International Journal of Security and Its Applications
Vol.8, No.2 (2014), pp.341-352
http://dx.doi.org/10.14257/ijsia.2014.8.2.35

A Design Approach for Wireless Communication Security in Bluetooth Network

Bijoy Kumar Mandal[1], Debnath Bhattacharyya[1] and Tai-hoon Kim[2*]

[1]*Department of Computer Science and Engineering, Faculty of Engineering and Technology, NSHM Knowledge Campus – Durgapur, Durgapur-713212, India*
[2]*Department of Convergence Security, Sungshin Women's University, 249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea*
[1]*{writetobijoy,debnathb}@gmail.com,* [2]*taihoonn@daum.net*
(Corresponding Author)

Abstract

Exponential growth of the volume of Bluetooth-enabled devices indicates that it has become a popular way of wireless interconnections for exchanging information. Bluetooth technology has become an integral part of this modern society. The availability of mobile phones, game controllers, Personal Digital Assistant (PDA) and personal computers has made Bluetooth a popular technology for short range wireless communication. However, as the Bluetooth technology becomes widespread, vulnerabilities in its security protocols are increasing which can be potentially dangerous to the privacy of personal information of user. It is the kind of wireless Ad hoc network. Low cost, low power, low complexity and robustness are the basic features of Bluetooth. It works on Radio frequency. Bluetooth communication range is categorized as high, medium and low depending upon power level. High range of Bluetooth communication is up to 91 meter, medium range is up to 9 meter and low range is up to 1 meter. Bluetooth is a recently proposed protocol for local wireless communication and has become a de facto standard for short-range ad hoc radio connections. Security concern is one of the most important problems delaying the mass adoption of Bluetooth. This article provides a study on the security issues behind the Bluetooth standard. After an overview of the general Bluetooth protocol, a security framework is introduced for the description of the Bluetooth security layout. Then both link-level and service-level security schemes are discussed in detail on the basis of the framework. Some weaknesses of the Bluetooth security strategies are analyzed, together with potential risks and possible attacks against the vulnerabilities. Corresponding countermeasures are also proposed in order to improve the Bluetooth security.

Keywords: *Bluetooth Security, WPAN, PDA, Bluetooth Protocol, Piconet, RF, L2CAP, RFCOMM, LMP*

1. Introduction

Bluetooth [1, 2] is a wireless communication technology for short range communication. It was developed by Ericsson in 1994. It uses short wavelength radio transmissions from mobile or fixed devices. The Bluetooth system operates in the worldwide unlicensed 2.4 GHz ISM frequency band. To make the link robust to interference, it employs a Frequency Hopping (FH) technique, in which the carrier frequency is changed at every packet transmission. To

* Corresponding Author

ISSN: 1738-9976 IJSIA

minimize complexity and to reduce the cost of the transceiver, a simple binary Gaussian frequency shift keying modulation is adopted. In order to allow efficient wideband data transmission the bit rate is 1 Mbps. Two or more Bluetooth units sharing the same channel form a piconet. Within a piconet a Bluetooth unit can be either master or slave. Within each piconet there may be only one master and up to seven active slaves. Any Bluetooth unit can become a master in a piconet. Furthermore, two or more piconets can be interconnected, forming what is called a Scatternet. The connection point between two piconets consists of a Bluetooth unit that is a member of both piconets. A Bluetooth unit can simultaneously be a slave member of multiple piconets, but a master in only one, and can only transmit and receive data in one piconet at a time, so participation in multiple piconets has to be on a time division multiplex basis.

The primary design goal of Bluetooth is a cable replacement protocol for wireless connectivity. Now it has extended to include the application scenarios of both voice/data access points and personal ad hoc networks. A diverse set of wired and wireless devices are Bluetooth connectable, including office appliances, *e.g.*, desktop PCs, printers, projectors, laptops, and PDAs; communication appliances, *e.g.*, speakers, handsets, pagers, and mobile phones; home appliances, *e.g.*, DVD players, digital cameras, cooking ovens, washing machines, refrigerators, and thermostats. Bluetooth is suitable for a wide range of applications, *e.g.*, wireless office and meeting room, smart home and vehicle, intelligent parking, electrical paying and banking. Bluetooth is a de facto standard for ubiquitous devices to achieve the pervasive connectivity by low-power, short-range, low-cost embedded radio. The normal transmitting power is 1mW (0dBm) and the option is100mW (-30 to +20dBm). The normal range is 10m and the optional one 100m. Power consumption is from 20mA to 30mA on different operating states. The cost of a single-chip Bluetooth solution expects to be around $5 per device. Bluetooth adopts a master-slave architecture to form an ad hoc wireless network named piconet. A master in a piconet may communicate with up to seven active slaves. Several connected piconets can further form a scatternet. Bluetooth specification is a free open standard and the latest version 1.1 was approved in February 2001 [3, 4]. The Wireless Personal Area Network (WPAN) standard, developed by the IEEE 802.15 Working Group [5], is based on the Bluetooth. Security is always one of the most important issues to any communication technique. In a wireless scenario, such as the Bluetooth, this problem becomes more severe for the totally open-air transmission. The aim of this paper is to provide a study on Bluetooth security, including an overview of the fundamentals, an introduction of implementation issues, and an analysis of potential vulnerabilities. The Bluetooth system provides full-duplex transmission using a slotted time division duplex (TDD) scheme where each slot is 0.625 ms long. Master-to-slave transmissions always start in an even-numbered time slot, while slave-to-master transmissions always start in an odd-numbered time slot. An even-numbered time slot and its subsequent odd-numbered time slot together are called a frame. There is no direct transmission between slaves in a Bluetooth piconet; transmission is only between a master and a slave, and vice versa. The communication within a piconet is organized such that the master polls each slave. A slave is only allowed to transmit after the master has polled it. The slave will then start its transmission in the slave-to-master time slot immediately following the packet received from the master.

2. Bluetooth Architecture and Protocols

The architecture of the Bluetooth technology is divided into several layers, varying in their functions and illustrated in Figure 1.

2.1. Radio Frequency (RF) Layers

The radio layer is the physical wireless connection. In order to reduce collisions with other devices using the ISM range, the radio uses frequency mapping to separate the range into 79MHz bands, starting at 2.402GHz and stopping at 2.480Hz and uses this spread spectrum to hop from one channel to another, up to 1600 times per second.

2.2. Base Band Layer

The base band allows the physical connection between devices. It is responsible for controlling and sending data packets over the radio link. When a Bluetooth device connects to another Bluetooth device, they form a small network called a piconet. A piconet is a small network of Bluetooth devices, where every device in the network can be in one of the following states.

- Master: The Bluetooth device that initiates communication. The master sets the time and broadcasts its clock to all slaves providing the hopping pattern, in which they hop frequency at the same time.

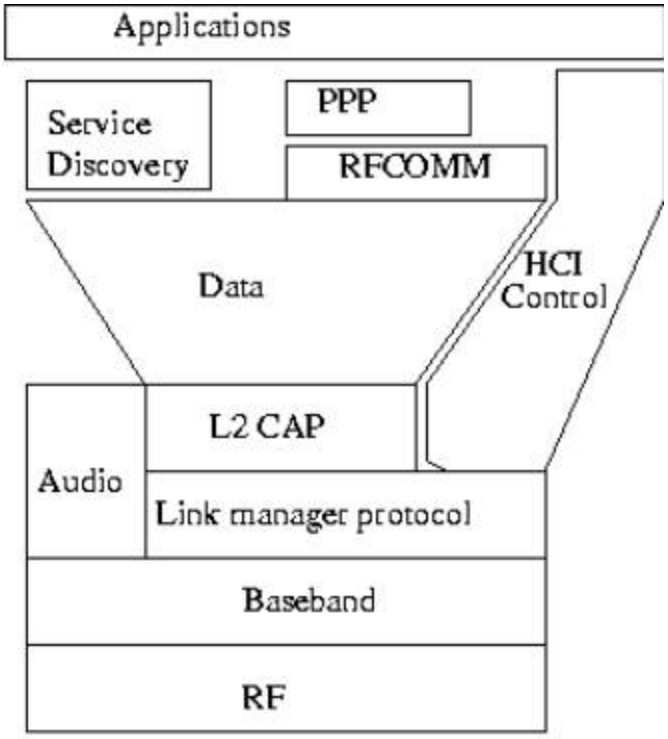

Figure 1. Bluetooth Architecture

- Slaves: The state given to all devices that are connected to another. The device can be an active slave if it actively transmits or receives data from the master, or a passive slave if it is not currently sending or receiving any information. The passive slaves check if there is a connection request from the master by enabling their RF receivers periodically.

- Standby: All devices that are not connected to a master (*i.e.*, not slave) are called standby devices. When searching for other devices, a device enters the inquiry state. When

a device starts creating a Bluetooth link, it enters the page state. Also a device can go to a low power mode to save power.

2.3. Link 2 Manager Protocol (LMP)

The LMP protocol uses the links set up between devices by the base band to establish logical connection responsibilities of the LMP. It also includes security aspects and device authentication.

2.4. Logical Link Control and Adaptation Protocol (L2CAP)

The L2CAP is responsible for receiving applicative data from the upper layers and translates it to the Bluetooth format so that it can be transmitted to the higher layer protocol over the base band.

2.5. Radio Frequency Communication Protocol (RFCOMM)

The RFCOMM is used to emulate serial connections over the base band layer to provide transport capabilities for upper level services and avoiding direct interface of the application layer with L2CAP.

2.6. Service Discovery Protocol (SDP)

The SDP protocol is used to discover services, providing the basis for all the usage models.

2.7. Telephony Control and Signaling Layer (TCS)

The TCS protocol defines the call control signaling for the establishment of speech and data calls between Bluetooth devices. TCS signaling messages are carried over L2CAP.

2.8. Application Layer

The application layer contains the user application. The applications interact with the RFCOMM protocol layer to establish an emulated serial connection.

3. Bluetooth Security

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.

3.1. Basic Definitions

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. Typical attacks to a wireless network include DoS (Denial-of-Service), man-inthe- middle, spoofing,

impersonating, session hijacking, eavesdropping, *etc*. Bluetooth launches three main techniques to achieve security features.

- Confidentiality: The first goal of Bluetooth is confidentiality or privacy. This service prevents an eavesdropper from reading critical information. In general, with this security service only the authorized user can access the data. The process of transforming data into a form that it cannot be understood without a key. Both data and control information can be encrypted.

- Authentication: Providing identity verification of the communicating devices is the second goal of Bluetooth. Authentication allows the communicating devices able to recognize each other; hence communication aborts if the user is not authorized. The process of verifying 'who' is at the other end of the link. Authentication is performed for both devices and users.

- Authorization: The third goal of Bluetooth is to control access to the resources. This is achieved by determining the users who are authorized to use the resources The process of deciding if a device is allowed to have access to a service. Authorization always includes authentication.

3.2. Modes of Security

Each Bluetooth device can operate on one of the 3 security modes. Mode 1 is a non secure mode in which a Bluetooth device shall never initiate any security procedure. Mode 2 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. Mode 3 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, corresponding to security mode 3. The Bluetooth device initiates security procedures before the channel is established. This is the built in security mechanism and it is not aware of service/application layer security.

- Service-level security, corresponding to security mode 2. 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.

3.3. Levels of Security

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 entrusted 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 entrusted 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.

4. Link Level Security

Figure 2 illustrates the link-level security framework of Bluetooth. In the figure, one of the two Bluetooth devices (the claimant) tries to reach the other one (the verifier). Generally four parts exist in the whole scheme as shown top down in the Figure 2.

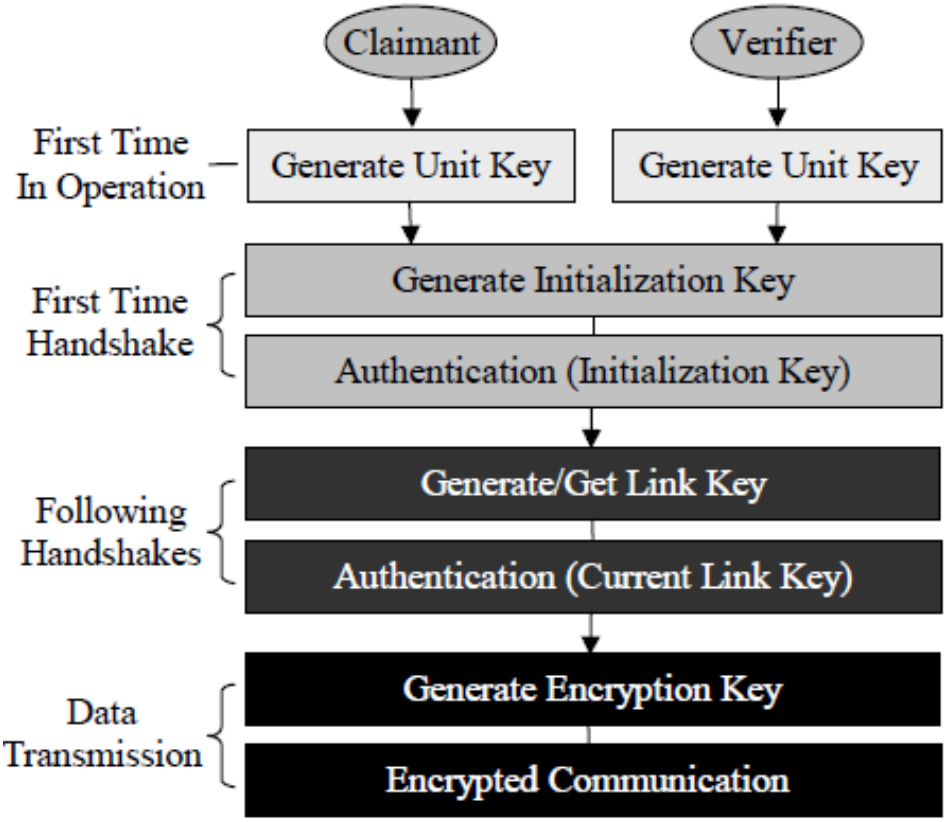

Figure 2. Bluetooth Link-level Security Scheme

4.1. Key Management Scheme

Key management scheme is used to generate, store, and distribute keys, which compasses the first step of each of the four parts in Figure 2. Basically, Bluetooth security scheme is based on symmetric key cryptography, *i.e.*, a private key called link key is shared between two or more parties. The link keys can have different lifetimes. A semi-permanent key can be used after the current session is terminated, while a temporary key is valid only until the current session is over. A total of four types of link keys have been defined, as shown in Figure 3. The initialization key is used only during the initialization process. The unit key is

generated once at the installation of the unit. The combination key is derived by both units for services that require more security. The master key, generated by the master device, is used when the master wants to broadcast messages. There is also a Bluetooth PIN used for authentication and to generate the initialization key before exchanging link keys.

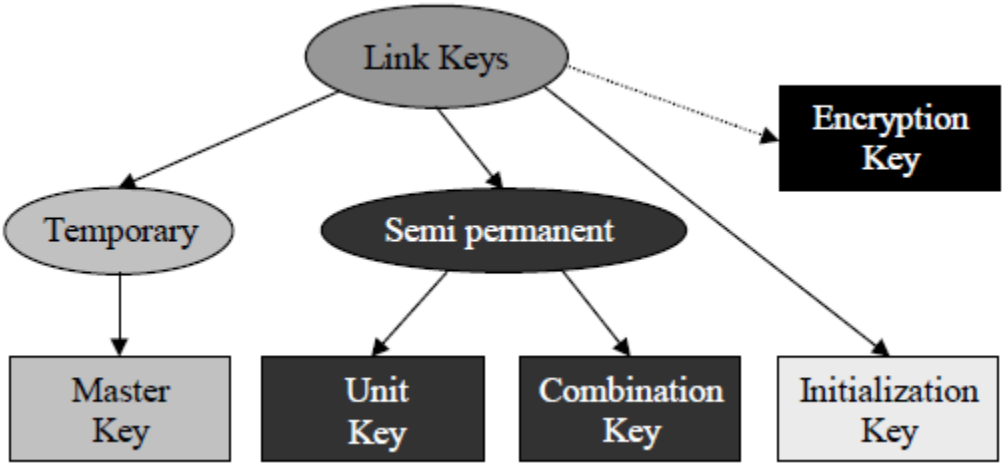

Figure 3. Bluetooth Key Structure

4.2. Authentication Scheme

The Bluetooth authentication scheme uses a challenge-response strategy in which a 2-move protocol is employed to check a claimant's knowledge of a secret key, as shown in Figure 4. If authentication fails, a certain waiting interval must pass before a new attempt can be made. The waiting interval will increase exponentially. This is to prevent an intruder to repeat the authentication procedure with different keys.

4.3. Encryption Scheme

Figure 5 shows the encryption procedure. The encryption key (KC) is generated from the current link key. There are several encryption modes in which broadcast messages and individually addressed traffic can be either encrypted or not, depending on whether a device uses a semi-permanent link key or a master key.

5. Security Level of Service

This section describes the practical issues involved in the implementation of security mechanisms, i.e. an approach for a flexible security architecture built on top of the link-level security features of Bluetooth. More information can be found in [6]. Figure 6 illustrates the general security architecture. The key component in the architecture is a security manager, with the following functions. Store security-related information on both services and devices into corresponding service and device databases.

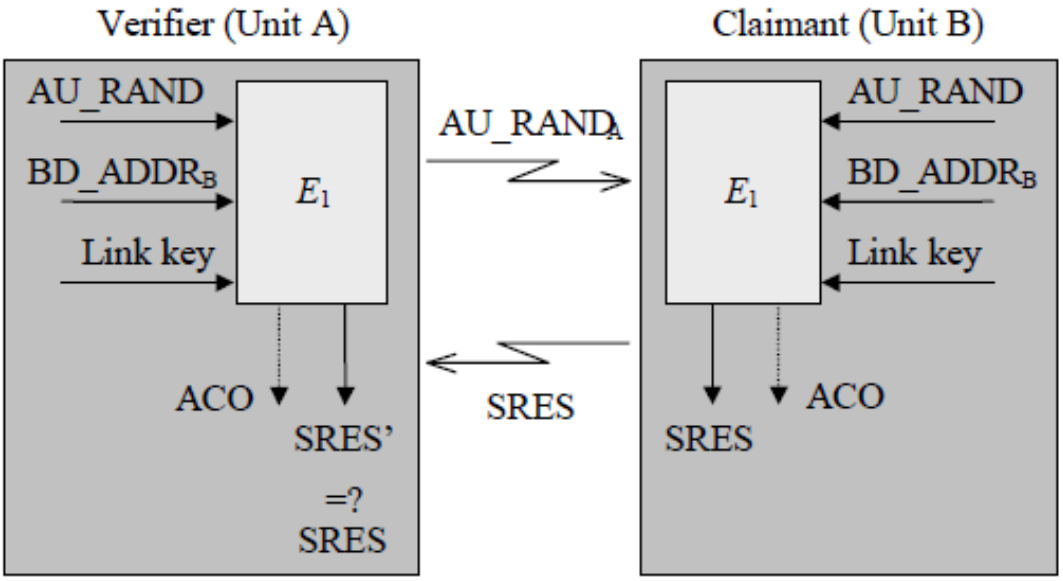

Figure 4. Challenge-response for the Bluetooth Authentication

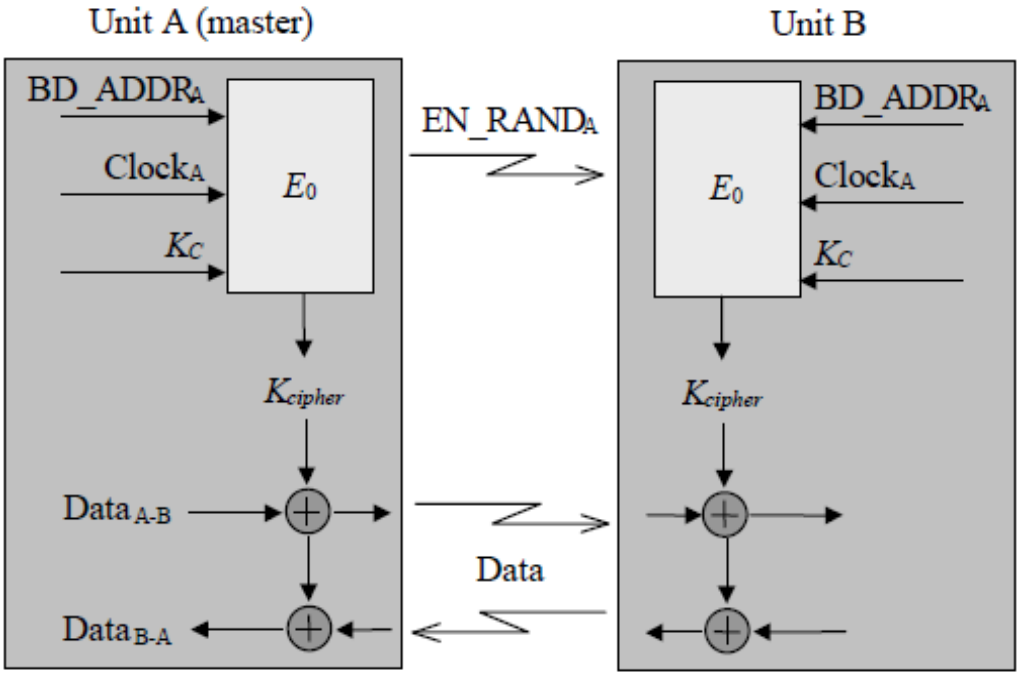

Figure 5. Encryption Procedure

- Grant or refuse access requested by protocol implementations or applications.
- Command the link manager to enforce authentication and/or encryption before connecting to the application, using the HCI.
- Query PIN entry to set-up trusted device relationship.

Employing such a centralized security manager is flexible to implement different access policies and easy to add new policies without affecting other parts. Moreover, the security manager acts as a bridge to join application level and link level security controls together and thus helps in providing end-to-end security.

Authentication should be performed after determining what the security level of the requested service is. That is to say, the authentication can only be performed when a connection request to a service (SCO link) is submitted.

6. Vulnerability

Although the Bluetooth network system is relatively secure, by employing the schemes described above, there are still a number of weaknesses in the standard. Several pieces of research on addressing security flaws present in Bluetooth networks have been carried out. Table 1 lists the detailed description and analysis of Bluetooth vulnerabilities, together with possible attacks/risks and countermeasures corresponding to each of the weakness issues.

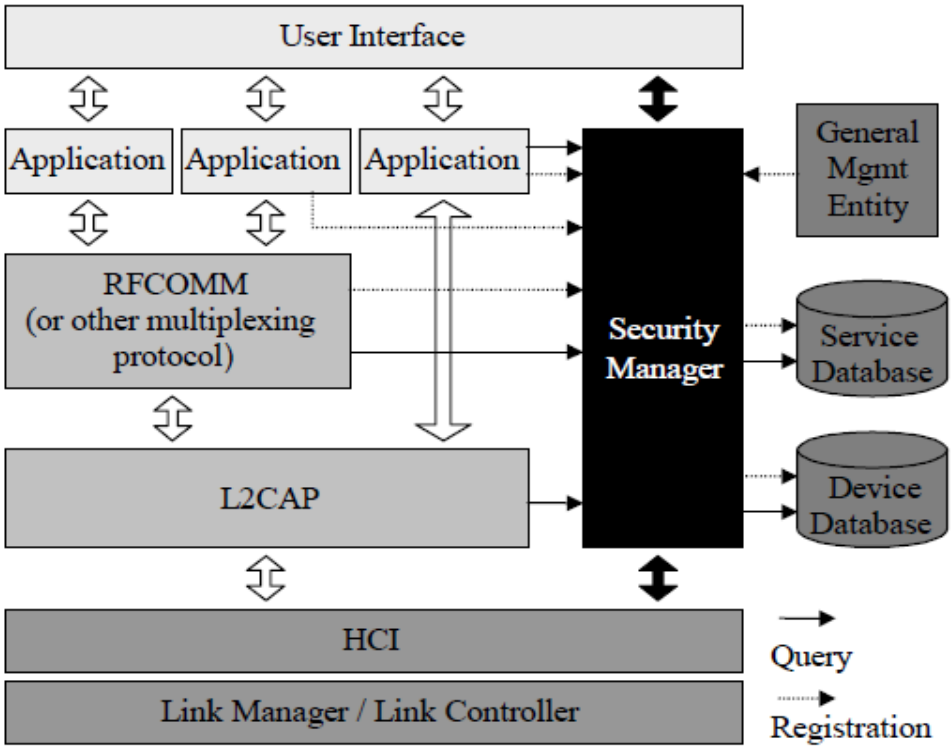

Figure 6. Bluetooth Security Architecture

The table concerns the evaluations on all of the Bluetooth security specific protocols, including general security scheme, key management, authentication, encryption, and authorization. It is worthy to note that the entire framework of the Bluetooth security is acceptable. The weaknesses of the general Bluetooth protocols come from the wireless nature, ad hoc nature, and device address scheme. For security specific protocols, weaknesses fall into methods for PIN code, random number generation, unchangeable unit key, and security manager. More security can be expected through the employment of high-level security schemes by protocols and/or applications upon the Bluetooth.

Table 1. Vulnerability Analysis of the Bluetooth Standard

Weakness	Attack / Risk	Countermeasure
The quality of pseudorandom number generator is undetermined.	Guess the generator implementation or the generated pseudorandom number.	Statistical tests to detect non-repeating and randomly generated requirements.
PIN key is too short and default PIN is all zero.	Easy to exhaustively search or guess PIN key.	Increase the PIN code length.
Need to physically enter PIN code to devices.	Inconvenient PIN code input.	Application level key agreement software.
Initialization key is too weak.	Depend only on RAND and PIN which are both unsafe.	Employ new strong initialization key generation scheme.
Unit key is reusable, and is public to the other side once used.	Calculate encryption key or impersonate other devices with their unit key.	Use unit key as input to generate a random key. Use a key set instead of only one unit key.
Shared master key.	Impersonating or disclosing.	Change broadcast scheme.
No user authentication.	Device embezzling.	Application level security and employ user authentication.
Repeating attempts for authentication.	Disabling authentication attempts from legitimate devices.	Encrypt device address. Limit the entry number of the list.
Weak E_0 stream cipher.	Shortcut attack: guess the contents of E_0.	Replace the cipher with other advanced scheme.
Negotiable key length.	Encryption abort. Use too short a key.	Globe agreement on minimal key length.
Leak support for legacy applications.	Security manager stands idle, no security for legacy applications.	Add a Bluetooth-aware "adapter" application for the legacy application.
No separately defined authorization for services.	No service-related flexible device trusting assignment.	Modify the security manager and the registration processes.
Unidirectional access check but bi-directional traffic.	Malicious verifier attacks claimant by nasty messages.	Access check at all the phases and mutually. Check-consistent data flow direction.

7. Conclusion

Bluetooth is one of several new wireless technologies that are changing the enterprise environment. Because it is very low power, shorter range, lower bandwidth, used for less sensitive applications, and more sparsely used than the other wireless technologies, it is inherently lower risk. Although more and more qualified products emerge, at present Bluetooth is still more a laboratory technology to be studied than a widely used supporting technique for multitudinous products. The protocol is still in its research phase partly because of the security problems. Since the Bluetooth security scheme is reasonably robust to applications with less security requirements, the final features may depend more on the implementation than significant changes to the specification.

Based on the original design goal of cable replacement, Bluetooth is more suitable to short-range and small-size wireless personal area networks than for connecting with outside public networks, comparing to *e.g.*, WLAN. To applications such as large ad hoc networks and outside interconnection access, high level security schemes should preferably be enforced for complementation. Examples include *e.g.*, IPSEC for IP, secure routing protocols, distributed secret schemes, *etc*.

References

[1] The official Bluetooth technology info site, http: //www.bluetooth.com.
[2] C. S. Lee, "Bluetooth Security Protocol Analysis and Improvements", M.Sc. thesis at San Jose State University, http://www.cs.sjsu.edu/faculty/stamp/students/cs298ReportSteven.pdf.
[3] Bluetooth SIG, Specification of the Bluetooth System: Core, Version 1.1, vol. 1, **(2001)** February 22.
[4] Bluetooth SIG, Specification of the Bluetooth System: Profile, Version 1.1, vol. 2, **(2001)** February 22.
[5] IEEE 802.15 Working Group for WPANs, http://ieee802.org/15/.
[6] J. C. Haartsen, "The Bluetooth Radio System", IEEE Personal Communications, vol. 7, no. 1, **(2000)** February, pp. 28-36.
[7] T. Muller, "Bluetooth Security Architecture: Version 1.0", Bluetooth White Paper, Document # 1.C.116/1.0, **(1999)** July 15.
[8] K. Dasgupta, "Bluetooth Protocol and Security Architecture Review", online report, http://www.cs.utk.edu/~dasgupta/bluetooth/.
[9] J. T. Vainio, "Bluetooth Security", Online report, **(2000)** May 25, http://www.niksula.cs.hut.fi/~jiitv/bluesec.html.
[10] M. Jakobsson and S. Wetzel, "Security Weaknesses in Bluetooth", online report, http://www.bell-labs.com/user/markusj/bluetooth.pdf.
[11] C. Candolin, "Security Issues for Wearable Computing and Bluetooth Technology", Online report, http://www.cs.hut.fi/Opinnot/Tik- 86.174/btwearable.pdf
[12] R. Mettala, "Bluetooth Protocol Architecture: Version 1.0", Bluetooth White Paper, Document # 1.C.120/1.0, **(1999)** August 25.

Authors

Bijoy Kumar Mandal, is, currently, associated with Computer Science and Engineering Department, Faculty of Engineering and Technology, NSHM Knowledge Campus – Durgapur, as an Assistant Professor. He is pursuing Ph.D. (Computer Science and Engineering) in NIT, Durgapur. He published 10 Research papers in international Journals and Conferences.

Debnath Bhattacharyya, M.Tech (CSE), Ph.D. (Tech.), currently, associated with Computer Science and Engineering Department, Faculty of Engineering and Technology, NSHM Knowledge Campus – Durgapur, as a Professor and Head. Dr. Bhattacharyya has 17 years of experience in Teaching and Research. He published more than 135 research papers in international Journals and Conferences. He published 4 Text Books for B. Tech, and MCA, so far. He is also associated with West Bengal University of Technology, University of Calcutta and many leading National and International Universities as the Ph.D. Supervisor.

Tai-hoon Kim, M.S., Ph. D (Electricity, Electronics and Computer Engineering), currently, Professor of Sungshin Women's University, Korea. His research interests include Multimedia security, security for IT Products, systems, development processes, operational environments, etc. He has 18 Years of experience in Teaching & Research. He has already got distinctive Academic Records in international levels. He has published more than 300 Research papers in International & National Journals and Conferences.