SECURITY APPLICATION IN BLUETOOTH TECHNOLOGY

Ismaila, I. & Morufu, O.
Department of Cyber Security Science
Federal University of Technology, Minna, Niger State. Nigeria
E-mail: Ismi_idris@yahoo.co.uk[1] & lerejide@gmail.com[2]

Abstract

Before implementing some new technologies, a simulation program is usually designed to first demonstrate how the technology works. If it works perfectly, then the real implementation takes place, but if it fails, correction is made before the implementation. In this paper, we shall examine a program that demonstrates security application in Bluetooth technology. We shall also discuss how Bluetooth technology provides security measures at both the application layer and the data link layer. Finally we look at the two kinds of inherent features that make attacks more difficult.

Keyword: Bluetooth, Security, Network, Protocol, Application

Introduction

Over the years wireless technology has been promising a world without wires but look around, you will see lots of interconnecting wires. Look at your good old PC isn't it cluttered with wires? Wires connecting your PC to the printer, scanner, mouse, keyboard etc. It is a total mess. Some initial solutions using short range wireless connectivity with frequencies in the scientific, industrial and medical bands have resulted in some success in reducing this mess but there was very little scope for interoperability between devices due to their proprietary standards. A printer and a laptop could only be interconnected if they are bought from the same manufacturer. These and a host of other problems made these initiatives less feasible. But this is going to change for better. Bluetooth technology, originally developed by Ericsson but now controlled by the Bluetooth SIG (Special Interest Group), a consortium of 1000+ companies, offers the promise of a global standard for short-range wireless communication between an ever-increasing variety of devices and peripherals.

The fancy name for this short-range wireless connectivity protocol comes from the 10th century Viking king, Harald Bluetooth, who united Scandinavia after years of fighting and destructive competition. Today Bluetooth is following the same symbolic path to establish a common platform for communicating between disparate types of computing devices. Beyond the colorful origin of its name, Bluetooth is a compelling new radio technology that opens up a new world of opportunity for uniting and empowering mobile device users.

Bluetooth Specification in Brief

- Maximum data rate 750 kbps
- Master-Slave communication model.
- Operating Frequency is globally available 2.4-2.5 GHz free ISM band with spread spectrum technology
- Frequency hopping, full duplex signal at 1600 hops/sec.
- 79 frequencies with 1 MHz interval to provide noise immunity
- A device can be master of 7 slaves forming a network called piconet. Several piconets can interconnect to form a large network called scatternet.
- Royalty free standard

Bluetooth Protocol Overview

The Bluetooth protocol stack, can be divided into four layers according to their purpose, in the following ways:

1. Bluetooth Core Protocols, including Baseband, LMP, L2CAP, and SDP, comprise exclusively Bluetooth-specific protocols developed by the Bluetooth SIG that are required by most of the Bluetooth devices.
2. Cable Replacement Protocol, i.e. RFCOMM protocol, is based on the ETSI TS 07.10 that emulates serial line control and data signals over Bluetooth Baseband to provide transport capabilities for upper level services.
3. Telephony Control Protocols, including TCS Binary and AT-commands, are used to define the call control signaling, mobility management procedures, and multiple usage models for the Bluetooth devices to establish the speech and data calls and provide FAX and modem services.
4. Adopted Protocols, including PPP, UDP/TCP/IP, WAP, WAE, etc. Due to the open nature of the Bluetooth specification, additional protocols (e.g., HTTP, FTP, etc.) can be accommodated in an interoperable fashion.
5. Host Controller Interface (HCI), i.e. the boundary between hardware and software, provides a uniform command interface to access capabilities of hardware, e.g. Baseband controller, link manager, control and event registers.

Bluetooth Protocol Stack

The layers of Cable Replacement, Telephony Control, and Adopted Protocols form the application-oriented protocols that enable applications to run over the Bluetooth core protocols. Not all applications make use of all the protocols, applications run over one or more vertical slices of this protocol stack. In other words, applications may run over different protocol stacks (Bluetooth SIG, 2002). Nevertheless, each one of these different protocol stacks uses a common Bluetooth data link and physical layer, i.e. Bluetooth core protocols, including:

(i) Baseband. Based on the physical radio link, the Baseband can form the piconet between Bluetooth units and decide the roles of master and slave in the piconet. The Baseband provides physical links of both Synchronous Connection-Oriented (SCO) and Asynchronous Connectionless (ACL) to support the transmission of data and/or audio with corresponding packets (Java Community Process, 2001). Other functions include error correction, link management and control, audio transmission, etc.

(ii) Link Manager Protocol (LMP). The Bluetooth protocol LMP is responsible for link set-up between Bluetooth devices. This includes security aspects and the control and negotiation of Baseband packet sizes. Furthermore, it controls the power modes and duty cycles of the Bluetooth radio device, and the connection states of a Bluetooth unit in a piconet.

(iii) Logical Link Control and Adaptation Protocol (L2CAP). The protocol of L2CAP provides connection-oriented and connectionless data services to the upper layer protocols over the Baseband, with protocol multiplexing capability, segmentation and reassembly operation, and group abstractions, which permits higher level protocols and applications to transmit and receive L2CAP data packets. L2CAP is defined only for ACL links (Java Community Process, 2001).

(iv) Service Discovery Protocol (SDP). Using SDP to discover services is a crucial part of the Bluetooth framework and provides the basis for all the usage models. SDP query device information, services information, and the characteristics of the services, according to which a suitable connection between two or more Bluetooth devices can be established.

Security Framework

The Bluetooth technology provides security measures at both the application layer and the link layer. Besides there are two kinds of inherent features that make attacks more difficult.

A hop selection mechanism of up to 1600 hops/sec is employed to avoid the interference from external or other piconets. An automatic output power adaptation scheme is also included in the standard for the low power consumption of light-weight mobile devices, which can reduce the radio spread range for data transmission exactly according to requirements based on the detected intensity. A total of three different information security objectives are to be reached one or all. Confidentiality means that the data can only be used by authorized users and/or parties. Integrity means that the data cannot be modified during transfer and stored by adversaries. Availability means that the data is always available for authorized use (The Open Group, 1997). Typical attacks to a wireless network include DoS (Denial-of-Service), man-in the middle, spoofing, impersonating, session hijacking, eavesdropping, etc. Bluetooth launches three main techniques to achieve security features, including:

(i) Encryption: The process of transforming data into a form that it cannot be understood without a key. Both data and control information can be encrypted.

(ii) Authentication: The process of verifying 'who' is at the other end of the link. Authentication is performed for both devices and users.

(iii) Authorization: The process of deciding if a device is allowed to have access to a service. Authorization always includes authentication.

Security Modes

Each Bluetooth device can operate on one of the 3 security modes. First mode is a non secure mode in which a Bluetooth device shall never initiate any security procedure. Second mode is service-level enforced security where a device does not initiate security procedures before channel establishment at L2CAP level, and whether to initiate or not depends on the security requirements of the requested channel or service (Bluetooth SIG, 2003). Third mode is a link-level enforced security in which a Bluetooth device shall initiate security procedures before the link set-up at the LMP level is completed. Accordingly, two levels of Bluetooth security scheme can be identified as follows:

Link-level security corresponds to third mode. The Bluetooth device Initiates security procedure before the channel is established. This is the built-in security mechanism and it is not aware of service/application layer security. Second mode corresponds to service-level security. The Bluetooth device initiates security procedures after the channel is established, i.e. at the higher layers. This is a kind of add-in mechanism and is regarded as a practical issue.

Security Levels

Bluetooth allows different security levels to be defined for devices and services. Two security levels can be defined for a device. A trusted device has unrestricted access to all or some specific services. Basically this means that the device has been previously authenticated and marked as “trusted”. An untrusted device has restricted access to services. Usually the device has been previously authenticated but has not been marked as “trusted”. An unknown device is also an untrusted device. Three levels of service security are allowed to be defined so that the requirements for authorization, authentication, and encryption can be set independently, including services that require authorization and authentication, services that require authentication only, and services open to all devices. These three security levels can be described by using the following three attributes:

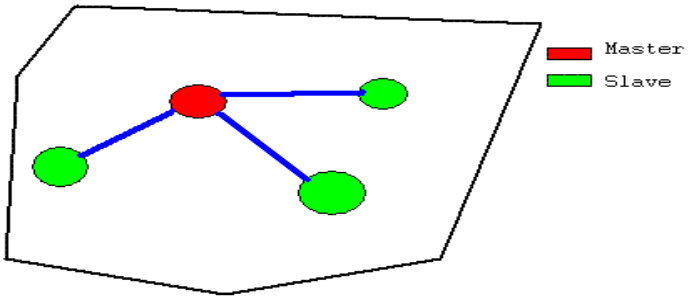
Authorization Required: Access is only granted after an authorization procedure. Only trusted devices would get automatic access.

Authentication Required: The remote device must be authenticated before being able to connect to the application.

Encryption Required: The link between the two devices must be encrypted before the application can be accessed.

How Bluetooth Works

Now a Bluetooth network actually consists of small subnets or piconets. A piconet consists of two or more connected nodes sharing the same channel. Every piconet have one master and up to 7 slaves. There is never a direct transmission between slaves. Rather all communications go through the master.



A Piconet

Two or more connected piconets form a scatternet. To connect piconets simply let them have a node in common. A node may be a slave in one piconet and a master in another. This is the basis for forming ad-hoc networks in Bluetooth.

The core Bluetooth protocol stack contains 5 layers. The radio and baseband layers describe the physical implementation of Bluetooth. It operates on the 2.4GHz frequency. There are 79 1MHz channels and upper and lower guard bands. The technology uses frequency hopping spread spectrum for information transmission with 1600 hops per second. Each channel is occupied for 0.625ms, called a slot and the slots are number sequentially. The master in the piconet determines the frequency hopping sequence and it is a function of the master's address

Conclusion

Conclusively, this paper explores security in Bluetooth technology and also layers in security implementation using Bluetooth technology. Security modes and also security level in Bluetooth technology is also examine.

Further research that will be recommended here is to design a complete simulation that can take care of all the security issues in a mobile ad hoc network including both misused and anomaly detection of intrusions. A real or physical implementation of the simulation on any JAVA enabled mobile phone is also recommended to see in real life how the security features will work physically.

Further research work can also be done to increase the radius covered by Bluetooth to discover devices and transfer data.

References

Bluetooth SIG, (2003). *Bluetooth Network Encapsulation Protocol (BNEP) Specification*, Revision 1.0.

Bluetooth SIG, (2002). *Hardcopy Cable Replacement Profile Interoperability Specification,* Revision 1.0a.

Java Community Process, (2001). J2ME Foundation Profile (JSR-46). Retrieved from http://www.jcp.org/en/jsr/detail?id=46.

The Open group, (1997). DCE 1.1: *Remote Procedure Call,* Appendix A. Document Number C706. Retrieved from http://www.opengroup.org/dce/info/faq-mauney.html