International Journal of Security and Its Applications
Vol.8, No.4 (2014), pp.219-228
http://dx.doi.org/10.14257/ijsia.2014.8.4.19

Securing Bluetooth Communication with Hybrid Pairing Protocol

J. T. Lalis[1], B. D. Gerardo[2] and Y. Byun[3*]

[1]*College of Computer Studies, La Salle University, Ozamiz City, Philippines*
[2]*Institute of ICT, West Visayas State University, Luna St., Lapaz Iloilo City, Philippines*
[3]*Dept. of Computer Engineering, Jeju National University, Jeju, Korea*
j_lalis@yahoo.com[1], bgerardo@wvsu.edu.ph[2], and ycb@jejunu.ac.kr[3]

Abstract

To improve the level of security of Bluetooth communication, a hybrid pairing protocol based on Diffie-Hellman Key Exchange protocol, MD5 and Hummingbird-2 is proposed. The developed hybrid pairing protocol adopted the DH Key agreement protocol to securely compute both parties' shared secret key. MD5 hash function is used to solve the problem(s) caused by having a short PIN. This mechanism is integrated with the Hummingbird-2, a lightweight encryption algorithm, to further strengthen the pairing mechanism and at the same time, making it suitable for devices that has limited processing power and memory. This hybrid pairing protocol is expected to increase the security of the Bluetooth devices against known attacks, such as man-in-the-middle attack and eavesdropping, by combining these strong yet lightweight algorithms.

Keywords: *Bluetooth, Diffie-Hellman, MD5, Hummingbird-2, pairing protocol*

1. Introduction

Recent innovations in the mobile technology made modern devices and equipment to be smaller and yet more flexible and cheaper. These advances bring the portable devices closer to consumers and increasing its demand to the market. Furthermore, one key feature of these devices is its capability to exchange data from one device to another through a wireless network. There are different ways to exchange data in a wireless network and Bluetooth technology is one of it. BT offers an efficient, low-power, and cheap way of transferring data from one device to another. This technology uses a short-radio links to allow two or more devices to connect and exchange data with each other [8].

Automatic synchronization is just one of the promising uses of BT, wherein data like photos taken through a smart phone or camera are automatically transferred or synchronized with the other portable devices such as laptop and be printed to printer without docking the cables. Recent studies of BT are now into the new modes of healthcare and home monitoring, or also known as smart home. According to [10], smart homes controlled through wireless network, make the life easier, secured, and more convenient. Possible applications of Bluetooth technology in smart homes are now being looked into also by the researchers.

However, the vulnerability of BT against different attacks also increases as the demand for it increases [1]. Several vulnerabilities of BT were discovered in the study

* Corresponding Author

ISSN: 1738-9976 IJSIA

of [7] due to pitfalls and flaws in its current pairing and authentication protocol. In the current protocol, users are only asked to enter short, around 4 digits, and simple pin to make it more friendly and easy to remember. Moreover, some of the portable devices, such as mobile phones, have a limited input capability making it impossible for the users to enter complex pin. But forcing the users to use long and complex is generally not feasible and impractical. Another problem is that most of the portable devices have limited memory and CPU processing power making it difficult for it to accept and process complex pairing and authentication algorithm. Thus, these problems motivated the researchers to develop a lightweight yet strong pairing protocol that will also allow the users to enter a short and user-friendly pin to increase the security of Bluetooth communication.

2. Review of Related Literature

As wireless communication becomes an integral part of this modern society, the arising issues in the security of Bluetooth technology become active research areas in industry and academia. It has been reported in the study of Minar and Tarique [1] that the communication initiated through the current pairing protocol of Bluetooth is vulnerable against different attacks, such as impersonation, personal identification number (PIN) cracking, MAC spoofing attack and *etc.*, The discovered security issues due to flaws or pitfalls in the pairing and authentication procedure of BT were also summarized by [7]. Various studies [2-4] had already been conducted recently to address these problems in BT. To secure the wireless Bluetooth sensor system, Nayar [2] deals with its architectural design. In the study of Patheja, *et al.*, [3], the 64-bit triple DES algorithm was used to produce the cipher text of the key. The TIGER encryption algorithm was then used to encrypt the original message with the previously created key. To increase speed and easiness in encrypting the distributed key, Shrivastava [2] took advantage of the RSA algorithm.

2.1. Diffie-Hellman Key Agreement Protocol

In order to have a secure end to end transmission between two devices, it is important have a secure and efficient way of exchanging keys in the network [9]. The Diffie-Hellman key agreement protocol enables the two parties to have a shared secret key. DH is more on a combination of mathematical functions rather than an encryption or decryption algorithm. In this process, both parties (Alice and Bob for instance) agree on a large prime number p and a public value g. Alice will then choose a secret value a and b for Bob. The chosen secret values by both parties are then used to calculate the public values A= $g^a \bmod p$ and B= $g^b \bmod p$. These calculated values are then forwarded respectively to both parties through the network publicly, as shown in Figure 1. The secret key can then be derived by Alice and Bob using the generated public values, $B^a \bmod p$ and $A^b \bmod p$ respectively. Since the values a and b are unknown, it is impossible for the eavesdroppers to derive the shared secret key.

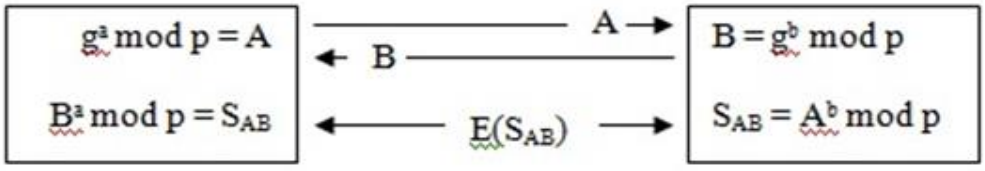

Figure 1. Key Exchange using Diffie-helmen Key Agreement Protocol

2.2. The md5 Algorithm

Ron Rivest designed a cryptographic hash function that accepts a message with arbitrary length and produces a 16-byte or 128-bit hash value, also known as the message digest. It has been widely in various applications of information security, notably for digital signatures, checking data integrity and other forms of authentication. MD5 works as follows

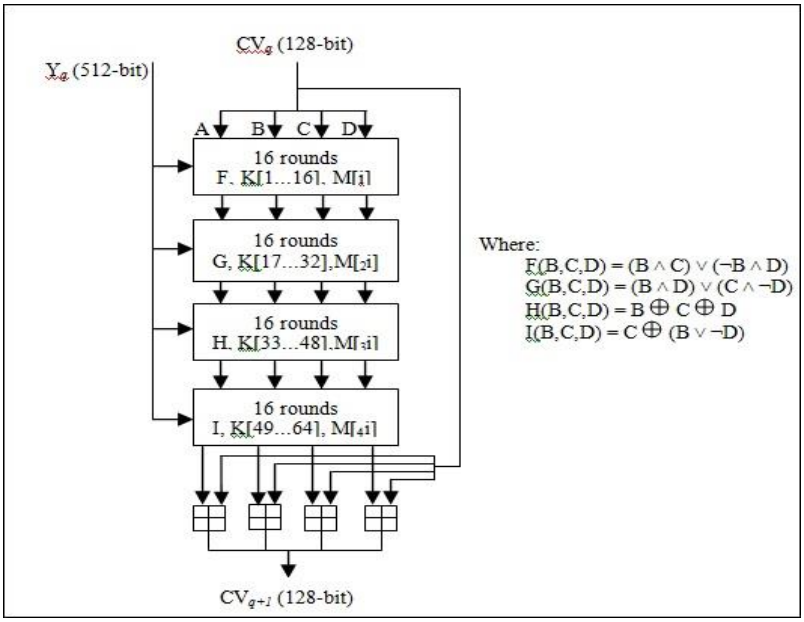

Figure 2. Proposed Pairing Protocol

MD5 accepts an input message with variable-length and process it to produce a fixed 128-bit message. It is done by grouping the input message into 512-bit blocks where each block contains sixteen words with size of 32-bit each. A padding is added to the input message if in case that the input message is not divisible by 512. MD5 function operates in a four 32-bit words, called as state, denoted as A, B, C and D that are initialized with fixed values. As shown in Figure 2, each 512-bit block is processed by the MD5, modifying its state. Processing is done in four similar stages, where each stage has sixteen similar rounds. Figure 3 illustrates the processes within each round based on modulo 232, non-linear function *F*, and left rotation.

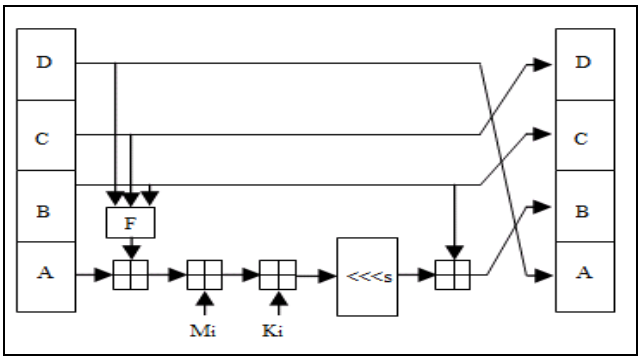

Figure 2. Proposed Pairing Protocol

2.3. The Lightweight Hummingbird-2

The Hummingbird-2 is an encryption algorithm with a 128-bit secret key K and a 128-bit internal state R which is initialized using a 64-bit Initialization Vector IV. It is entirely built from operations on 16-bit words using the exclusive-or (EOR) operation, addition modulo 65536, and a nonlinear mixing function f(x). It has been designed to have very small software or hardware footprint which makes this suitable for resource-constrained devices such as RFID tags, wireless controllers, and sensors. It is believed to be resistant to all standard attacks to block and stream ciphers [6].

3. Hybrid Pairing Protocol Simulation

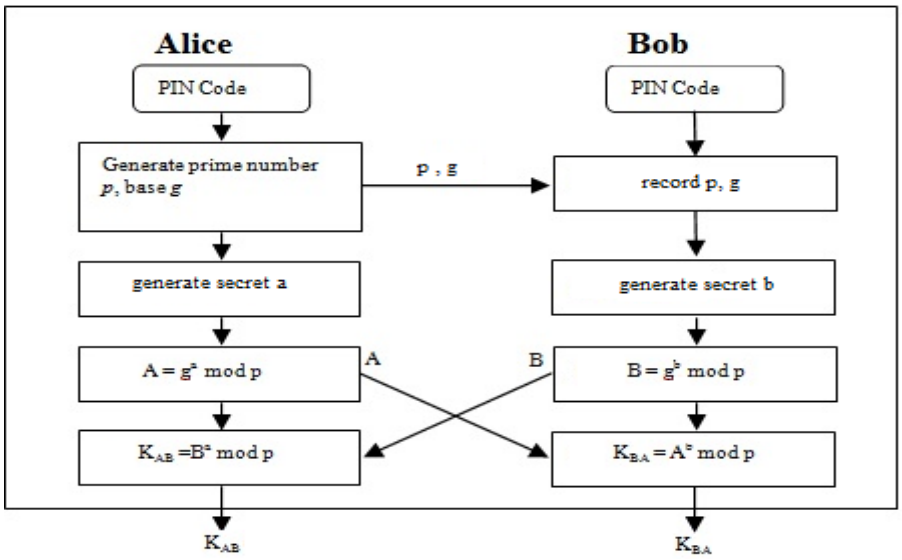

Figure 3. Secret Key Computation of Two Parties

A trusted relationship called "pairing" in Bluetooth is essential in order for it to work securely in the online communication. It is formed by authorized communicating parties through the exchange of key(s) or secret key(s). This secret key(s) should be protected to make it undiscoverable for unauthorized parties such as eavesdropper. Figure 4 above shows the process of the hybrid pairing scheme for two Bluetooth devices. The proposed pairing protocol works as follows:

1. PIN codes are first entered by Alice and Bob.
2. The base g and large prime number p are then generated by Alice.
3. These *p* and *g* are then sent to Bob publicly.
4. Alice then chooses a secret integer *a*, then sends A = g^a mod *p* to Bob.
5. Bob also chooses a secret integer *b*, then sends B = g^b mod *p* to Alice.

Table 1. Input Values for Simulation

Input				
PIN Code	p	g	A	b
A0BC	107_{10}	2_{10}	6_{10}	2_{10}

Table 1 shows the prime number p and base g generated by Alice and sent publicly to Bob. The table also shows the chosen secret key a and b of Alice and Bob respectively.

6. After receiving B, Alice can then computes the secret key $K_{AB} = B^a \bmod p$.
7. At the same time, Bob computes the secret key $K_{BA} = A^b \bmod p$ using the received A.

Table 2. Resulting Shared Secret Keys

A	B	K_{AB}	K_{BA}
64_{10}	4_{10}	30_{10}	30_{10}

In adopting the Diffie-Hellman Key Agreement Protocol, Alice and Bob will arrive at the same value for secret keys K_{AB} and K_{BA} if they have the exact value of a and b as shown in Table 2.

8. The PINs inputted by Alice and Bob are processed using the MD5 hashing function to obtain the secured 128-bit key K.

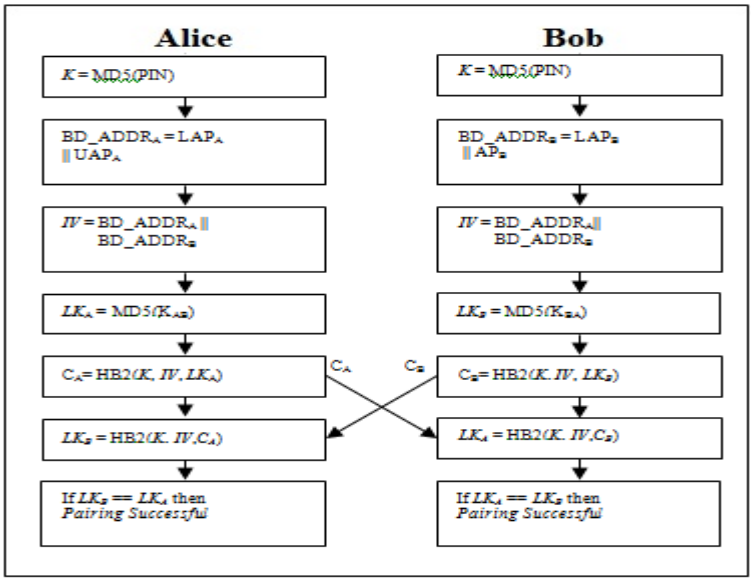

Figure 4. The Hybrid Pairing Protocol Algorithm

Table 3 illustrates a more secured 128-bit key generated after applying step 8. This also ensures that the key K will have a fixed length of 128 bits regardless of the PIN length.

Table 3. Resulting K After Applying MD5

K								
Base 16	9f0a	ea66	365c	dca7	96c1	c2c1	38c6	681e
Base 2	1001	1110	0011	1101	1001	1100	0011	0110
	1111	1010	0110	1100	0110	0010	1000	1000
	0000	0110	0101	1010	1100	1100	1100	0001
	1010	0110	1100	0111	0001	0001	0110	1110

9. The Bluetooth address BD_ADDR_A of Alice is then generated by concatenating the 24-bit part LAP_A and 8-bit upper part UAP_A of the Bluetooth address, denoted as $BD\_ADDR_A = LAP_A \| UAP_A$,
10. Bob uses the same process to derives its 32-bit $BD\_ADDR_B = LAP_B \| UAP_B$
11. The 64-bit Initialization Vector *IV* can now be achieved by concatenating BD_ADDR_A and BD_ADDR_B, denoted as $IV = BD\_ADDR_A \| BD\_ADDR_B$, since both parties have each other's address,

Table 4. Resulting BD_ADDR of both Parties

	LAP_A	UAP_A	BD_ADDR_A	LAP_B	UAP_B	BD_ADDR_B
Base 16	12b7d5	48	12b7d548	b7d548	12	b7d54812
Base 2	0001 0010 1011 0111 1101 0101	0100 1000	0001 0010 1011 0111 1101 0101 0100 1000	1011 0111 1101 0101 0100 1000	0001 0010	1011 0111 1101 0101 0100 1000 0001 0010

Hummingbird-2 will require an initialization vector IV to encrypt the input message. In this study, IV is designed to be dependent on two devices, and therefore, it is derived from the information of both devices as shown in Table 4 and Table 5.

Table 5. Initialization Vector based on BD Addresses

Initialization Vector	
	$BD\_ADDR_A \| BD\_ADDR_B$
Base 16	12b7d548b7d54812
Base 2	0001001010110111111010101001000 1011011111010101010100100000010010

12. Alice then calculates it Link key LK_A by hashing the secret key K_{AB} using the MD5 function.
13. Bob also calculate its link key LK_B using secret key K_{BA} as input to the MD5 function.

Table 6. Resulting LK After Applying MD5

LK								
Base 16	3417	3cb3	8f07	F89d	dbeb	c2ac	9128	303f
Base 2	0011 0100 0001 0111	0011 1100 1011 0011	1000 1111 0000 0111	1111 1000 1001 1101	1101 1011 1110 1011	1100 0010 1010 1100	1001 0001 0010 1000	0011 0000 0011 1111

Table 6 shows the digested 128-bit link key *LK* which is essential for a secured transmission of data between the two devices. This *LK* is then encrypted by both parties, resulting to stronger and reliable link keys.

14. Alice uses the Hummingbird-2 algorithm to encrypt the LK_A, denoted as C_A= HB2 (*K*, *IV*, LK_A), and it to Bob.
15. Bob also encrypts its link key LK_B using the Hummingbird-2 algorithm, C_B = HB2 (*K*, *IV*, LK_B), and send it to Alice.

The digested 128-bit secret key *K* and the 64-bit initialization vector *IV* are being used by both parties to encrypt the digested link key *LK* using the Hummingbird-2 encryption algorithm. The resulting ciphered *LK* is shown in Table 7.

Table 7. Hummingbird-2 Vectors

	Base	Hummingbird-2
K	16	9f0aea66365cdca796c1c2c138c6681e
	2	10011111000010101110101001100110 00110110010111001101110010100111 10010110110000011100001011000001 00111000110001100110100000011110
IV	16	12b7d548b7d54812
	2	00010010101101111101010101001000 10110111110101010100100000010010
LK	16	34173cb38f07f89ddbebc2ac9128303f
	2	00110100000101110011110010110011 10001111000001111111100010011101 11011011111010111100001010101100 10010001001010000011000000111111
C	16	763f bac838619e725fcb6097eda0fc7d
	2	01110110001111111011101011001000 00111000011000011001111001110010 01011111110010110110000010010111 11101101101000001111110001111101

16. After receiving the link key of Bob, Alice then decrypts it using the Hummingbird-2 algorithm, denoted as LK_B = HB2(K, IV, C_B), and compare it with its LK_A.
17. Bob decrypts Alice's link key by using the Hummingbird-2 algorithm, denoted as LK_A = HB2(K, IV, C_A), and compare it with its LK_B.
18. The pairing is then considered to be successful if Alice's and Bob's link keys matched with each other.

By using the Diffie-Hellman key agreement protocol, the security of Bluetooth against unit key attack is believed to be strengthened. Guessing of PIN code through PIN cracking attack and Off-line PIN recovery attack will also not be feasible regardless of its length through the use of MD5. The Hummingbird-2, lightweight yet strong, encryption algorithm addressed the current security problem of man-in-the-middle attack while maintaining its advantages in terms of speed, cost and power efficiency.

4. Conclusion

To address the current vulnerabilities of Bluetooth technology, a hybrid pairing protocol has been presented in this study. The combination of Diffie-Hellman Key Agreement Protocol, MD5 and Hummingbird-2 encryption algorithm formed a lightweight but relatively strong pairing protocol that is believed to strengthen the security of Bluetooth communication against known attacks. Moreover, the proposed protocol is well suited for ubiquitous devices and sensor systems that consider data security as priori since it only requires small footprints for it to be implemented.

References

[1] N. B. I Minar and M. Tarique, "Bluetooth Security Threats and Solutions: A Survey", International Journal of Distributed and Parallel Systems, vol. 3, no. 1, **(2012),** pp 127-148.
[2] A. Nayar, "Securing Wireless Bluetooth Sensor Systems", Journal of Computer Applications. vol. 4, no. 1, **(2011),** pp. 4-7.
[3] P. S. Patheja, A. Waoo and S. Nagwanshi, "A Hybrid Encryption Technique To Secure Bluetooth Communication", IJCA Proceedings on International Conference on Computer Communication and Networks, vol. 1, **(2011),** pp. 26-32.
[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, **(2011)**, pp. 567-572.
[5] D. Engels, M. Saarinen, P. Schweitzer and E. Smith, "The Hummingbird-2 Lightweight Authenticated Encryption Algorithm", In Proceedings of the Seventh International Conference of RFID Security and Privacy, Springer-Verlag, Berlin, Heidelberg, **(2012)**, pp 19-31.
[6] Q. Chai and G. Gong, "A Cryptanalysis of Hummingbird-2: The Differential Sequence Analysis", International Association for Cryptologic Research Cryptology, e-Print Archive, **(2012)**, pp. 233.
[7] W. Diffie and M. E. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, vol. IT-22, **(1976)**, pp. 644–654.
[8] S. Lee, H. Latchman and B. Park, "ELRR – Enhanced Limited Round Robin Mechanism using Priority Policy over Bluetooth Network", International Journal of Advanced Science and Technology, vol. 6, **(2009)**, pp. 69 -78.
[9] M. Mana, M. Feham and B. A. Bensaber, "SEKEBAN (Secure and Efficient Key Exchange for Wireless Body Area Network", International Journal of Advanced Science and Technology, vol.12, **(2009)**, pp. 45-60.
[10] R. J. Robles and T. Kim, "A Review on Security in Smart Home Development", International Journal of Advanced Science and Technology, vol. 15, **(2010)**, pp. 13 – 22.

Authors

Jeremias T. Lalis, he received his B.S. degree in Computer Science from La Salle University, Philippines in the year 2005 and M. degree in Information Technology from Cebu Institute of Technology – University of Cebu City, Philippines in 2011. He is currently pursuing his D. degree in Information Technology in Cebu Institute of Technology-University, Philippines. His research interest includes IT security, image processing, machine learning and data mining.

Bobby D. Gerado, he finished his B.S. in Electrical Engineering from Western Institute of Technology, Philippines in 1994, M.A. Ed Mathematics from the University of the Philippines, Diliman in 2000, and Ph.D. in Information and Telecommunications Engineering from Kunsan National University, South Korea in 2007. Now, he is a Faculty of Information Technology and Mathematics at West Visayas State University, La Paz, Iloilo City. His research interests lie on the area of distributed systems, data mining, ubiquitous computing, mobile communications, and Statistics.

Yung-Cheol Byun, he received the B.S. degree in computer engineering from Jeju National University, Korea in 1993. He received the M.S. and Ph.D. degree in computer science from Yonsei University, Korea in 1995 and 2001, respectively. He joined Electronics and Telecom- munications Research Institute (ETRI) as a senior researcher in Fall 2001. He was promoted to join the dept. of Telecommunication and Computer Engineering at Jeju National University in 2002, and he is currently a Full Professor. His research interests include USN and RFID middleware, ubiquitous computing, Location sensing using pattern recognition methods, and intelligent computing.