A Protocol to Secure Bluetooth Communication

J. T. Lalis*, B. D. Gerardo** and Y. Byun***

*College of Computer Studies, Cebu Institute of Technology-University, Cebu City, Philippines
**Institute of ICT, West Visayas State University, Luna St., Lapaz, Iloilo City, Philippines
***Dept. of Computer Engineering, Jeju National University, Jeju, Korea

j_lalis@yahoo.com, bgerardo@wvsu.edu.ph and ycb@jejunu.ac.kr

Abstract. The focus of this paper is the development of new pairing protocol for secure data communication using Bluetooth technology. An improved pairing protocol has been developed by adopting the Diffie-Hellman Key Exchange protocol in computing the shared secret value of both parties. MD5 and a lightweight encryption algorithm, the Hummingbird-2, were then employed to further strengthen the pairing mechanism and at the same time, making it suitable for devices that has limited processing power and memory. The proposed protocol is expected to provide Bluetooth devices a greater security against eavesdropping and man-in-the-middle attacks.

1. Introduction

Bluetooth technology is now considered as a cheap, low-power, and efficient means of data communication. It uses short-range radio links to enable different devices to connect and communicate with each other. Modern devices and equipment are now getting smaller, cheaper, and more flexible making it more accessible to the consumers and in-demand to the market. More and more people are now getting into portable devices due to its efficiency and flexibility. One promising use of Bluetooth technology is the automatic synchronization, wherein data such as pictures taken through a digital camera or mobile phone can be automatically transferred to a laptop and personal computer and be printed to a printer without docking the cables. Researchers are now also looking into the new modes of home and healthcare monitoring through Bluetooth technology. However, as the demand for it increases, its vulnerability against different attacks also increases [1]. In the study of [7], several vulnerabilities were discovered due to flaws and pitfalls in the current pairing and authentication protocols of BT. Users tend to enter short and simple pin, around 4 digits, since it is user-friendly and some of the devices, such as mobile phones, have a limited input capability. But forcing the user to use long and complex pin is generally not practical and not feasible.

Moreover, portable devices have limited CPU processing power and memory

*** Corresponding author.

ISA 2013, ASTL Vol. 21, pp. 299 - 303, 2013

constraining it to have a complex pairing and authentication algorithm. Thus, these problems encourage the researcher to develop a lightweight but strong pairing protocol with a user-friendly short pin to secure Bluetooth communication.

2. Review of Related Literature

The arising security issues of Bluetooth technology becomes an active research area in academia and industry as wireless communication becomes an integral part of this modern society. In the report of Minar and Tarique [1], communication through Bluetooth pairing protocol is vulnerable against MAC spoofing attack, PIN cracking attack, impersonation attack and etc. [7] summarizes the security issues that they have discovered due to flaws or pitfalls in the pairing and authentication procedure of Bluetooth. Recent studies [2], [3], [4] have already been conducted to address these problems. Nayar [2] deals with the architectural design of a secure wireless Bluetooth sensor system. Patheja et al [3] used the 64-bit triple DES algorithm to produce the cipher text of the key and the TIGER encryption algorithm to encrypt the original message. Shrivastava [2] takes the advantage of RSA algorithm in encrypting the distributed key in easy and fast manner.

A. Diffie-Hellman Key Agreement Protocol

Diffie-Hellman key agreement is a protocol that enables two parties to have a shared secret key. It is not an encryption or decryption algorithm, but rather, a combination of mathematical functions wherein both parties (Alice and Bob) agree on a public value g and a large prime number p. Next, Alice and Bob choose secret values a and b respectively. Each party then uses their secret values to compute the public values A and B, ga mod p and gb mod p, respectively. These values are then sent to each other parties through the network publicly. Both parties use these public values to derive one secret key, Aa mod p for Alice and Bb mod p for Bob. Eavesdroppers cannot derive the shared secret key since the secret values, a and b, are unknown to them.

B. The MD5 Message-Digest Algorithm

MD5 is a cryptographic hash function designed by Ron Rivest that accepts a message with arbitrary length and produces a 128-bit (16-byte) hash value or known as message digest. MD5 has been widely used in variety of information security applications, notably to check data integrity, digital signatures, and other forms of authentication.

3. Simulation of the proposed pairing protocol

In Bluetooth, a trusted relationship called 'pairing' is essential to work for online communication securely. It can be formed by exchanging secret code(s) or key(s) of authorized communicating parties. The secret key(s) must be protected from discovery by unauthorized parties such as eavesdropper.

Fig. 1 below shows the process of the improved pairing scheme for two Bluetooth devices.

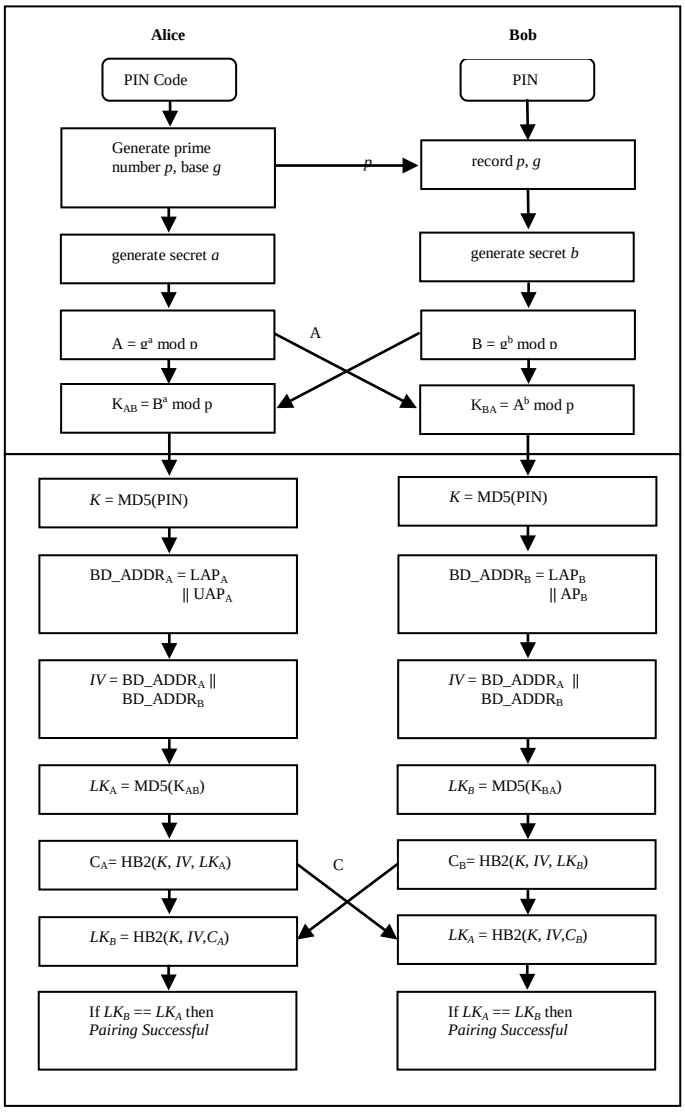

Fig. 1. Proposed Pairing Protocol.

1. Alice and Bob must first enter the PIN code.
2. Alice generates the large prime number p and base g.
3. Alice sends p and g to Bob publicly.
4. Alice chooses a secret integer a, then sends Bob $A = g^a \bmod p$
5. Bob chooses a secret integer b, then sends Alice $B = g^b \bmod p$
6. Alice computes the secret key $K_{AB} = B^a \bmod p$
7. At the same time, Bob computes the secret key $K_{BA} = A^b \bmod p$

8. To obtain the 128-bit key K, Alice and Bob perform MD5 hashing function using the PIN as input.

9. Concatenate the lower 24-bit part LAP_A and 8-bit upper part UAP_A of the Bluetooth address BD_ADDR_A of Alice, denoted as $BD\_ADDR_A = LAP_A \| UAP_A$,
10. At the same time, Bob derives its 32-bit $BD\_ADDR_B = LAP_B \| UAP_B$

11. Since both parties have each other's address, the 64-bit Initialization Vector IV was achieved by concatenating BD_ADDR_A and BD_ADDR_B, denoted as $IV = BD\_ADDR_A \| BD\_ADDR_B$

12. Link key LK_A is computed by Alice using the MD5 function and secret key K_{AB} as input.
13. Bob also computes its link key LK_B using the MD5 function and secret key K_{BA} as input.

14. Alice encrypts the LK_A using the Hummingbird-2 algorithm, $C_A = HB2(K, IV, LK_A)$, and send C_A to Bob
15. Bob encrypts the LK_B using the Hummingbird-2 algorithm, $C_B = HB2(K, IV, LK_B)$, and send C_B to Alice

16. Alice decrypts LK_B using the Hummingbird-2 algorithm, $LK_B = HB2(K, IV, C_B)$, and compare it with its LK_A
17. Bob decrypts LK_A using the Hummingbird-2 algorithm, $LK_A = HB2(K, IV, C_A)$, and compare it with its LK_B
18. If Alice's and Bob's link keys matched with each other, pairing is considered to be successful.

The use of Diffie-Hellman Key Agreement Protocol is believed to strengthen the Bluetooth security against unit key attack. And by making use of MD5 to digest the PIN, guessing the PIN code, regardless of its length, through PIN cracking attack and Off-line PIN recovery attack would be infeasible. The lightweight but relatively strong Hummingbird-2 cipher solved the current security problem of man-in-the-middle-attack while maintaining its advantages such as speed, low-cost, and power efficiency.

4. Conclusion

In this paper, an improved pairing protocol has been presented to address the vulnerabilities of Bluetooth in the link layer. The combination of the three lightweight but strong algorithms (Diffie-Hellman Key Agreement Protocol, MD5, and Hum-

mingbird-2) will require small footprint implementation, making it well suited for ubiquitous devices and sensor systems that consider data security as priori.

References

1. N.B.I Minar, M. Tarique. “Bluetooth security threats and solutions: a survey”, International Journal of Distributed and Parallel Systems, vol. 3, no. 1, pp 127-148 (2012)
2. A. Nayar, “Securing wireless Bluetooth sensor systems”. Journal of Computer Applications, vol. 4, no. 1,pp 4-7 (2011)
3. P.S Patheja, A. Waoo, S. Nagwanshi, “A hybrid encryption technique to secure Bluetooth communication”, IJCA Proceedings on International Conference on Computer Communication and Networks, vol. 1,pp 26-32 (2011)
4. G. Shrivastava, “An integrated encryption scheme used in Bluetooth communication mechanism”, VRSD International Journal of Computer Science and Information Technology, vol. 1, no. 8, pp 567-572 (2011)
5. D. Engels, , M. Saarinen , P. Schweitzer, E. Smith, “The hummingbird-2 lightweight authenticated encryption algorithm”, In Proceedings of the seventh international conference of rfid security and privacy, RFIDSec’11 2012, Springer-Verlag, Berlin, Heidelberg, pp 19-31 (2012)
6. Q. Chai, G. Gong, “A cryptanalysis of hummingbird-2: the differential sequence analysis”, International Association for Cryptologic Research Cryptology ePrint Archive, p 233, 2012.
7. W. Diffie, M. E. Hellman, “New Directions in Cryptography”, IEEE Transactions on Information Theory, vol. IT-22, pp 644–654 (1976)