CURRENT TRENDS AND REASERCH ISSUES IN BLUETOOTH COMUNICATION

P S Patheja *

Akhilesh A Waoo **

Sudhir Nagwanshi ***

ABSTRACT

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 a 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.

Keyword: *Bluetooth, E0, E1, E2, E3, Key Stream, Data Transmission.*

***** Head, Department of M Tech, BIST, Bhopal.

****** Assistant Professor, Department of M Tech, BIST, Bhopal.

******* BIST, Bhopal.

I. INTRODUCTION:

A Bluetooth, is a recently proposed standard for local wireless communication and is becoming hotter and hotter a topic. 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. Bluetooth is a high-speed, low-power microwave wireless link technology, which is based on chip that provide a wireless link to connect phones, laptops and other portable equipment together. Bluetooth is used for a short-range radio frequency (RF) technology that operates at 2.4 GHz and is capable of transmitting voice and data from one device to other. The effective range of Bluetooth devices is 32 feet (10 meters). Bluetooth transfers data at the rate of 1 Mbps, which is from three to eight times to the average speed of parallel and serial transmission. It was invented to get rid of wires[1]. Bluetooth is more suited for connecting two point-to-point devices. Security issues arising from Bluetooth are relatively less publicized, possibly due to less critical nature of information at stake - an individual's cell phone data against corporate data thefts and associated hard losses. Nevertheless, with respect to personal privacy and perimeter security, an insecure Bluetooth device or technology can pose serious risk of information compromise. Now let's explore the categories in which Bluetooth hacking is often classified. This will show how real the issue of security in Bluetooth devices is. 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 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.[1,2]

II. BLUETOOTH PROTOCOL OVERVIEW:

Bluetooth protocol stack, which can be divided into four layers according to their purpose, in the following way

- 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.

- Cable Replacement Protocol, i.e. RFCOMM protocol, is based on the ETSI TS 07.10 that emulate serial line control and data signals over Bluetooth Baseband to provide transport capabilities for upper level services.
- 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.
- 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.
- 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.

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 shown in Figure 1. Instead, applications run over one or more vertical slices of this protocol stack. In other words, applications may run over different protocol stacks. Nevertheless, each one of these different protocol stacks uses a common Bluetooth data link and physical layer, i.e. Bluetooth core protocols, including:[2]

- 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. Other functions include error correction, link management and control, audio transmission, etc.
- 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.
- 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.

- 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.[1,2]

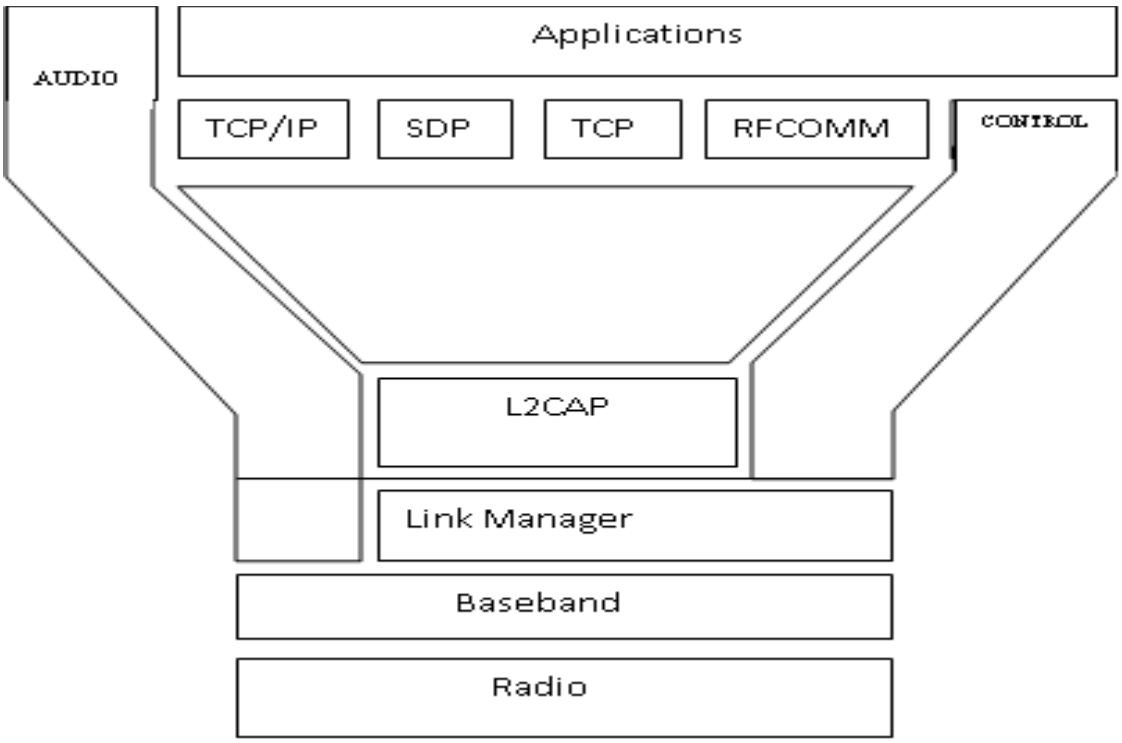

Figure 1. Bluetooth protocol stack.

III. OVERVIEW

A. Security Mechanism in Bluetooth

The Bluetooth defines three security modes.

Safe mode 1: No safe mode, which has the lowest security level.

Safe Mode 2: Service-oriented security model, which start after the establishment of the channel.

Safe Mode 3: Link-oriented security model, which install and initial before communication link is established.

Bluetooth system provides safety precautions in the application layer and link layer, and both sides achieve authentication and encryption in the same way. Link layer uses four entities to ensure the safety:[5]

1) 48-bit of the Bluetooth device address, which is global uniqueness decided by the IEEE;

2) The authentication key for entity authentication is 128-bit;

3) The secret key for data encryption is 8 ~ 128-bit;

4) 128-bit random number trades once, changes once.

Initially two keys are generated and do not open, encryption key is generated during certification process from the authentication key, but it is different from the authentication key, a new secret key is generated every time when we activate the encryption. Authentication key is more stable, after key generation[5]. The random numbers of Bluetooth demands "random generation" and "non-repeatability", that is to say the random numbers are almost impossible to duplicate and can not be significantly greater than zero probability estimate of the random numbers in the authentication key life.

B. Authentication and encryption

Bluetooth security-mechanism is divided into three modules key generation, authentication and encryption, and adopts four kinds of algorithms as E0 E1, E2, and E3. Link layer is responsible to provides authentication, encryption and key management. PIN code was entered by user, by means of the E2 algorithm for generating the link key, by means of E3 algorithm, getting encryption key, make use of E0 algorithm generated key stream, and encrypt plaintext, then get cipher text. Figure 1 is the process of Bluetooth encryption.[5,6,7]

The three modules of Figure 1 are as follows:

1) Key generation module, algorithm E2 is used for generating the link key, and its input parameter is a 4-digit passwords number which is entered by the user, the algorithm E3 calculates encryption key KC by the use of E2 link key encryption key as input parameters.

2) Encryption module, algorithm E0 can be used for generating keys stream to encrypt the original data.

3) Authentication module, algorithm E1 is the crucial algorithms in the authentication process, the two units in need of certification use each authentication algorithm E1 to generate identification word and compare, then complete certification.

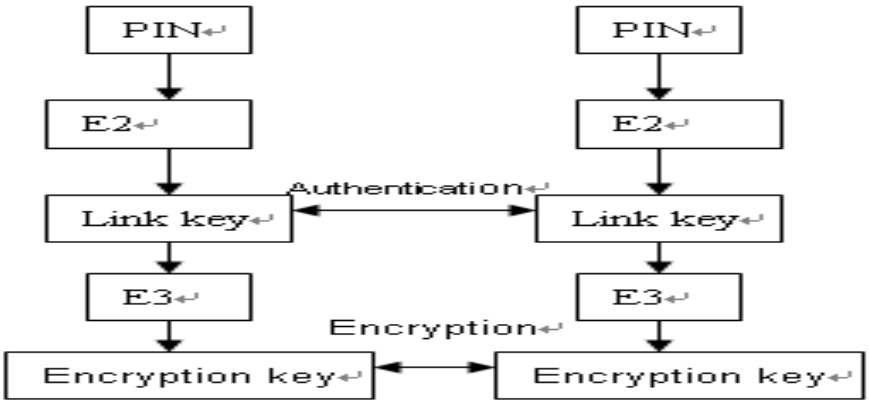

Figure 2: Bluetooth encryption process.

C. Analysis of E0 Algorithms

E0 belongs to stream encryption method, that is to say it takes data flow and the key bit stream Exclusive-or operation. The payload of each packet is encrypted separately, and the encryption occurs before MPE-FEC, after the cyclic redundancy check. The main principle is to use linear feedback shift register to generate pseudo-random sequence, after that form key stream that can be used for encryption, and then take the key stream and data stream that need encryption Exclusive-or operation, and achieve encryption. During decryption, the cipher text takes Exclusive-or operation once more, re-plaintext can be obtained.[5,6]

IV. TYPES OF WEAKNESS ATTAKS AND THERE COUNTERMEASURES

A. WEAKNESS[3]

- The quality of pseudorandom number generator is undetermined.
- PIN key is too short and default PIN is all zero.
- Need to physically enter PIN code to devices.
- Shared master key.
- No user authentication.
- Repeating attempts for authentication.
- Weak *E*0 stream cipher.
- Negotiable key length.
- Leak support for legacy applications.
- No separately defined authorization for services.
- Unidirectional access check but bi-directional traffic.

B. ATTAKS/RISKS[3]

- Guess the generator implementation or the generated pseudorandom number.
- Easy to exhaustively search or guess PIN key.
- Impersonating or disclosing.
- Device embezzling.
- Disabling authentication attempts from legitimate devices.
- Shortcut attack: guess the contents of *E*0.
- Security manager stands idle, no security for legacy applications.
- No service-related flexible device trusting assignment.
- Malicious verifier attacks claimant by nasty messages.

C. COUNTERMEASURES[3]

- Statistical tests to detect non-repeating and randomly generated requirements.
- Increase the PIN code length.
- Application level key agreement software.
- Change broadcast scheme.
- Application level security and employ user authentication.
- Encrypt device address. Limit the entry number of the list.
- Replace the cipher with other advanced scheme.
- Replace the cipher with other advanced scheme.
- Add a Bluetooth-aware "adapter" application for the legacy application.
- Modify the security manager and the registration processes.
- Access check at all the phases and mutually. Check-consistent data flow direction.

V. CONCLUSION

Bluetooth technology is a new technology for transmitting Data from one device to another. For communication between devices it uses wireless mode for the transmission of data from one device to another. Compared to the fixed line network Bluetooth network is more vulnerable to be attacked. For those applications that take data security as priori, achieving a high level of data security is essential. Currently, stream cipher E0 used in Bluetooth standard has many shortcomings, while using some kind of hybrid encryption algorithm like RSA and DES is relatively more secure and easier to achieve, thus it ensures that data transmission between the Bluetooth device are more safe than traditional E0 Bluetooth Algorithm.

VI. ACKNOWLEDGMENT

I express my sincere gratitude and acknowledgement towards P S Patheja sir and Akhilesh A Waoo sir, who guided me. It was their constant support and inspiration without which my effort would not have taken this shape. I sincerely thank them for this and seek them support for all my future endeavors.

VII. REFERENCES

1. Design, implementation, and evaluation of Bluetooth security; jun-zhao sun, douglas howie, antti koivisto, and jaakko sauvola
2. Bluetooth™ Security White Paper; Christian Gehrmann 2002
3. Security Weakness in Bluetooth: Markus Jakobsson,Susanne Watzil
4. A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication, Wuling Ren, Zhiqian Miao, College of Computer and Information Engineering Zhejiang Gongshang University 2010
5. Performance Analysis of SAFER+ and Triple DES security algorithms for Bluetooth Security Systems , Dr.R.Neelaveni,D.Sharmila
6. Bluetooth Hacking: A Case Study, Dennis Browning, Gary C. Kessler
7. Zheng Hu. Network and Information Security [M]. Peking: Tsinghua University Pres, 2006.
8. Man Young Rhee. Network Security Encryption Principle, algorithm and Protocol[M]. Peking: Tsinghua University Pres, 2007.
9. Suri, P. R.; Rani, S. Bluetooth security Need to increase the efficiency in pairing [J]. IEEE/ Southeastcon, 2008.
10. Fengying Wang. Dynamic Key 3DES Algorithm of Discrete System Based on Multi-dimension Chaos [J]. Microelectronics and Computer, 2005, 7: 25-28.
11. Falk A. The IETF, the IRTF and the networking research Community.Computer Communication Review, v35, n5, Oct. 2005:6970.
12. Data Encryption using DES/Triple-DES Functionality in Spartan-II FPGAs, Amit Dhir
13. Cryptanalysis of Bluetooth Keystream Generator Two-level E0, Yi Lu? and Serge Vaudenay
14. On the Existence of low-degree Equations for Algebraic Attacks, Frederik Armknecht?

15. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher Revised 19 May 2008 William C. Barker
16. Tiger: A Fast New Hash Function, Ross Anderson, Eli Biham
17. Serpent: A New Block Cipher Proposal, Eli Biham, Ross Anderson and Lars Knudsen
18. Cracking the Bluetooth PIN, Yaniv Shaked and Avishai Wool
19. Yaniv Shaked, Avishai Wool. Cracking t he Bluetooth P[C]. 3rd USEN IX/ ACM Conf. Mobile Systems, Application and Services (MobiSys). Seattle, WA, June 2005:39250.