RESEARCH ARTICLE OPEN ACCESS

Bluetooth Security Threats: A Survey

[1]Rajendra kumar , [2]Namrata Dhanda

Department of CSE G I T M Lucknow

Abstract:

Bluetooth technology has part of this modern society. The availability of different mobile phones, game controllers, Personal Digital Assistant (PDA) and other personal computers has made Bluetooth a popular technology for small distance wireless communication. However, as the Bluetooth technology becomes widespread, security protocols are increasing which can be dangerous to the privacy of a user's personal information. The security issues of Bluetooth have been worked on for the last few years. This paper presents security protocols of this technology along with some past security threats reported in the literatures which have been surveyed and summarized in this paper. It also presents some tips that end-users can implement immediately to become more cautious about their private information and future security enhancements that can be implemented in the Bluetooth standard.

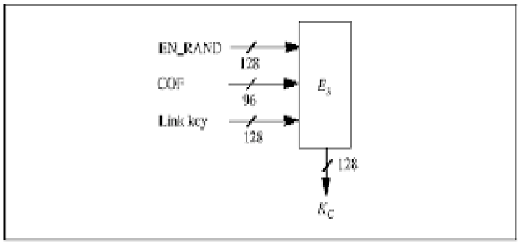
Keywords — **Bluetooth, encryption, security protocols, security threats, Bluetooth advantages..**

Introduction

Bluetooth works on the devices to establish ad hoc networks. Ad hoc networks allow easy connection between devices in the same network area without need of any wired devices. The master system operates and builds the network, including defining the network's frequency hopping scheme. Although one piconet had one master, time division multiplexing allows a slave in one piconet to be master for another piconet simultaneously, hence creating a sequence of networks, called a scatternet. Even the topology gets changes once the device moves away or towards the master device, along with the relationships of the devices in the immediate network.

Encryption concepts

For the encryption routine there are numbers of algorithms are used where the shiphring bit are use to send encrypted bit of data over the air interface. The payload chipred after the CRC bits appended but prior to the FEC encoding. Each packet will chipred separately The chiper algorithm Eo is used to the master Bluetooth address. Master Bluetooth is used 26 bits and the encryption key Kc as input. The Kc is derived by an algorithm E3 form current link key. The ciphering OFfset number and 128-bit number. The COF is find by two ways. One is current key such as master key. Then COF is derived by the master key BD_ADDR. Otherwise the value of COF is derived from ACO from authentication process. The random number issued by the master key before entering encryption process. The real time clock is incremented in slots. The Eo algorithms is re-initialized is start in each new packets. By using clock at least one bit change in one transmission process. Thus the new key stream is initialized at the start at each new packet. For the packet covering in more than the one slots, the Bluetooth clock is found as a first slot is being used for the entire packet.

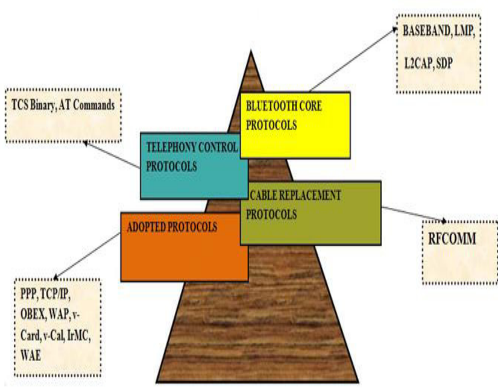


Security protocols

Thus the three basic link level securities are to bee needed:

1. Authorization and authentication
2. Authentication only
3. No Authorization or Authentication – implying services open to all devices

Bluetooth protocol comprises of a number of protocols which can be divided into four categories. Each of these protocols is responsible for specific type of task and stands on its own. In the previous Bluetooth article we talked about the basic terms, the specific values of power, frequency, range and many more. The concept of master, slaves, Pico nets and scatter net forming ad-hoc network. This part of Bluetooth will deal with the protocols responsible for the working of Bluetooth technology. The four categories in which these protocols are divided are shown below:



Bluetooth Core Protocols

Baseband

The baseband worked on the radio frequency based link between Bluetooth devices to form a Pico-net. Information is interchanged within the packets in Bluetooth. A packet is a binary data unit carries the details of user information routed through a computer network. There tow network are operates such as circuit switching and packet switching is used to transfer the packets in the network. Packet-switched networks move data in separate, small blocks packets to the destination address in each packet. When received, packets are arrange in the proper sequence to original message. Circuit-switched networks require dedicated point-to-point connections during calls and used in telephone lines for exchange.

The Link Manager Protocol

The link manager protocol is responsible to manage a link between two Bluetooth devices. This protocol layer is responsible for security issues like authentication, encryption, exchanging and checking the link and encryption keys.

Logical Link Control and Adaptation - Layer

The Bluetooth logical link control and adaptation layer supports higher level multiplexing, segmentation and reassembly of packets and quality of service communication and groups. This layer is not responsible for reliability and uses ARQ to ensure it.

Service Discovery Protocol (SDP)

SDP is the basis for discovery of services on all Bluetooth devices. It is necessary for all Bluetooth models because with SDP device information, services and the characteristics of the services can be queried and after that connection between two or more Bluetooth devices may be established. maybe used in conjunction with the Bluetooth SDP protocol.

Bluetooth security threats

Authentication: Approved the characteristics of communicate procedure base on their Bluetooth gadget address. Bluetooth does not give native client verification.

Confidentiality: prevent information concession caused by eavesdrop by ensuring that only allowed devices can right to use and view transmit information.

Authorization: allow managing resources by ensure that a gadget is official to use a service before permit it to do so.

Advantage of Bluetooth

Cable Replacement: Bluetooth technologies overcome cables at a great extent, such as those that were previously used for secondary devices like mouse, keyboard, printers, etc.

Ease of file sharing: A Bluetooth-enabled device can form a link atmosphere to file sharing capabilities with other Bluetooth devices, such as laptops.

Wireless synchronization: Bluetooth can provide file sharing Bluetooth-enabled devices. For example, synchronization of electronic contacts and calendar using Bluetooth.

Internet connectivity: Internet may well be shared on or after one Bluetooth enabled device to the other.

Conclusion

Most of the people fascinate for the wireless devices. Bluetooth technology is a global standard for wireless connectivity of entire world. This facilitates the replacement of wires or cables and other guided medium used to interconnect between devices. Bluetooth devices are small in size, very low cost in comparison to the other devices, and the utilization of power is very low. Bluetooth can imitate a universal bridge to attach the existing data networks, and also as a mechanism for forming ad-hoc networks. This is designed to operate in noisy frequency environments, the Bluetooth radio uses a morefast acknowledgement and frequency hopping scheme to make the link robust.

References

[1]- Guide to Bluetooth Security, Recommendations of the National Institute of Standards and Technology, Overview of Bluetooth Technology(June 2012)

[2] PairingandAuthenticationSecurityTechnol ogiesinLo wPowerBluetooth (2013 ieee)

[3] Kathrine Aguilar Masagca, An Investigation of Bluetooth Security Threats , BlueBugging: (2011) [4] HariharanRajasekaran, A Leaky Bucket called Smartphone ,2012 IEEE (19 March 2012)

[4] Oman P. and Hagemeister J., ―Metrics for assessing a software system's maintainability, Software Maintenance, 1992, pp.337-334.

[5] Rizvi S.W.A.And Khan R.A., ―Maintainability Estimation Model for Object-Oriented Software in Sannella Design Phase (MEMOOD),‖Journal of Computing, Volume 2, Issue 4, April 2010.

[6] Hincheeranan Alisara and Rivepiboon Wanchai , ―A Maintainability Estimation Model and Tool,‖ International Journal of Computer and Communication Engineering, Vol.1, No.2, july2012.

[7] Hall John M., ―The Maintainability of Object-Oriented Software.

[8] Rosenberg Dr.Linda, Hammer Ted and Shaw Jack, ―Software Metrics and Reliability. [9] EI-Emam, K.EI and Melo, W., "The Prediction of Faulty Classes Using Object-Oriented Design Metrics", National Research Council Canada, Nov. 1999

[10] S. Muthanna, K. Kontogiannis, K. Ponnambalam, and B. Stacey, "A Maintainability Model for Industrial Software Systems Using Design Level Metrics," Proc. 7th Working Conference on Reverse Engineering(WCRE'00), 23 - 25 Nov., 2000, pp. 248 – 256, Brisbane, Australia,2000.