Analysis of Bluetooth Threats and v4.0 Security Features

Sandhya S
Department of MCA
RV College of Engineering
Bangalore, India
sandhyas@rvce.edu.in

Sumithra Devi K A
Department of MCA
RV College of Engineering
Bangalore, India
sumithraka@gmail.com

Abstract— **The advent of Bluetooth technology has made wireless communication easier. Any new invention or improvement is viewed very closely by people who are looking to gain information in an unauthorized manner. Security in any area is given more importance as it leads to better product and satisfied customers. The initial days of any technological invention is more challenging as they deal with new issues every day. The product/ invention needs to keep evolving to address the growing list of new features requirement and handling of security issues. Bluetooth security has evolved a lot with different versions of blue tooth. Keeping in mind the growing list of Bluetooth products in the market, there has been lot of improvements done in the version 4.0 of Bluetooth. The LE (Low Energy) operational mode which is new in version 4.0 has slightly different security association models. In this paper, a review of the recent studies in the analysis of Bluetooth security issues and new security features of v4.0 is done. Specifically the paper covers secure simple pairing in Bluetooth normal mode and low energy mode. For each threat, the particular issues are addressed and a review of major approaches to improve security of Bluetooth communication using secure simple pairing is discussed.**

Keywords- ***Bluetooth Low Energy, Secure Simple Pairing, Association Models, Man in the Middle***

I. INTRODUCTION

Bluetooth is a wireless communication technology for short range communications. Blue tooth was designed for low power consumption and data transfer in moderate rate over short ranges. The system operates in the 2.4 GHz ISM Band. This frequency band is 2400 – 2483.5 MHz. The technology allows the formation of Adhoc networks called piconets between two or more wireless devices. The connected devices communicate on the same physical channel with a common clock and hopping sequence. A number of independent piconets may exist in close proximity. This will mean that each piconet will have a different master device and an independent timing and hopping sequence. A blue tooth device may participate in two or more piconets at the same time. This is achieved using a process called time-division multiplexing. A blue tooth device cannot be a master of more than one piconet. But it can be a slave in many independent piconets [1].

Bluetooth security works on the basis of authentication and encryption. There are four security modes in Bluetooth which are Security Mode 1, Security Mode 2, Security Mode 3 and Security Mode 4. Mode 1 does not require authentication or encryption. Mode 2 uses authentication and encryption only for individual service communication such as file transfer or synchronization. Mode 3 enforces authentication and encryption before the link is established and hence all the traffic will be encrypted. Mode 4 uses secure simple pairing method to create service level security [2].

The remainder of this paper is devoted to look at the studies done in the analysis of Bluetooth security issues. Section 2 overviews the list of Bluetooth threats and the classification of these threats as per [2]. Section 3 overviews the process of secure simple pairing and how it can be used to fight passive and active eavesdropping threats. Section 4 discusses the various association models used in secure simple pairing. Section 5 reviews the recent security studies done on secure simple pairing and suggests the association models that could be used in various scenarios.

II. BLUETOOTH SECURITY THREATS

Bluetooth hacking has gained a lot of momentum these days. With the release of new version blue tooth (4.0), some of these threats have been taken care of. One must member that this protection is available automatically only to Bluetooth products that supports the latest version. The other products that have been in use that are based on legacy versions of Bluetooth still are vulnerable to attacks. As there are many different threats present, classifying these threats becomes very important. Classification can help in determining threat severity, measures that could be taken to avoid them and taking inputs for the next version to avoid this threat by design.

In the survey of Bluetooth threats by John Paul Dunning [2], the threats are classified based on a framework called “A Bluetooth Threat Taxonomy” (Aboott). This consists of nine different classes many of which are part of the cyber security standard terminology. The classifications are surveillance, range extension, obfuscation, fuzzer, sniffing, denial of service (DoS), malware, unauthorized direct data access (UDDA) and man in the middle (MITM). The paper also explains each of these classes in detail and gives a gist of attack classification in the form of a table which is given below in Table.1

Attack Classification	Threats
Surveillance	Blueprinting, bt_audit, redfang, War-nibbling, Bluefish, sdptool, Bluescanner, BTScanner
Range Extension	BlueSniping, bluetooone, Vera-NG
Obfuscation	Bdaddr, hciconfig, Spooftooph
Fuzzer	BluePass, Bluetooth Stack Smasher, BlueSmack, Tanya, BlueStab
Sniffing	FTS4BT, Merlin, BlueSniff, HCIDump, Wireshark, kismet
Denial Of Service	Battery exhaustion, signal jamming, BlueSYN, Blueper, BlueJacking, vCardBlaster
Malware	BlueBag, Caribe, CommWarrior
Unauthorized Direct Data Access	Bloover, BlueBug, BlueSnarf, BlueSnarf++, BTCrack, Car Whisperer, HeloMoto, btpincrack
Man In The Middle	BT-SSP-Printer-MITM, BlueSpooof, bthidproxy

Table 1. Bluetooth Attacks [2]

The author in paper [2] also discusses the threat levels for every classification. The threat levels are given in Table 2. John Paul Dunning [2] concludes by giving a detailed set of steps that can be taken by the vendors/specification and the end users to try and reduce the threats as much as possible.

Attack Classification	Threat Level
Surveillance	*Low*: Main purpose is to observe and gather information about the device and its location
Range Extension	*Low*: Main purpose is to extend the device range so that attacks could be conducted from far way distance
Obfuscation	*Low*: Main purpose is to hide the attacker's identity.
Fuzzer	*Medium*: Main purpose is to submit non standard input to get different results.
Sniffing	*Medium*: Main purpose is to capture the Bluetooth traffic in transit.
Denial Of Service	*Medium*: Main purpose is to deny resources to a target by saturating the communication channel.
Malware	*Medium*: Main purpose is to carry out attacks typically using self replicating form of software.
Unauthorized Direct Data Access	*High*: Main purpose is to gather private information in an unauthorized manner. This is very serious as very important information can be stolen.
Man In The Middle	*High*: Main purpose is to place a device between two connected devices. All the information sent through the channel are available to the device in between.

Table 2. Threat Levels [2]

Figure 1 Shows the threat levels in a pie chart

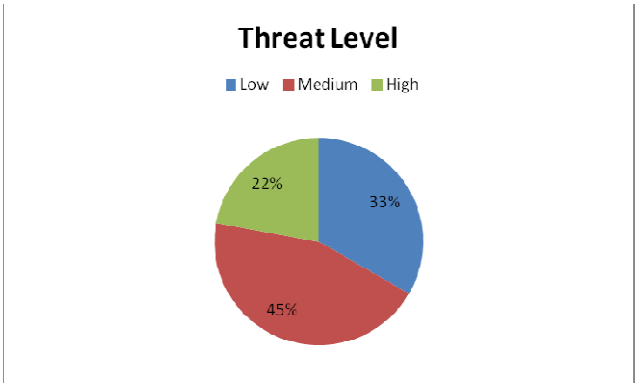

Fig 1. Threat Level Pie Chart

III. SECURE SIMPLE PAIRING

When two Bluetooth devices want to communicate with each other, there needs to be a process of authentication and establishing of a shared link key which is obviously secret. This key is used to secure subsequent communication between the devices. This process is called pairing and the process in v4.0 is called Secure Simple pairing. The primary goal of secure simple pairing is to simplify the pairing procedure for the user. The secondary goal is to improve the security in Bluetooth technology [1]. The SIG has taken enormous care to maximize security while minimizing the end user complexity. There are two security goals for the pairing process, protection against passive eavesdropping and protection against man-in-the-middle (MITM) attacks. To maximize security, this process uses a 16 alphanumeric PIN. The Bluetooth version 2.0 + EDR and earlier versions use a 4 digit PIN or a fixed PIN Passive Eavesdropping Protection.

A strong link key coupled with strong encryption algorithm is necessary to give protection against passive eavesdropping. The link key strength is based on the randomness in the PIN. If a four digit PIN is used, then it can be very easily cracked as the permutations and combinations are not huge and can be done very quickly using an algorithm. The secure simple pairing gives the same protection against recording and passive eavesdropping attacks even when the user is not required to do anything. Secure Simple pairing uses Elliptic Curve Diffie Hellman (ECDH) public key cryptography as a means to protect passive eavesdropping attacks. Though this provides a very high degree of protection against passive eavesdropping, it may be subject to MITM attacks which are harder to perform than passive eavesdropping.

A. Man In The Middle Protection

A man in the middle attack occurs when a user wants to connect two devices but instead of connecting with each other they unknowingly connect to a third device. The third device

then relays the information between the two devices. In this attack, all the information sent between the two devices is compromised. Secure simple pairing offers two user assisted numeric methods to prevent MITM attacks: numerical comparison or passkey entry. This protects the user from MITM attacks by using a six digit number for numerical comparison and pass key entry.

IV. Association Models

The association model definitions as stated in [1] are given below. Secure simple pairing uses four association models referred to as Numeric Comparison, Just Works, Out of Band and Passkey entry. The appropriate model is chosen based on the input/output capabilities of the two devices.

A. Numeric Comparison Model

The numeric comparison model is used where both the devices are capable of displaying a six digit number and both of them allow the user to enter a "yes" or "no". The user has to say yes or no to indicate if the six digit numbers shown on their device is same or not. If yes in entered in both the devices then pairing is done. The numeric comparison provides protection against MITM attacks.

B. Just Works Model

This model is primarily used for scenarios where one of the devices does not have a capability to display 6 digit numbers. They also do not have the capability to enter 6 digits. This uses the numeric comparison protocol and the application may connect based on user acceptance. This provides protection against passive eavesdropping but no protection against MITM.

C. Out of Band Model

This is designed for scenarios where an out of band mechanism is used to discover both the devices and also to exchange cryptographic numbers used in the pairing process. In order to be secure, the out of band channel should provide different security properties than the Bluetooth radio channel. The out of band channel should be resistant to MITM attacks.

D. Passkey Entry Model

This is designed for scenario where one device has the input capability but does not have the capability to display six digits and the other device has output capabilities. The user is shown six digits and asked to enter in the other device. If the value entered is correct, then pairing is successful.

Association models for Bluetooth LE are referred to as Just Works, Out of Band and Pass key entry. Bluetooth LE does not have an equivalent of numeric comparison. Just works and passkey entry do not provide any passive eavesdropping protection. This is because of the fact that SSP uses Elliptic Curve Diffie Hellman and LE does not use the same.

V. Related Work

Kuo et al. [12] briefly looks at the potential security risks of Bluetooth considering that it supports multiple setup mechanisms. A remark about a security issue for SSP in the Passkey Entry model in terms of passkey leakage was also mentioned en passant therein, as was later independently observed by Lindell [13, 14]. Their observations relate to potential password leakage, yet the passkey in the Bluetooth context is different from a conventional password in that a passkey is mainly used for authentication rather than secrecy; and its existence is to add an extra security factor to the pairing authentication between Bluetooth parties. Thus, even if the passkey is guessable, SSP in the PE model remains secure unless all of its stages are vulnerable to attack. Suomalainen et al. [19] gives a comparative overview of different pairing models in personal networks including Bluetooth. They identify as a potential attack scenario where the security of a more IO-capable device is compromised by having it interact with another device of restricted IO-capability e.g. one without display capability. Chang and Shmatikov [5] applied a formal methods tool to analyze the authentication aspect of SSP in the numeric comparison model, and showed that if the same device is used concurrently in different sessions then authentication fails. This is because even if the user correctly checks that the numbers displayed on both devices are equal, they may not necessarily be involved in the same intended session.

Haataja et al. [7–10] exploited the fact that prior to SSP the devices exchange their respective input/output capabilities without any authentication, and so describe that one could modify these exchange messages to force devices to use the Just Works (JW) association model whose SSP is not designed to resist MitM attacks, thus leading to an MitM attack on the devices.

Raphael and Patrick [3] have done an extensive analysis of the different association models with respect to secure simple pairing in Bluetooth 4.0 for both (BR/EDR) and LE operational modes. Each model has been evaluated based on the common security properties required [3]. The SSP is in fact similar to authentication [17,20] and key establishment (AKE) [18] protocols, and therefore we consider the following basic security properties required of such protocols [15].

• Known key security (KKS) [15]: Compromising a session key does not leak out other session keys.

• Key control (KC) [15, 16]: No device should be able to influence a link key to some biased value.

• Perfect forward secrecy (PFS) [15]: If long-term secrets or private keys of any device are compromised, the secrecy of previously established session keys should not be affected.
This attempts to still offer some security guarantee in spite of the fact that the long-term secret has been leaked.

• Key-compromise impersonation (KCI) resilience [4,11]: The compromise of any device A's long-term key or secret should not enable the attacker to impersonate any other devices to A.

• Unknown key-share attack (UKS) resilience [6,15]: UKS is an attack where a device A believes that it shares a key with another device B upon completion of a protocol run (this is in fact the case), but B falsely believes that the key is instead shared with a device E _= A.

• Man-in-the-Middle (MitM) attack resilience: For any protocol where devices desire to authenticate each other, it should not be possible for an attacker to place himself in the middle of the two devices and cause them to have false beliefs about how the protocol actually executed.

The summary of the study done by Raphael and Patrick [3] is given below. OoB is the best choice if the underlying OoB channel is secure. NC can be used if no secure OoB channel exists other than a human being able to view the screen and press "yes"/"no" in each device. Despite that the SSP for Bluetooth BR/EDRwas designed with multi-factor authentication layers, namely the use of elliptic curve public-private keys to protect the secrecy of the established DH key, and the use of out-of-band SAS to provide authentication of communicated protocol message transcripts without needing a PKI; They also highlight the fact that key substitution attacks are possible on the DH key exchange of Bluetooth BR/EDR's SSP leads to cases where an adversary computes the shared DH key and subsequently has less obstacles in bypassing the security mechanisms within the SSP, i.e. he has one less authentication factor to worry about. In contrast, the Bluetooth LE does not exhibit this problem since the DH key is not used. Furthermore, the non-usage of the DH key in Bluetooth LE also means that compromise of the long-term private key does not affect the shared secret between Bluetooth parties. Indeed, the gist of the PFS, KCI and MitM attacks on Bluetooth BR/EDR exploit the fact that the private key directly influences the shared DH key; hence Bluetooth LE is not affected by PFS, KCI or MitM attacks. They also suggest that SSP to have its stage 1 via an out of band authenticated channel involving the human user to setup the initial trust in each device's public key, so that key substitution attacks are prevented. This will in turn avoid all the UKS and MITM security issues.

VI. Conclusion

Bluetooth is a very remarkable technology for communicating the wireless way. It is critical that the version 4.0 undergo a continual security analysis process by people involved. Considering that Bluetooth devices are slowly getting used to transmit lot of data, an integrated approach is needed to protect data privacy and to prevent misuse of data. Some of the existing usage scenarios can be analyzed from the perspective of data privacy and prevention of data misuse using Bluetooth v4.0 features.

References

[1] Bluetooth, S. I. G. (2010). Bluetooth Core Specification v4.0. 30 June 2010 Available online at https:// www. bluetooth.org /Technical /Specifications/adopted.htm

[2] John Paul Dunning (2010). Taming the blue beast: A Survey of Bluetooth-Based Threats. Security & Privacy, IEEE

[3] Raphael C.-W. Phan, Patrick Mingard. (2010). Analyzing the Secure Simple Pairing in Bluetooth v4.0, Springer

[4] Boyd, C., & Mathuria, A. (2003). Protocols for authentication and key establishment. Berlin: Springer

[5] Chang, R., & Shmatikov, V. (2007). Formal analysis of authentication in bluetooth device pairing. Proceedings of LICS/ICALP workshop on foundations of computer security and automated reasoning for security protocol analysis (FCS-ARSPA '07), July.

[6] Diffie, W., van Oorschot, P. C., & Wiener, M. J. (1992). Authentication and authenticated key exchange. Designs, Codes and Cryptography, 2, 107–125.

[7] Haataja, K., & Toivanen, P. (2008). Practical man-in-the-middle attacks against bluetooth secure simple pairing. Proceedings of IEEE international conference on wireless communications, networking and mobile computing (WiCOM '08) (pp. 1–5).

[8] Haataja, K., & Toivanen, P. (2010). Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures. IEEE Transactions on Wireless Communications, 9(1), 384–392.

[9] Hyppönen, K., & Haataja, K. (2007). Niño Man-in-the-Middle Attack on Bluetooth Secure Simple Pairing. Proceedings of IEEE international conference in Central Asia on Internet (ICI '07) (pp. 1–5).

[10] Hyppönen, K., & Haataja, K. (2008). Man-in-the-middle attacks on bluetooth: A comparative analysis, a novel attack, and countermeasures. Proceedings of IEEE international symposium on communications,coding and signal processing (ISCCSP '08) (pp. 1096–1102).

[11] Just, M., & Vaudenay, S. (1996). Authenticated multi-party key agreement. In Advances in Cryptology— Asiacrypt '96, LNCS 1163 (pp. 36–49).

[12] Kuo, C., Walker, J., & Perrig, A. (2007). Low-cost manufacturing, usability, and security: An analysis of bluetooth simple pairing and Wi-Fi protected setup. Proceedings of international conference on usable security (USEC '07) (pp. 325–340).

[13] Lindell, A. (2008). Bluetooth v2.1—A new security infrastructure and new vulnerabilities. BlackHat Briefings, Las Vegas.

[14] Lindell, A. (2008). Attacks on password pairing in bluetooth v2.1. CSI '08, Maryland.

[15] Menezes, A. J., Oorschot, P. C.van , & Vanstone, S. A. (1997). Handbook of applied cryptography. BocaRaton: CRC Press.

[16] Mitchell, C. J., Ward, M., & Wilson, P. (1998). Key control in key agreement protocols. IEE Electronics Letters, 34(10), 980–981

[17] Moon, J. S., Park, J. H., Lee, D. G., & Lee, I.-Y. (2010). Authentication and ID-based key management protocol in pervasive environment. Wireless Personal Communications, 55(1), 91–103.

[18] Ntantogian, C., & Xenakis, C. (2009). One-pass EAP-AKA authentication in 3G-WLAN integrated networks. Wireless Personal Communications, 48(4), 569–584.

[19] Suomalainen, J., Valkonen, J., & Asokan, N. (2007). Security associations in personal networks: A comparative analysis. Proceedings of European workshop on security and privacy in ad-hoc and sensor networks (ESAS '07), LNCS 4572 (pp. 43–57).

[20] Yoon, E.-J., Yoo, K.-Y., Yeo, S.-S., & Lee, C. (2010). Robust deniable authentication protocol. Wireless Personal Communications, 55(1), 81–90.