a security mechanism at a user's level, where by the user would be able to stop any intrusions from occurring or recognize any intrusions occurring on his or her mobile phone.

As the research progressed, it discussed on existing Bluetooth security products used in mobile phones to improve Bluetooth security. The research revealed that existing Bluetooth security products either have their own limitations in mobile phones or are not fully capable of capturing intrusions specific to mobile phones. As a result, the research proposed a new Bluetooth security solution for mobile phones, namely the Bluetooth Logging Agent (BLA) for overcoming current vulnerabilities, intrusions and enhancing overall Bluetooth security. In doing so, the research also attempted to compare the proposed solution with existing security products.

The research then provided the BLA's detailed design with an analysis of different modules, their communications and the interfacing of the BLA with the Bluetooth module in mobile phones. Chapter 7 explained and illustrated the BLA prototype developed for the proposed design. Subsequently, the prototype was implemented as proof- of- concept to emphasise the significance of this research, to demonstrate the power of BLA in detecting intrusions, and also to prove that it is implementable in a real Bluetooth mobile phones.

8.2 Significance of the BLA prototype

In the BLA prototype, an alert mechanism notifies the mobile phone user whenever there is an attempt of an intrusion or attack. While the alert mechanism adds a slight overhead, it is negligible when compared to mobile phones that run file scanners and antivirus applications in the

background to add a significant overhead to these devices. The alert mechanism employed by the BLA is also extremely useful in that it provides the user with a real time indication of the Bluetooth activities occurring in the mobile phone.

The BLA enables the mobile phone user to participate actively in all Bluetooth transactions. Since the BLA keeps track all the Bluetooth transactions, it allows the user to make flexible decisions such as allowing a basic Bluetooth connection to the user's mobile device from a remote device, thereby safeguarding against the intruders.

The BLA directs Bluetooth transactions only with devices that the mobile phone user permits. This important feature is not available in any of the existing security products. Existing Bluetooth security products, which currently protect mobile phones from intrusion, do not have a facility to identify when a remote device silently establishes a Bluetooth connection to its mobile phone to compromise the device.

Consider a scenario where an existing Bluetooth security product runs in a mobile phone and a remote device attempts to intrude into the mobile phone with a new type of intrusion, unknown to the security product. In this scenario, the security product will not know that there had been an attack and the phone was compromised. However, introduction of the BLA in Bluetooth mobile phones would play a vital role in solving the user's level security problem to a great extent.

The importance of BLA emerges in that it does not allow any hidden Bluetooth communication. The BLA uses its databases extensively to determine the authenticity of a request from a remote device. The databases enable BLA to determine if a request from a remote device is authentic or an intrusion. Whenever there is any Bluetooth transaction request, it alerts the user. The BLA, through the alert mechanism, allows the user to participate in the Bluetooth activities occurring in the mobile phone and thereby creates Bluetooth security awareness among mobile users.

The BLA significantly improves the authentication of the existing Bluetooth security implementation in that it does not authenticate a remote device if the length of the PIN code received is less than 8. Even though the PIN code length can be up to 16 bytes, the current

Bluetooth security implementations in the mobile phones allow PIN codes of shorter lengths, majority of which are 4 bytes in length. As a result, the PIN is easily obtainable by way of a brute force attack.

The BLA prototype, when compared to the existing Bluetooth security solutions, is unique in that it provides a message-by-message logging of each Bluetooth session. This logging feature is advantageous for future use, to retrieve important communication logs and intrusion information. In addition, the logs obtained by the BLA can be used as evidence to claim for major catastrophes resulting from an intrusion.

8.3 Verification and validation of test results

In this research, as outlined in chapter 1 a qualitative approach is used to collect and evaluate the test results of the BLA prototype. Verification and validation is carried out by providing valid and invalid inputs to get the expected output results as per the scenario. This is proved in the prototype and the proof of verification and validation has been provided through log files and screen shots from the prototype.

A Bluetooth Intrusion Simulator (BIS) is implemented along with BLA to simulate the performance of the BLA Prototype implementation. The BIS generates safe requests, intrusions and random requests in order to test, verify, analyse and emulate the power of the BLA. The BIS is extensively discussed in section 7.5 of chapter 7.

The test results are captured in the form of log files and screen shots like as shown in Figure 8.1 and Figure 8.2. A detailed analysis and testing of each type of intrusion attempt and BLA's capability in detecting intrusions is covered Chapter 7.

As illustrated in Figure 8.1, BLA log files give every detail of the Bluetooth session between the Bluetooth mobile phone and the remote Bluetooth device; such as when the current Bluetooth session started, what incoming data was coming in from which device, what was the action taken by BLA and when was the session ended.

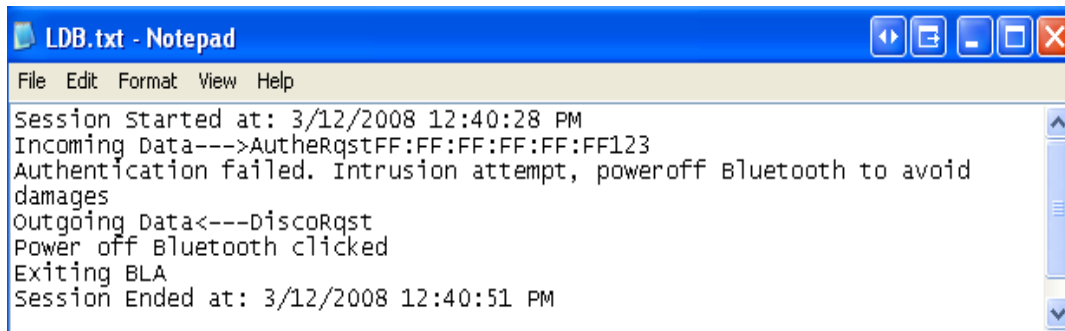


FIGURE 8.1 BLA TEST RESULT: LOG FILE SHOWING INTRUSION DETECTION

Apart from the above capability of logging all the transaction messages, the BLA is also equipped to give instantaneous intrusion alerts to the user as and when it occurs, as shown below.



FIGURE 8.2 BLA TEST RESULT: INTRUSION DETECTION ALERT IN USER INTERFACE

By analysing the test results shown in Chapter 7 in the form of log files and screen shots, it is evident that the BLA prototype is successful and efficient in detecting intrusions. The BLA prototype proves that it is capable of resolving the issues that were addressed in the motivation to conduct this research (Section 1.2 of Chapter 1). Further, a hypothesis can be made that the prototype will be efficient, effective and robust security mechanism if converted to a full fledged

project which suites the requirements of the Bluetooth enabled mobile phones of the popular mobile phone manufacturers such as Nokia, Motorola and Samsung.

The next section discusses about the significance of BLA prototype to mobile phone manufacturers.

8.4 How valuable is BLA to mobile phone manufactures

This research is valuable to mobile phone manufacturers in that they can use it as a ready reference for enhancing security in their Bluetooth-enabled mobile phones, thereby protecting their phones against intrusion. Even though the research focused on improving Bluetooth security in mobile phones, there is scope for further enhancement and modification to improve the Bluetooth security for all Bluetooth-enabled devices such as PCs, laptops, PDAs, headsets and car-kits. Hence, there is room for improving the security of the full spectrum of Bluetooth-enabled devices.

Users of Bluetooth-enabled mobile phones will also greatly benefit from this research, as it will help them to protect their valuable information from intrusion.

The BLA's message logging module, the database module and the intrusion detection and verification module all together contribute to enhance existing security and reduce Bluetooth security issues and vulnerabilities

The next section analyses the feasibility of implementing the prototype in mobile phones.

8.5 Feasibility of implementing the BLA prototype in mobile phones

The Bluetooth communication between the BLA and the remote device is simulated through Socket communication. Hence, the prototype can be easily migrated to real Bluetooth mobile phones. In this research, the proof-of-concept of the BLA is implemented in the Microsoft Smartphone 2003 Emulator. The Socket communication is easily replaceable by a Bluetooth communication when deploying the BLA to Bluetooth mobile phones. To accomplish this, the

BLA prototype must have access to the Application Programming Interfaces (APIs) of the underlying mobile phone manufacturer's Bluetooth Module. In essence, the BLA and Bluetooth Module should be interfaced. Bluetooth messages received by the Bluetooth Module should be routed to the BLA and requests from the BLA should be routed back to the Bluetooth Module. The BLA Database in the prototype should be replaced by a database that is supported in the underlying Bluetooth mobile phone.

The next section concludes the research by pointing out the scope for further research.

8.6 Scope for future research

The BLA prototype may be further enhanced with a rules database. This can be used to store criteria for enabling the Bluetooth transaction with the device under consideration. A Rule Processing Module (RPM) may be incorporated accordingly to the Intrusion Detection and Verification Module (IDVM), to process the rules database. The current BLA mobile phone user interface may be slightly changed to present the user with an option to enter new rules. The log messages obtained by BLA may also be automated to derive new rules based on existing log messages. The rules database may also be updated dynamically.

Further research may analyse the feasibility of publishing intrusion logs obtained from the logging database to peer Bluetooth devices or to the Bluetooth Local Area Network (LAN) access points. In doing so, the BLA component in those devices will be useful in blacklisting intruders and updating their rules.

Bibliography

- [1] Ann Cavoukian; Wireless Communication Technologies: Safeguarding Privacy & Security; 2007; http://www.ipc.on.ca/images/Resources/up-1fact_14_e.pdf;
Last Accessed: 2008/09/09
- [2] Hewlett-Packard Development Company, L.P; Wireless Technology; 2006;
http://h20331.www2.hp.com/Hpsub/downloads/Wireless_Technology.pdf;
Last Accessed: 2008/09/09
- [3] Entrepreneurial Programming And Research On Mobiles;
Massachusetts Institute of Technology; 2008;
<http://web.mit.edu/eprom/whyafrika.html>; Last Accessed: 2008/09/09
- [4] Jonathan Fildes; Mobile web gears up for lift-off; BBC News; 2006;
<http://news.bbc.co.uk/1/hi/technology/5015856.stm>; Last Accessed: 2008/09/09
- [5] Paul Miller, Engadget; Sony Ericsson and Fossil team up for Bluetooth Watch; 2006;
<http://www.engadget.com/2006/09/28/sony-ericsson-and-fossil-team-up-for-bluetooth-watch/>;
Last Accessed: 2008/10/07
- [6] Catharina Candolin; Security Issues for Wearable Computing and Bluetooth Technology; University of Technology, Finland; 2000;
<http://citeseer.ist.psu.edu/cache/papers/cs/2438/http:zSzzSzwww.tml.hut.fizSz~candolinSzPublicationszSzBTzSzbtwearable.pdf/candolin00security.pdf>; Last Accessed: 2008/09/09
- [7] Collin Mulliner; Security and Privacy Issues of Wireless Technologies; CS595M Wireless Technology, New Applications and Social Interaction; 2005;

<http://www.cs.ucsb.edu/~almeroth/classes/tech-soc/2005-Fall/11-01.pdf>;

Last Accessed: 2008/09/09

[8] Matt Hartley; Mobile Lifestyle, Bluetooth alleged to be source of UK crime wave; 2005; <http://www.lockergnome.com/nexus/mobile/2005/06/16/bluetooth-alleged-to-be-source-of-uk-crime-wave/#more-1238>;

Last Accessed: 2008/09/09

[9] Marek Bialoglowy; Bluetooth Security Review, Part 2; 2006;

<http://www.securityfocus.com/infocus/1836>; Last Accessed: 2008/09/09

[10] X-Force Threat Insight Quarterly; Wireless Technology; 2006;

http://documents.iss.net/ThreatIQ/ISS_XFTIQ_Q106.pdf; Last Accessed: 2008/09/09

[11] Megha Banduni; Mobile Enterprise, Secure mobility; 2001;

<http://www.networkmagazineindia.com/200607/coverstories04.shtml>;

Last Accessed: 2008/09/09

[12] Ppcsg; First PC/Phone Crossover Virus Found - Cardtrp !; 2005;

<http://www.ppcsg.com/index.php?showtopic=60280>; Last Accessed: 2008/09/09

[13] Celeste Biever; New Scientist; New hack cracks secure Bluetooth Devices; 2005;

<http://www.newscientist.com/article.ns?id=dn7461>; Last Accessed: 2008/10/07

[14] Adam Laurie and Ben Laurie; Serious flaws in Bluetooth security lead to disclosure of personal data; A.L. Digital; 2005;

<http://www.thebunker.net/security/bluetooth.htm>; Last Accessed: 2008/09/09

[15] Jun-Zhao Sun, Douglas Howie, Antti Koivisto, And Jaakko Sauvola; Design, Implementation, And Evaluation Of

Bluetooth Security; MediaTeam; University of Oulu, Finland; 2004;

<http://www.mediateam.oulu.fi/publications/pdf/87.pdf>; Last Accessed: 2008/09/09

[16] Interop; Bluetooth® Wireless Awareness Soars Among Consumers; 2006;

<http://www.interop.ru/?page=newsview&id=109&offset=0&language=eng>;

Last Accessed: 2008/09/11

[17] Bonphi Technology Limited; Bluetooth Knowledge; 2006;

http://www.bonphi.com/down/bluetooth_knowledge.pdf; Last Accessed: 2008/09/11

[18] Bluetooth Specification Version 1.1; 2008;

<https://www.bluetooth.org/spec>; Last Accessed: 2008/09/11

[19] Thomas Muller; Bluetooth Security Architecture Specification, Version 1.0; 1999;

http://bluetooth.com/Bluetooth/Technology/Building/Research/Bluetooth_Security_Architecture.htm; Last Accessed: 2008/09/11

[20] Greg Day; vnunet.com; 2006;

<http://www.vnunet.com/vnunet/news/2154875/major-mobile-virus-attack>;

Last Accessed: 2008/09/11

[21] Eugene H.Spafford; Computer Viruses as Artificial Life; Purdue University;

1994; <http://homes.cerias.purdue.edu/~spaf/tech-reps/985.pdf>; Last Accessed: 2008/09/11

[22] Anders Edlund; Popularity of Bluetooth, Bluetooth Wireless Technology 2005 Update; 2005; Bluetooth Special Interest Group;

<http://www.touchbriefings.com/pdf/1433/Edlund.pdf>; Last Accessed: 2008/09/11

- [23] Answers.com; 2008;
<http://www.answers.com/topic/trojan-horse-computing?cat=technology>;
Last Accessed: 2008/09/11
- [24] M.M Pillai, Jan Eloff, H.S Venter; An approach to build an intrusion detection system using Genetic Algorithms; University of Pretoria; ACM International Conference Proceeding Series; Vol. 75 ; 2004;
<http://portal.acm.org/citation.cfm?id=1035080>; Last Accessed: 2008/09/11
- [25] Mikhail Gordeev; Intrusion Detection Techniques and Approaches; 2004;
<http://www.ict.tuwein.ac.at>; Last Accessed: 2008/09/11
- [26] Aurobindo Sundaram; An Introduction to Intrusion Detection; 2001;
<http://www.acm.org>; Last Accessed: 2008/09/11
- [27] Rebecca Bace and Peter Mell; Intrusion Detection Systems; 2004;
<http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf>; Last Accessed: 2008/09/11
- [28] Oxford English Dictionary; 2008; <http://www.oed.com>; Last Accessed: 2008/09/11
- [29] Jennifer Bray and Charles F Sturman; Bluetooth™ Connect Without Cables; Publisher: Prentice Hall; 2 edition; 2002;
<http://www.amazon.co.uk/Bluetooth-1-1-Connect-Without-Cables/dp/0130661066>;
Last Accessed: 2008/09/11
- [30] Dee M. Bakker and Diane McMichael Gilster; Bluetooth End to End; Publisher: John Wiley & Sons; 2002;
<http://www.amazon.co.uk/Bluetooth-End-Dee-M-Bakker/dp/0764548875>;
Last Accessed: 2008/09/11

- [31] Bluetooth Specification Version 1.2; 2008; <https://www.bluetooth.org/spec>;
Last Accessed: 2008/09/11
- [32] Bluetooth SIG; About the Bluetooth SIG; 2008;
<http://www.bluetooth.com/Bluetooth/SIG/>; Last Accessed: 2008/09/11
- [33] Kenneth Carey, R.A. Guinee and Fergus O' Reilly; Bluetooth-enabled
Wireless Mouse and Keyboard Interconnectivity; Cork Institute of Technology;
2008; <http://citeseer.ist.psu.edu/507721.html>; Last Accessed: 2008/09/11
- [34] Jaap C.Haartsen and Svenmattisson;
Bluetooth-A New Low Power Radio Interface Providing Short Range
Connectivity; IEEE; 2008;
<http://citeseer.ist.psu.edu/haartsen00bluetooth.html>; Last Accessed: 2008/09/11
- [35] David Espinosa Alfaro; Simulation of Bluetooth™ Scattemet for battery life
optimization; Mälardalen University; 2006;
<http://www.diva-portal.org/mdh/opus/publication.xml?id=1909>; Last Accessed: 2008/09/11
- [36] Riku Mettala; Bluetooth Protocol Architecture, Version 1.0; 1999;
http://www.bluetooth.com/NR/rdonlyres/7F6DEA50-05CC-4A8D-B87B5AA02AD78EF/0/Protocol_Architecture.pdf; Last Accessed: 2008/09/11
- [37] Au-System; Bluetooth™ White Paper 1.1; 2000;
<http://whitepapers.techrepublic.com.com/abstract.aspx?docid=21120>;
Last Accessed: 2008/09/11
- [38] Protocol Stack; Tutorial-Reports.com; 2008;
<http://www.tutorial-reports.com/wireless/bluetooth/protocolstack.php?PHPSESSID=b38fe4559a113df5a6b>; Last Accessed: 2008/09/11

- [39] Bluetooth White Paper 1.1; Au-System; 2000;
<http://www.ausystem.com/>; Last Accessed: 2008/09/11
- [40] Bluetooth Tutorial – Profiles; Palowireless Bluetooth Resource Center; 2008;
<http://www.palowireless.com/infotooth/tutorial/profiles.asp>; Last Accessed: 2008/09/11
- [41] Specification of the Bluetooth System, Wireless connections made easy, Profiles; v1.1
Voting Draft; 2001; <http://www.bluetooth.com>; Last Accessed: 2008/09/11
- [42] Stollmann; Communications-ready for integration; 2008;
[http://www.stollmann.de/template/index_e.php3?
flag=bt_tut_e¶=bt_tut_tech_e](http://www.stollmann.de/template/index_e.php3?flag=bt_tut_e¶=bt_tut_tech_e); Last Accessed: 2008/09/11
- [43] Brent A Miller; Future Applications for Bluetooth™ Wireless Technology;
2001; <http://www.informit.com/articles/article.aspx?p=24243&seqNum=1>;
Last Accessed: 2008/09/11
- [44] William Stallings; Introduction to Bluetooth; informIT; 2001;
<http://www.informit.com/articles/article.aspx?p=23760>; Last Accessed: 2008/09/11
- [45] David Blankenbeckler; An Introduction to Bluetooth;
Wireless Developer Network; 2001;
<http://www.wirelessdevnet.com/channels/bluetooth/features/bluetooth.html>;
Last Accessed: 2008/09/11
- [46] Six Cool Uses for Bluetooth Beyond the Desktop; Accenture; 2008;
[http://www.accenture.com/Global/Services/By_Industry/Communications/
Access_Newsletter/Article_Index/SixDesktop.htm](http://www.accenture.com/Global/Services/By_Industry/Communications/Access_Newsletter/Article_Index/SixDesktop.htm); Last Accessed: 2008/09/11

- [47] Bluetooth Wireless Networking Explained; The Travel Insider LLC; 2008; <http://www.thetravelinsider.info/roadwarriorcontent/bluetooth.htm>;
Last Accessed: 2008/09/11
- [48] TechRepublic; 10 Benefits of Bluetooth; 2008;
<http://whitepapers.techrepublic.com.com/whitepaper.aspx?docid=178260>;
Last Accessed: 2008/09/11
- [49] Bluetooth - An Overview; Johnson Consulting; 2001;
<http://www.swedetrack.com/images/bluet11.htm>; Last Accessed: 2008/09/11
- [50] Bluetooth interview questions; TechInterviews.com - Q&A from tech companies; 2008;
<http://www.techinterviews.com/?p=172>; Last Accessed: 2008/09/11
- [51] Bluetooth Security; Cybertrust; 2005;
http://www.cybertrust.com/media/white_papers/cybertrust_wp_blue.pdf;
Last Accessed: 2008/09/11
- [52] Nikhil Anand; An Overview of Bluetooth Security; 2001;
<http://citeseer.ist.psu.edu/nikhil01overview.html>; Last Accessed: 2008/09/11
- [53] Tom Karygiannis and Les Owens; National Institute of Standards and Technology, Wireless Network Security 802.11; Bluetooth and Handheld Devices; 2002;
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf;
Last Accessed: 2008/09/11
- [54] Anthony Gauvin; Security for Wireless Computing; 2008;
http://perleybrook.umfk.maine.edu/reports/wireless_insecurity.PDF;
Last Accessed: 2008/09/11

- [55] Jonathan Hassell; SecurityFocus™, Wireless Attacks and Penetration Testing (part 1 of 3); 2004; <http://www.securityfocus.com/infocus/1783>; Last Accessed: 2008/09/11
- [56] Vikram Gupta, Srikanth Krishnamurthy, and Michalis Faloutsos; Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks; 2008; http://www.cs.ucr.edu/~krish/milcom_vik.pdf; Last Accessed: 2008/09/11
- [57] Paul A. Karger, Thomas J. Watson; IBM Research Center; Mashups Legitimize Man-in-the-Middle Attacks: A Position Paper for the 2007 IEEE Web 2.0 Security and Privacy Workshop; 2008; http://seclab.cs.rice.edu/w2sp/2007/papers/paper-141-z_5622.pdf; Last Accessed: 2008/09/11
- [58] Stuart McClure, Joel Scambray and George Kurtz; Hacking Exposed Fifth Edition: Network Security Secrets & Solutions; Publisher: McGraw-Hill Osborne Media edition; 2005; <http://www.amazon.com/Hacking-Exposed-5th/dp/0072260815>; Last Accessed: 2008/09/11
- [59] Christian Gehrman; Bluetooth™ Security White Paper, Bluetooth SIG Security Expert Group; 2005; http://www.bluetooth.com/Bluetooth/Technology/Building/Research/Bluetooth_Security_White_Paper.htm; Last Accessed: 2008/09/11
- [60] Paul Simoneau; The OSI Model: Understanding the Seven Layers of Computer Networks; Expert Reference Series of White Papers; Global Knowledge; 2006; http://courses.cs.tamu.edu/pooch/463_spring2008/BOOKS/WP_Simoneau_OSIModel.pdf; Last Accessed: 2008/09/11

- [61] Robert Morrow; Bluetooth: Operation and Use; Publisher: McGraw-Hill Professional; 1st edition; 2002; <http://www.amazon.com/Bluetooth-Operation-Use-Robert-Morrow/dp/007138779X>; Last Accessed: 2008/09/11
- [62] Gregory Lamm, Gerlando Falauto, Jorge Estrada, Jag Gadiyaram; Bluetooth Wireless Networks Security Features, University of Virginia Information & Technology; 2001; [http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2A2\(26\).pdf](http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2A2(26).pdf); Last Accessed: 2008/09/11
- [63] Marjaana Träskbäck; Security of Bluetooth: An overview of Bluetooth Security; Department of Electrical and Communications Engineering; 2008; <http://citeseer.ist.psu.edu/400595.html>; Last Accessed: 2008/09/11
- [64] Jim Rendon; Protecting phones, handhelds from attack; TechTarget; 2004; http://searchmobilecomputing.techtarget.com/news/interview/0,289202,sid40_gci955283,00.html; Last Accessed: 2008/09/11
- [65] Andrew Lockhart; Wireless Vulnerabilities & Exploits, BlueSnarf++; WVE™; Network Chemistry; 2005; <http://www.wirelessve.org/entries/show/WVE-2005-0006>; Last Accessed: 2008/09/11
- [66] Kim Zetter; Security Cavities Ail Bluetooth; WIRED; CondéNet, Inc.; 2004; <http://www.wired.com/politics/security/news/2004/08/64463>; Last Accessed: 2008/09/11
- [67] James Lewis; Bluetooth Security; 2005; <http://islab.oregonstate.edu/koc/ece478/05Report/Lewis.pdf> ; Last Accessed: 2008/09/11
- [68] Jennifer Thom-Santelli, Alex Ainslie, and Geri Gay; A Study of Bluejacking Practices; Cornell University, HCI Group; 2007; <http://www.people.cornell.edu/pages/jt17/chibluejack.pdf> ; Last Accessed: 2008/09/11

- [69] Bluetooth SIG; Security Q & A; 2008; http://www.bluetooth.com/NR/exeres/2F0D2E9A-295B-4D9E-ABDA-8E33BFA2E399_frameless.htm?NRMODE=Published;
Last Accessed: 2008/09/11
- [70] BlueSnarf™; trifinite.stuff; trifinite.group; 2008;
http://trifinite.org/trifinite_stuff_bluesnarf.html; Last Accessed: 2008/09/11
- [71] Andreas Becker; Bluetooth Security & Hacks; Seminar ITS; 2007;
http://www.crypto.rub.de/imperia/md/content/seminare/itsss07/slides_bluetooth_security_and_hacks.pdf; Last Accessed: 2008/10/07
- [72] BlueSnarf++™; trifinite.stuff; trifinite.group; 2008;
http://trifinite.org/trifinite_stuff_bluesnarfpp.html; Last Accessed: 2008/09/11
- [73] BlueBump™; trifinite.stuff; trifinite.group; 2008;
http://trifinite.org/trifinite_stuff_bluebump.html; Last Accessed: 2008/09/11
- [74] Adam Laurie, Marcel Holtmann, and Martin Herfurt; Wireless Vulnerabilities & Exploits, BlueBump; WVE™; 2005;
<http://www.wirelessve.org/entries/show/WVE-2005-0012>; Last Accessed: 2008/09/11
- [75] BlueDump™; trifinite.stuff; trifinite.group; 2008;
http://trifinite.org/trifinite_stuff_bluedump.html; Last Accessed: 2008/09/11
- [76] Konstantin Saproonov; Kaspersky Lab; Viruslist.com: Bluetooth, Bluetooth Security and New Year War-nibbling; 2006;
<http://www.viruslist.com/en/analysis?pubid=181198286>; Last Accessed: 2008/09/11
- [77] HeloMoto; trifinite.stuff; trifinite.group; 2008;
http://trifinite.org/trifinite_stuff_helomoto.html; Last Accessed: 2008/09/11

- [78] Car Whisperer; trifinite.stuff; trifinite.group; 2008;
http://trifinite.org/trifinite_stuff_carwhisperer.html; Last Accessed: 2008/09/11
- [79] RedFang 2.5; Help Net Security; 2008;
<http://www.net-security.org/software.php?id=519>; Last Accessed: 2008/10/07
- [80] Cabir; F-Secure Malware Information Pages; 2006; F-Secure Corporation;
<http://www.f-secure.com/v-descs/cabir.shtml>; Last Accessed: 2008/09/11
- [81] Mary Landesman; Antivirus Software, Cabir worm bluejacks cellphones;
About, Inc.; 2008; <http://antivirus.about.com/od/wirelessthreat1/a/cabir.htm>;
Last Accessed: 2008/09/11
- [82] Tim Gray; New Cabir Variants are Spreading Fast: Code for virus that hits
Symbian-based cell phones released; 2004;
<http://www.internetnews.com/security/article.php/3452981>; Last Accessed: 2008/09/11
- [83] Paul Roberts; Two new Cabir mobile phone worms spotted: Worm source code
may have been released on the Internet; 2004;
<http://www.computerworld.com/newsletter/0,4902,98578,00.html?nlid=SEC2>;
Last Accessed: 2008/09/11
- [84] Jarno Niemela; F-Secure Virus Descriptions: Mabir.A; F-Secure Corporation;
2005; <http://www.f-secure.com/v-descs/mabir.shtml>; Last Accessed: 2008/09/11
- [85] F-Secure Malware Information Pages: Lasco.A; F-Secure Corporation; 2006;
http://www.f-secure.com/v-descs/lasco_a.shtml; Last Accessed: 2008/09/11
- [86] F-Secure Malware Information Pages: Commwarrior; F-Secure Corporation;
2008; <http://www.f-secure.com/v-descs/commwarrior.shtml>; Last Accessed: 2008/09/11

- [87] Jeremy Kirk; InfoWorld: Mobile worm variant causes alarm; IDG Network; 2006; http://www.infoworld.com/article/06/08/04/HNmobiworm_1.html;
Last Accessed: 2008/09/11
- [88] Ollie Whitehouse; War Nibbling: Bluetooth Insecurity; 2003;
http://www.rootsecure.net/content/downloads/pdf/atstake_war_nibbling.pdf;
Last Accessed: 2008/09/11
- [89] @stake Inc; 2008;
<http://www.atstake.com>; Last Accessed: 2008/09/11
- [90] The Linux Kernel Archives; 2008; <http://www.kernel.org/>; Last Accessed: 2008/09/11
- [91] BlueZ Official Linux Bluetooth protocol stack; BlueZ Project; 2008;
<http://www.bluez.org/>; Last Accessed: 2008/09/11
- [92] vmware; VMware, Inc.; 2008; <http://www.vmware.com/>; Last Accessed: 2008/09/11
- [93] IBM – T30 OEM; IBM, Inc.; 2008; <http://www.ibm.com/>; Last Accessed: 2008/09/11
- [94] TDK USB Bluetooth Adapter, TDK, Inc.; 2008
<http://www.tdksystems.com/products/bluetoothchoice.asp?id=1>; Last Accessed: 2008/09/11
- [95] A.Veeraraghavan and A.J.Elbert; Computerworld Mobile & Wireless:
Securing your Bluetooth devices; University of Massachusetts Lowell; 2008;
[http://www.computerworld.com/mobiletopics/
mobile/story/0,10801,89495,00.html?SKC=mobile-89495](http://www.computerworld.com/mobiletopics/mobile/story/0,10801,89495,00.html?SKC=mobile-89495); Last Accessed: 2008/09/11
- [96] Yaniv Shaked and Avishai Wool; Cracking the Bluetooth PIN; 2005;
<http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/>; Last Accessed: 2008/09/11

- [97] Sarah Hicks; Best practices for securing mobile devices; TechTarget; 2006;
http://searchmobilecomputing.techtarget.com/generic/0,295582,sid40_gci1163542,00.html; Last Accessed: 2008/09/11
- [98] AirDefense™; Bluetooth Monitoring; AirDefense, Inc.; 2008;
<http://www.airdefense.net/products/bluewatch/index.php>; Last Accessed: 2008/09/11
- [99] Red-M (Communications); Managing Mobility, Enterprise Secure Wireless Control A Red-M Paper; 2004; <http://www.red-m.com/>; Last Accessed: 2008/09/11
- [100] Victor R. Garza; Techworld: Red-M Red-Detect wireless IDS review A wireless IDS that fights back; Infoworld, IDG; 2004;
<http://www.techworld.com/reviews/index.cfm?reviewid=196>;
Last Accessed: 2008/09/11
- [101] Wireless Network Tools: Bluetooth Wireless Personal Area Network Audit and Monitoring Tools; Nsasoft llc; 2000;
<http://www.wirelessnetworktools.com/>; Last Accessed: 2008/09/11
- [102] AirMagnet: Your Wireless Network Assurance; AirMagnet, Inc; 2008;
http://www.airmagnet.com/news/press_releases/2005/10262005.php?zoom_highlight=Bluesweep; Last Accessed: 2008/09/11
- [103] Jeff Dixon; Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy; 2008;
http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf;
Last Accessed: 2008/09/11

- [104] Greg Sandoval; Mobile working Toolkit Sony Ericsson phones vulnerable to Bluetooth attack; ZDNet.co.uk; CNET Networks, Inc; 2006;
<http://news.zdnet.co.uk/hardware/0,1000000091,39251734,00.htm>;
Last Accessed: 2008/09/11
- [105] Marek Bialoglowy; Bluetooth Security Review, Part 1; 2005;
<http://www.securityfocus.com/infocus/1830>; Last Accessed: 2008/09/11
- [106] Bluetooth; 2005; <http://www.loosewireblog.com/bluetooth/index.html>;
Last Accessed: 2008/09/11
- [107] Addressing the Challenges of Updating Software and Firmware on Mobile Phones Over the Air; rend bend software; 2008;
<http://www.redbend.com/pdf/AddressingTheChallenge.pdf>;
Last Accessed: 2008/09/11
- [108] Trend Micro Mobile Security provides integrated mobile phone protection for device owners, mobile operators; Global Research Partners; 2008;
<http://www.itweb.co.za/office/securedata/0503310835.htm>; ; Last Accessed: 2008/09/11
- [109] Symantec Mobile Security; 2008;
<http://www.symantec.com/norton/products/overview.jsp?pcid=is&pvid=sms40symb>;
Last Accessed: 2008/09/11
- [110] F-Secure Mobile Security; 2008; <http://mobile.f-secure.com/productinfo/>;
Last Accessed: 2008/09/11
- [111] McAfee Mobile Security; 2008;
http://www.mcafee.com/us/enterprise/products/mobile_security/security_enterprise.html; Last Accessed: 2008/09/11

[112] Gold Lock™; 2008;

<http://www.gold-lock.com/?gclid=CKGAuL2t4I0CFQMfEgodjF3BmQ>;

Last Accessed: 2008/09/11

[113] Sophos Mobile Security™; 2008;

<http://www.sophos.com/products/enterprise/endpoint/security-and-control/mobile/>; Last Accessed: 2008/09/09

[114] Roger S Pressman; Software Engineering: A practitioners approach;

Publisher: McGraw-Hill Science/Engineering/Math; Sixth edition; 2004;

<http://www.amazon.com/Software-Engineering-Practitioners-Roger-Pressman/dp/007301933X>; Last Accessed: 2008/10/1

[115] Quantitative and Qualitative Research;

<http://www.socsci.uci.edu/ssarc/pcs/webdocs/QuantitativeandQualitativeResearch.pdf>;

Last Accessed: 2009/02/26

[116] Orit Hazzan; Qualitative Research in Software Engineering;

http://edu.technion.ac.il/faculty/orith/homepage/FrontierColumns/OritHazzan_SystemDesign_Frontier_Column8.pdf; Last Accessed: 2009/02/26

[117] Beverley Hancock; An Introduction to Qualitative Research;

<http://www.trentdsu.org.uk/cms/uploads/Qualitative%20Research.pdf>;

Last Accessed: 2009/02/26

Appendix – Prototype Implementation Disk

The attached CD contains the source code and executables of the Bluetooth Logging Agent (BLA) prototype and the Bluetooth Intrusion Simulator (BIS).

Please refer to the 'Readme.txt' from the 'Prototype Implementation' folder of the disk to launch BLA and BIS and set up their mutual communication.