Volume 2, No. 5, Sept-Oct 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

On Security in Bluetooth Wireless Network

Md. Alimul Haque
P.G. Department of Physics
V.K.S. University, Ara, India
E-mail: shadvksu@gmail.com

Abstract: Bluetooth is a way of connecting machines to each other without cables or any physical medium. It is a part of wireless communication as well as mobile communication. It uses radio waves to transfer information, so it is very easily affected by attacks. In this paper we discuss several features of the security of Bluetooth. Here we focus on the security of Bluetooth and Core Bluetooth protocols. This documents provides an overview of wireless personal area networking technology and security looking to reduce the risks associated with Bluetooth Wireless Architecture.

Keywords: Bluetooth, Authentication, Wireless, Encryption.

I. INTRODUCTION

Bluetooth is an open standard for short-range radio frequency communication. It has been designed to easily establish wireless personal area networks (WPAN), often referred to as ad – hoc or peer – to – peer networks. The Bluetooth wireless specification got its name from 10th – century Danish King who used diplomacy to negotiate a true between two feuding factions.

The Bluetooth operates in the world wide unlicensed 2.4 GHz ISM frequency band. Bluetooth devices within 10m of each other can share up to 720 Kbps of capacity. Bluetooth is intended to support an open ended list of applications, including data, audio, graphics and even video. Bluetooth is an increasingly popular technology that enables short-range wireless communication between variety of electronics devices. Its most significant feature is that it allows devices to "talk" wirelessly with one another, eliminating the need for seemingly endless tangle of cords, cables and adapters necessary for a lot of today's technology. [1]

II. SECURITY OF IEEE 8.02.15.1 (BLUETOOTH)

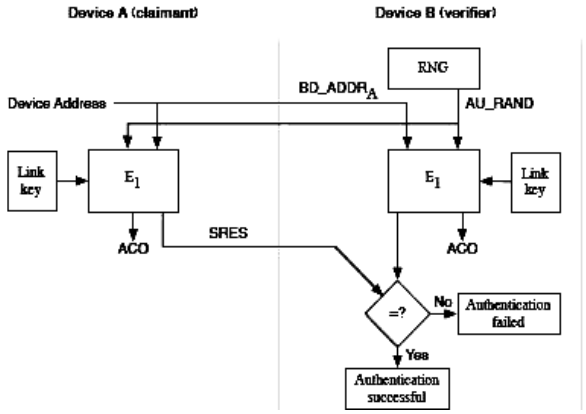
Security for Bluetooth is provided on the various wireless links. The BT standard specifies the following three security services.

- ***a. Authentication:*** This service authenticates the communicating devices. User authentication is not natively provided by Bluetooth.
- ***b. Confidentiality:*** Ensuring that not only authorized devices can access transmitted data, and therefore prevents all kinds of eavesdropping.
- ***c. Authorization:*** As Bluetooth allows the control connected resources (printers, headphones, etc), this service assures a device's authorization before allowing it to do so.[2]

A. Bluetooth Authentication Scheme:

The Bluetooth Authentication scheme uses a "Challenge-response strategy in which 2-more protocol is used to check whether the other party knows the secret key.[3] The protocol uses similar keys, so a successful authentication is based on the fact that both participants share the same key. The steps in the authentication process are following.

a. The claimant transmits its 48-bit address (BD ADDR) to the verifier.
b. The verifier transmits a 128-bit random challenge (AU RAND) to the claimant.
c. The verifier uses the E1 algorithm to compute an authentication response using the address, link key, and random challenge as inputs. The claimant performs the same computation.
d. The claimant returns the computed response, SRES, to the verifier.
e. The verifier compares the SRES from the claimant with the SRES that it computes.
f. If the two 32-bit SRES values are equal, the verifier will continue connection establishment.[4]



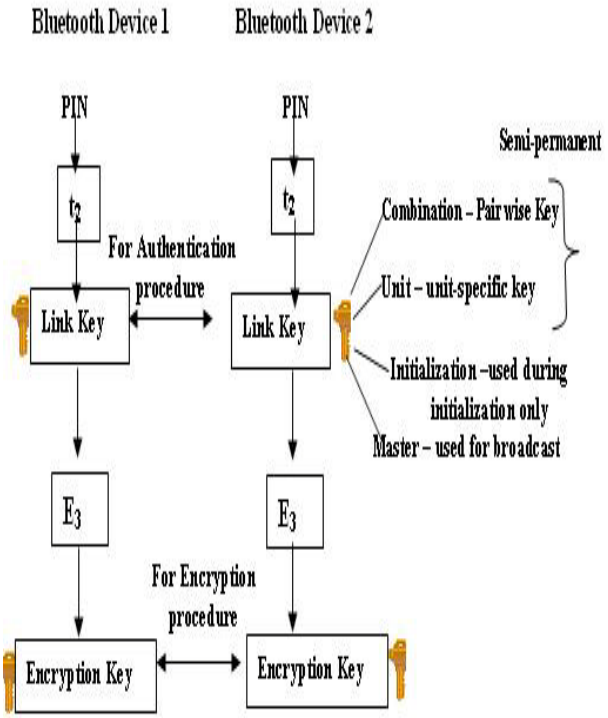
Bluetooth Authentication

B. Link Key Generation – Bluetooth:

The link key is generated during an initialization phase, while two Bluetooth devices that are communicating are "associated" or "bonded." The Bluetooth specification, two associated devices simultaneously derive link keys during the initialization phase when a user enters an identical PIN into both devices. The link key is generated during an initialization phase, while two Bluetooth devices that are communicating are "associated" or "bonded." The

PIN entry, device association, and key derivation are depicted conceptually in Figure.[5]

After initialization is complete, devices automatically and transparently authenticate and perform encryption of the link. It is possible to create a link key using higher layer key exchange methods and then import the link key into the Bluetooth modules.



Bluetooth Key Generation from PIN

C. Security Features of Bluetooth:

Each Bluetooth device can work on one of the three security modes. Depending on whether a device uses a semi link key or a master key, there are several encryption modes available. If a unit key or a combination key is used, broadcast traffic is not encrypted or not. If a master key is used, there are three possible modes.[6.

In Model 1, A device will not initiate any security procedures. In this nonsecure mode, the security functionality (authentication and encryption) is completely bypassed. In effect, the Bluetooth device in Mode 1 is in a "promiscuous" mode that allows other Bluetooth devices to connect to it. This mode is provided for applications for which security is not required, such as exchanging business cards.

In Model 2, The service-level security mode, security procedures are initiated after channel establishment at the Logical Link Control and Adaptation Protocol (L2CAP) level. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode, a security manager (as specified in the Bluetooth architecture) controls access to services and to devices. The centralized security manager maintains polices for access control and interfaces with other protocols and device users. Varying security polices and "trust" levels to restrict access may be defined for applications with different security requirements operating in parallel. Therefore, it is possible to grant access to some services without providing access to other services. Obviously, in this mode, the notion of authorization—that is the process of deciding if device A is allowed to have access to service X—is introduced.

In Model 3, The link-level security mode, a Bluetooth device initiates security procedures before the channel is established. This is a built-in security mechanism, and it is not aware of any application layer security that may exist. This mode supports authentication (unidirectional or mutual) and encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key, a pairing procedure is used when the two devices communicate for the first time.

D. Bluetooth Encryption Scheme:

The Bluetooth specification also allows three different encryption modes to support the confidentiality service.

- ***a. Encryption Mode 1:*** No encryption is performed on any traffic.
- ***b.* Encryption Mode 2:** Broadcast traffic goes unprotected (not encrypted), but individually addressed traffic is encrypted according to the individual link keys.
- ***c.* Encryption Mode 3:** All traffic is encrypted according to the master link key. [7]

E. Bluetooth Trust and Service Levels:

Bluetooth allows two trust levels and three service security levels. Trust levels are trusted and untrusted. Trusted devices have full access to all services provided by the connected devices while untrusted devices only receive restricted access. Service Security Levels allow toconfigure and alter the requirements for authorization, authentication and encryption independently. Bluetooth Service Security Levels.[8]

a. Service Level 1:

Authorization and authentication are required. Trusted devices are allowed to automatically connect to all services. Untrusted devices need manual authorization for all services.

b. Service Level 2:

This level requires authentication only. Access to services is granted only after the authentication procedure.

c. Service Level 3:

Access is granted automatically and to all devices with no authentication required. Trust and service levels allow the definition of policies to set trust relationships and may also be used to initiate user-based authentication.[9] Bluetooth core protocols usually only provide device authentication.

III. CONCLUSION

In the light of this study it seems that Security aspects are very important for wireless technology due to easy access of the attackers to the communication medium. Anyone with appropriate hardware can scan radio communication, log it and use today's powerful computer performance to obtain sensitive information. Bluetooth is

new wireless technology that is changing the enterprise environment. Because it is very low power, short range, lower bandwidth, used for less sensitive applications, and more sparsely used than the other wireless technologies, it is inherently lower risk.

In general, seems to be that the Bluetooth Security Architecture is reasonably robust and granular in its present form and is quite secure even in its default state. However since application developers may or may not choose to incorporate security into application layers, it is possible that the security strength of Bluetooth devices will depend more on making significant changes to the architecture.

IV. REFERENCES

[1]. Bluetooth SIG, Specification of the Bluetooth System: Volume 1, Core, Version 1.1, 2001.

[2]. Gunther Lackner, "Chapter5. Security in IEEE 802.15.1 (Bluetooth)", pp.47, 2011.

[3]. Specification of Bluetooth System Core vol. 1v1.1, Bluetooth Special Interest Group www.bluetooth.com

[4]. Karygiannist,T and Owens,L. "Wireless Network Security 802.11, Bluetooth and Handheld Devices" http://csrc.nist.gov/fasp/FASPDocs/policy-and-procedure/Wireless-Security.pdf.

[5]. Pawan Kumar, "Bluetooth Quality Issues, Threats and Security Tips", International Journal of Computer Science and Communication, Vol.2, No.1, pp.211-213,2011.

[6]. Lu, Y., W.Meier and S.Vaudenay, "The Conditional Correlation Attack. A Pratical Attack on Bluetooth Encryption, Santa Barbara, pp.14-18, 2005.

[7]. Gunther Lackner, "Chapter5. Security in IEEE 802.15.1 (Bluetooth)", pp.53-54, 2011.

[8]. A.Juels. RFID Security and Privacy: A Research Survey. IEEE Journal on Selected Areas in Communiaction, 24(2), pp.381-394, 2006.