



## A New Approach to Handel MITM Attack on Secure Simple Pairing

**Chetan N Dave**  
Research Scholar, JJTU,  
India

**Kamaljeet I Lakhtaria**  
Professor, Auro University,  
India

---

*Abstract-Following the increasing confidentiality of data being transferred, many concerns have been raised as to whether Bluetooth transmission is adequately secure. The Bluetooth 2.1 standard introduces a new security mechanism called Secure Simple Pairing (SSP). However, to avoid man-in-the-middle attacks, SSP uses a 6-digit number for authentication. If a human error occurs while conducting visual verification, then data security could be breached. This paper presents a direction of improvement to address this problem. This advancement not only secures consumer privacy, but also increases operational efficiency.*

**Keywords-SSP, Blowfish, Pairing, MITM, DH Key**

---

### I. INTRODUCTION

Bluetooth is relatively new technology. It had been invented in 2000. Bluetooth is named after Danish king Herald Bluetooth. Its primary design goal is to replace cable protocol. It functions without help of internet (Cost) in mobile and is increasing becoming popular for voice/data transfer. Blue tooth often stores a private data which he/she often transfer to his/her laptop privately. Days are not far when office employees will transfer their private data file from their mobile to laptop of a boss or coworker and vice versa. Bluetooth Special Interest Group (SIG) was formed to support and promote this technology. The SIG has over 14,000 members including some leading companies in the fields of telecommunications, computing, automotive, music, industrial automation, and network industries. Bluetooth permits devices to establish either ad hoc or infrastructure networks. Infrastructure networks use fixed Bluetooth access points (AP), which facilitate communication between Bluetooth devices [2].

Bluetooth specification [1] supports the establishment of symmetric keys to allow two devices to securely communicate with each other. The device pairing process comprises authentication, generation of the initialization in key, and generation of the key. Much research has been done on how pairing should be done.

Security has played a major role in the invention of Bluetooth. The Bluetooth [3][4]SIG has put Much effort into making Bluetooth a secure technology and has security experts who provide critical Security information. In general, Bluetooth security is divided into three modes:

(1) Non-secure; (2) Service level enforced security; and (3) link level enforced security.

In non-secure mode, a Bluetooth device does not initiate any security measures. In service-level enforced security mode, two Bluetooth Devices can establish a non secure Asynchronous Connection-Less (ACL) link. And in third security procedures, namely authentication, authorization and optional encryption, are initiated when a L2CAP (Logical Link Control and Adaptation Protocol) Connection-Oriented or Connection-Less channel request is made. The difference between service level enforced security and link level enforced security is that in the latter, the Bluetooth device initiates security procedures before the channel is established. As Mentioned above, Bluetooth's security procedures include authorization, authentication and optional Encryption. Authentication involves proving the identity of a computer or computer user, or in Bluetooth's case, proving the identity of one piconet member to another. Authorization is the process of Granting or denying access to a network resource. Encryption is the translation of data into secret code. It is used between Bluetooth devices so that eavesdroppers cannot read its contents. However, even with all of these defense mechanisms in place, Bluetooth has shown to have some security risks.

Now let us briefly discuss attacks that are possible on Bluetooth despite all the security that their designers claim.

Due to its wireless nature, the Bluetooth communication channel is already subject to several threats like eaves-dropping, impersonation, denial of service and man-in- the-middle. Other than the general wireless protocols' issues, there are the following threats specific to the Blue- tooth enabled devices:

### II. PAIRING

Secure simple pairing which replaced legacy pairing is discussed here. The major difference between Secure Simple Pairing and legacy pairing is that legacy pairing authenticates via PIN entry, while Secure Simple Pairing authenticates by visual number confirmation. The visual number confirmation is used by Secure Simple Pairing to prevent man-in-the-middle attacks caused by the Elliptic Curve Diffie-Hellman (ECDH) protocol.[5]

As shown in Figure 1, the ECDH is a key exchange protocol utilised to establish a shared key between two connecting devices. Each connecting device starts generating its own random number (device A with SKa, device B with SKb) as its private key, computes the corresponding public key (device A with PKa, device B with PKb), and then send its public key to the other device. Now each connecting device can derive DHKey with its secret key and the received public key. The shared key DHKey can be used as a session key to encrypt all the data transferred between the two connecting devices.

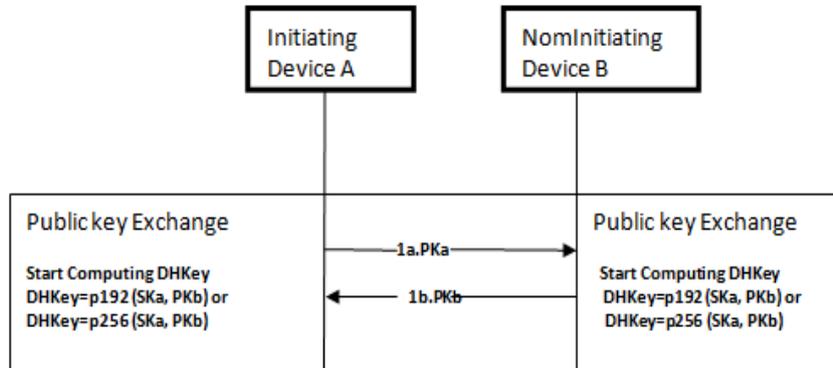


Fig 1. Initial Public Key Exchange in SSP.

**A. Weaknesses of Secure Simple Pairing**

The ECDH key exchange protocol is used by Secure Simple Pairing to provide confidentiality for the data being transferred. However, because the senders of the public keys (PKa, PKb) are not authenticated, the protocol is subject to the man-in-the-middle attack [7]. As shown in Figure 3, the attack works as follows. When A sends PKa to B, an attacker C intercepts this value and impersonates B by replying PKc to A. At the same time, C pretends to be A and sends B the value PKc, and then intercepts the respondent’s value PKb from B. The result is that C and A share  $P192 (SKa, PKc) = P192 (SKc, PKa)$ , C and B share  $P192 (SKc, PKb) = P192 (SKb, PKc)$ , but A and B mistakenly think they have successfully agreed.

On a shared key  $P192 (SKa, PKb) = P192 (SKb, PKa)$ . Then the attacker C can relay messages between A and B, making them believe that they are talking directly to each other over a private connection where in fact the entire conversation is controlled by the attacker.

SSP is completed in 6 phases and 1<sup>st</sup> phase involves exchange of public key via air in unsecured manner. The standard practice for Man-In-The-Middle Attack is that Attacker jams the physical layer and forces user to work for just works association model of SSP. When user deletes the Link key SSP is restarted, and attacker (in above figure C) establish pairing with 2 victim devices. Actually attacker use 2 separate Bluesnifer (Attack Device) having capability of adjusting Bluetooth Addresses.

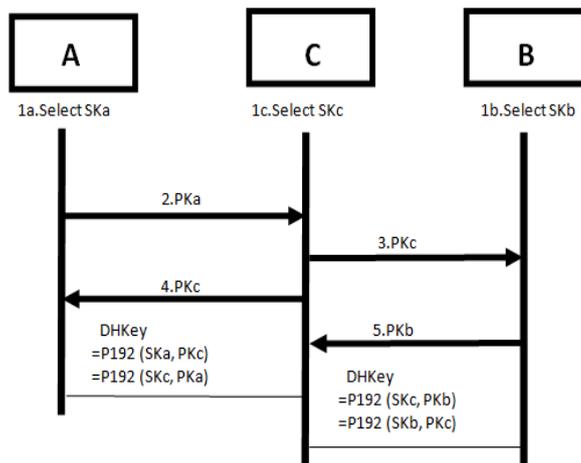


Fig 2.MITM Attack on Secure Simple Pairing.

**III. RELATED LITERATURE**

IT is a proven fact that Secure simple pairing is not so secure and man in the middle attacks are possible on it.[1,2,3,4,16]. All these man in the middle attacks are based upon certain facts. 1<sup>st</sup> attacker jams the physical channel, frustrated user deletes previously stored link key. During this Attacker device clones BD\_ADDR of victim devices, these addresses can be adjusted by device like Bluetooth sniffer. Than Attacker impersonates real users and starts pairing with victim devices and thus controls their communication.

In one such attack [24] attacking devices secure simple pairing till ssp reaches the stage of nounc exchange. Then channel can be jammed thus breaking the running pairing process. Till now Attacker collected all information required for impersonation and then as channel is jammed, Users are compelled to restart pairing. And then attacking device will be paired with victim devices. Here users do not delete stored linked key.

Suggestion to overcome above problems is that there should be an additional user side window to confirm pairing, use of 3<sup>rd</sup> party sensor or server which is not possible when only 2 Bluetooth devices are being connected. Additional user window will compromise usability. Most of researchers agree for use of OOB channel for security [1,2,3,4,16,24], but it is concluded that all pairing methods (e.g. compare & confirm, compare & select) require rethinking not from usability perspective but also from a security standpoint [8] as All these methods have some security failure.

Above facts led many researchers for either replacing ssp or improving ssp. A use of flashing light as a visual channel for pairing [5]. All Bluetooth devices cannot have flashing light, It is costly for users. A hybrid pairing [8] suggested, combination of Diffie-Hellman Key Agreement, MD5, Hummingbird2, instead of ssp. Bluetooth device has low processing power, Combination of such heavy protocol requires heavy processing power, There is also an idea of detecting man in the middle attack during 2<sup>nd</sup> stage of ssp [9], For that he suggested use of some cryptography before ssp starts, same thing suggested by [22]. But none of them have specified, which cryptography function should be used before ssp starts. ESSP [21] has also been suggested use of databases for storing link key (authentication records), fine user deletion won't have any impact but what if attacker succeeds in knowing key stored in database somehow. Here also there is a provision for encrypting public key, but which cryptographic function should be used is not clear.

There is also a proposal for using a combination key, encryption will be done on it using 128 bit random number [23], his solution gives protecting against PIN guessing attack but not against man-in-the-middle attack. His proposed solution also cannot be used with existing ssp.

There is also a proposal for using security token [10], But again for issuing security token you need 3<sup>rd</sup> party (a server) not advisable for piconet (a group of at most 7 Bluetooth devices) or even for 2 pairing device. A concept of individual key and group key and pair key presented [12] which need to be studied further. There is also a proposal for using zero knowledge proof but again requirement of a base station is there [15]. A key distribution scheme is also proposed in which each message will be encrypted with key [19].

Improving pairing will also have an impact on home security (An electronic home) [13]. Min-kyu Choi suggest systematic and effective approach for managing the risk [11]. A concept of global key was presented [12] which can be useful for securing piconet. There are certain suggestions emphasize smartness or eagerness to achieve security [14]. There must be an emphasize on power and energy while devising a security algorithm [15]. There are active attack, passive attack, routing attacks, transport layer attacks on adhoc network [17]. All Bluetooth securities and challenges are explored [25].

Lots of comparison type research work has also taken place for pairing methods. Simple number comparison is quite attractive overall being fast and secures [7]. A tool is also devised for comparing different pairing methods [18]. Vibrate Button or LED button is best suited for devices lacking screens, HAPAADEP is useful when one device has a speaker and other has a microphone [20]. Here also Number comparison is quite attractive method.

#### IV. OUR PROPOSED SOLUTION

We suggest that no of successful transactions should be maintained on both devices. In case where both devices are being paired 1<sup>st</sup> time an artificial number (eg. 999 Or 9999) can be utilized. Just like devices store the link key, this "total number of successful tranjections", we will call it Nt, can be stored or database can be also used. This Nt will be incremented each time; the successful tranjections will take place. Then we can use modified version of Blowfish algorithm to encrypt public key of each device using Nt as key.

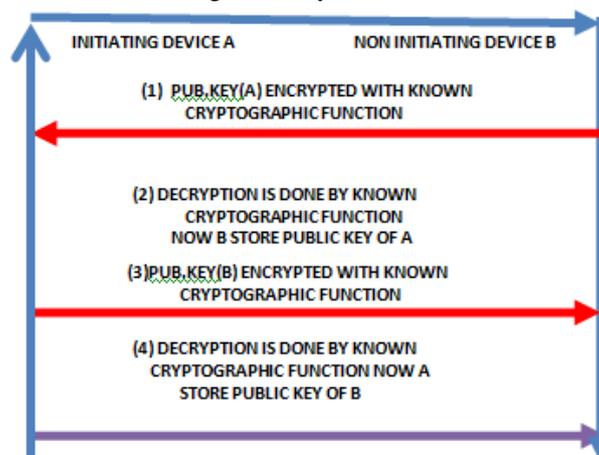


Fig 3. Apply Encryption on 1<sup>st</sup> phase of SSP.

The reason for selecting Blowfish is its shorter block size. And here Just Public key needs to be encrypted. This algorithm has key expansion feature which is ideal for Nt taking into consideration no of Bluetooth tranjections. We propose block size of 32 bits. And it can be secure as there are going to be less than 116 data blocks for public key in any case. Blowfish is not subject to any patents and is therefore freely available for anyone to use. This has contributed to its popularity in cryptographic software. Blowfish has a relatively large memory footprint of just over 4 kilobytes of RAM. This is not a problem even for older smaller smart phones and Bluetooth devices. The modified Blowfish algorithm can be described as follow.

=>initialize P-array and s-boxes.  
=>Xor P-Array with key bits. For ex. P Xor (first 16 bits of key), P Xor (second 16 bits of key).  
=>new output are P1 and P2.  
=>Encrypt new P1 and P2 with modified subkey.  
=>now output is P3 and P4.

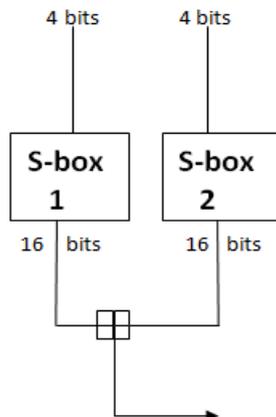


Fig 4. Apply Modified Blowfish for initial exchange off public key

Attacker can have no idea of successful tranjections that took place between 2 parties or in case of 1<sup>st</sup> pairing it is difficult to anticipate Nt and suppose attacker even guessing Nt then this Blowfish is quite difficult to crack when only less then at most 100 data blocks are being transferred. It is right that Attacker can jam the physical layer, but after it when it tries to start pairing with victim device, attacker will not succeed because of Modified Blowfish and thus attacker will get frustrated.

## V. CONCLUSION & FUTURE WORK

Blowfish algorithm should be tested practically and it should be tested in terms of how much time it takes. Appropriate P-array and S-Box should be designed so that whole process consumes less memory and works speedily. Blowfish algorithm can just be applied to transfer of public key. Possibility of applying Blowfish Algorithm as alternative of SSP should also be explored.

## REFERENCES

- [1] Konstantin Hypponen, Keijo M.J. Haataja, 2007, "Nino Man-In-The-Middle Attack on Bluetooth Secure Simple Pairing", 3rd IEEE/IFIP International Conference in Central Asia on Internet, Vol: issue: 1, pp.1-5.
- [2] Sanna Pasanen, Keijo Haataja, (2008), "Man-In-The-Middle Attacks on Bluetooth, a Comparative Analysis, a Novel Attack, and Countermeasures", ISCCSP, IEEE, pp.1096-1102
- [3] Keijo Haataja, Pekka Toivanen, (2010), "Practical Man-In-The-Middle Attacks against Bluetooth Secure Simple Pairing", Wireless Communications, IEEE Transactions on (Volume:9 , Issue: 1 ) pp.384 - 392
- [4] Arun Kumar, Nitesh Saxena, (2009), "Caveat eptor: A Comparative Study of Secure Device Pairing Methods", Pervasive Computing and Communications. Percom 2009. IEEE International Conference on, pp.1-10.
- [5] Nitesh Saxena, (2006), "Secure Device Pairing Based on a Visual Channel", Security and Privacy, 2006 IEEE Symposium on, pp. 313-318.
- [6] Ronald Kainda, Ivan Flechais, A.W. Roscoe,(2009), "Usability and Security of Out-Of-Band Channels in Secure Device Pairing Protocols", SOUPS '09 Proceedings of the 5th Symposium on Usable Privacy and Security ,ACM New York.article-11.
- [7] Arun Kumar, Nitesh Saxena, Gene Tsudik, Ersin Uzun,(2009), " A Comparative Study of Secure Device Pairing Methods", Pervasive and Mobile Computing Volume 5 Issue 6, December, 2009.pp. 734-749.
- [8] J. T. Lalis, B. D. Gerardo and Y. Byun, 2014, "Securing Bluetooth Communication with Hybrid Pairing Protocol", International Journal of Security and Its Applications Vol: 8, No.4, pp.219-228.
- [9] Praveen Kumar Mishra, 2013, "Analysis of MITM Attack in Secure Simple Pairing", Journal of Global Research in Computer Science Vol: 4, No. 2, pp.42-45.
- [10] Carsten Maple, Geraint Williams and Yong Yue, 2007 "Reliability, Availability and Security of Wireless Networks in the Community", Informatica, pp.201-208.
- [11] Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, 2008 "Wireless Network Security, Vulnerabilities, Threats and Countermeasures ", International Journal of Multimedia and Ubiquitous Engineering, Vol: 3, No. 3, pp.77-86.
- [12] Delan Alsoufi1, Khaled Elleithy, Tariq Abuzaghle and Ahmad Nassar, (2012), " Security in Wireless Sensor networks –Improving the Leap Protocol", International Journal of Computer Science & Engineering Survey, Vol:3, No.3, pp.1-14.
- [13] Prof. (Dr.) Khanna SamratVivekanand Omprakash, 2009, " Wireless Home Security System with Mobile", International Journal of Advanced Engineering Technology, Vol: 2, Issue 4, pp.396-397.

- [14] Anthony C. Ijeh, Allan J. Brimicombe, David S. Preston, Chris .O. Imafidon, 2009, “*Security Measures in Wired and Wireless Networks*”, Proceedings of the Third International Conference on Innovation and Information and Communication Technology, vol:4 pp.113-121.
- [15] Raj Kumar Singh<sup>1</sup> Dr.A.K.Jain<sup>2</sup>, 2012,”*Research Issues in Wireless Networks*”, International Journal of Advanced Research in Computer Science and Software Engineering Vol: 2 Issue: 4, pp.115-119.
- [16] Mr.K.Saravanan, Vijay Anand, R.K. Negesh, 2012,” *A Novel Bluetooth Man-In-The-Middle Attack Based on SSP using OOB Association model*”, <http://www.arxiv.org/pdf/1203.4649>.
- [17] Mahendra Kumar, Ajay Bhushan, Amit Kumar,2012, “*A Study of Wireless Ad-Hoc Network Attack and Routing Protocol Attack*”, International Journal of Advanced Research in Computer Science and Software Engineering, Vol: 2 Issue 4,pp. 30-33.
- [18] Yasir Arafat, Malkani and Lachhman Das Dhomeja, 2009, “*A Tool for Analysis of Device Pairing methods*”, International Journal of Network Security & Its Applications, Vol: 1, No.3, pp.127-148.
- [19] C. Krishna Kumar, G. Jai Arul Jose, C. Sajeew and C. Suyambulingom, 2012, “*Safety measures against MITM Attack in Key Exchange*”, ARPN Journal of Engineering and Applied Sciences, vol.:7, no. 2, pp.243-246.
- [20] Arun Kumar, Nitesh Saxena, Gene Tsudik, Ersin Uzun, 2009,” *A Comparative Study of Secure Device Pairing Methods*”, ELSEVI Pervasive and Mobile Computing vol: 5 pp. 734-749.
- [21] Iman AL Momani, Mohammed Al-Saruri, Mousa AL-Akhras, 2011, “*Secure Public Key Exchange Against MITM Attacks During Simple Secure Pairing (SSP) in Bluetooth*”, World Applied Sciences journal vol: 13, pp.769-780.
- [22] Nishant Mishra, Vishal. Gupta, 2012, “*Defense against MITM Attack in Secure Simple Pairing*”, Journal of Global Research in Computer Science, Vol: 3, No. 5, pp.78-82.
- [23] Tarun Kumar, (2009),” *Improving Pairing Mechanism in Bluetooth Security*”, International Journal of Recent Trends in Engineering, Vol 2, No. 2, pp.165-169.
- [24] Johannes Barnickel, Jian Wang,Ulrike Meyer,(2012),” *Implementing an Attack on Bluetooth 2.1+ Secure Simple Pairing in Passkey Entry Mode*”, Proceeding TRUSTCOM '12 Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, IEEE Computer Society, pp. 17-24.
- [25] Nishant Mishra, 2, Vishal. Gupta, 2012,” *An Overview of Bluetooth Security: Issues and Challenges*“, March, Journal of Global Research in Computer Science, Vol: 3, No. 3 pp.73-77.