International Journal of Security and Its Applications
Vol.8, No.3 (2014), pp.1-8
http://dx.doi.org/10.14257/ijsia.2014.8.3.01

An Architecture Design for Wireless Authentication Security in Bluetooth Network

Bijoy Kumar Mandal[1], Debnath Bhattacharyya[1] and Tai-hoon Kim[2*]

[1]Department of Computer Science and Engineering, Faculty of Engineering and Technology, NSHM Knowledge Campus – Durgapur,
Durgapur-713212, India
[2]Department of Convergence Security, Sungshin Women's University,
249-1, Dongseon-dong 3-ga, Seoul, 136-742, Korea
[1]{writetobijoy,debnathb}@gmail.com, [2]taihoonn@daum.net

Abstract

Bluetooth technology has become an integral part of this modern society. 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. Bluetooth communication range is categorized as high, medium and low depending upon power level. High range of Bluetooth communication is up to 91 meter, medium range is up to 9 meter and low range is up to 1 meter. Authentication and Encryption are the key security features that are used in Bluetooth communication. In this paper, we present architecture for authentication security of Bluetooth. The main goal of this paper is to design architecture of security for Bluetooth in real scenarios. In order to find out the major vulnerabilities in modern wireless Bluetooth-enabled devices that has performed successfully for several attacks such as Unauthorized Direct Data Access (UDDA) and Man-in-the-Middle Attack (MITM). This form of authentication presents an interesting modeling challenge. We discuss the implications of this authentication security for typical Bluetooth usage scenarios.

Keywords: *Bluetooth Security, MITM, UDDA, SIG, ACO, Link Key, PIN*

1. Introduction

Bluetooth, a new technology named after the 10th century Danish king Harald 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 radios are becoming ubiquitous in mobile devices such as cell phones, laptops, and even many modern cars. Over one billion Bluetooth enabled devices have been shipped to date [1]. These devices are often used to store users' private data. For example, a user may enjoy the convenience of being able to wirelessly transfer contact data between his or her laptop and a mobile phone, but probably does not want that contact data to be publicly available to all Bluetooth devices in range. The Bluetooth specification [2] 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. Bluetooth

[*] Corresponding Author

ISSN: 1738-9976 IJSIA

technology has been considered as a cheap, reliable, and power efficient replacement of cables for connecting electronic devices. This technology was officially approved in the summer of 1999 [3]. Since then it has widely been used in various electronic devices. Bluetooth Special Interest Group (SIG) was formed to nurture 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 [4]. 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. This document focuses on ad hoc piconets, which are much more common than infrastructure networks. Ad hoc networks provide easy connection establishment between mobile devices in the same physical area (*e.g.*, the same room) without the use of any infrastructure devices [5]. A Bluetooth client is simply a device with a Bluetooth radio and software incorporating the Bluetooth protocol stack and interfaces. Bluetooth can also be used to form ad hoc networks of several (up to eight) devices, called piconets. This can be useful for example in a meeting, where all participants have their own Bluetooth compatible laptops, and want to share files with each other [6]. Bluetooth offers several benefits and advantages, but the benefits of Bluetooth are not provided without risk. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification and resource misappropriation [7, 8]. Our main contribution is a formal, tool-supported security analysis of two Bluetooth device pairing protocols. The Simple Pairing protocol presents an interesting challenge to formal verification methods because it relies on out-of-band, human authentication (explained in more detail below). Human-verifiable protocols based on image- or audio-matching are becoming increasingly popular for mobile device authentication [9, 10, 11]. Although cryptographic security proofs have been manually derived for similar protocols [12, 13], we view our work as the initial step in applying formal methods to this class of protocols. Informally, the security properties we verify for both pairing protocols are [13] key secrecy for the initialization key [14] and authentication of session participants. Intuitively, our key secrecy property states that upon successfully completing a device pairing between devices A and B, the initialization key is known only to A and B. Our authentication property states that, if A has completed a device pairing in which A believes that it has successfully paired with B, then it has indeed paired with B (and vice versa).

The main part of this paper is devoted to the analysis of the Simple Pairing protocol, which was designed to rectify vulnerabilities caused by the use of low-entropy secrets in the standard pairing protocol. For key establishment, Simple Pairing uses plain, unauthenticated Diffie-Hellman key exchange. Authentication relies on an interesting out-of-band mechanism. Each device computes a short cryptographic hash of the established key and displays it on the device's screen. The two devices' owner(s) visually compares the displayed values and manually confirms that they match. In other words, authentication is done via key confirmation on a secure human channel, *i.e.*, a human "equality oracle". In this paper, we present the first formal architecture for this type of authentication. While there are other protocols in the literature that employ similar human authentication mechanisms to the best of our knowledge none of them have been formally analyzed.

2. Bluetooth Security

The Bluetooth technology provides security measures at both the application layer and the link layer. Besides there are two kinds of inherent features that make attacks more difficult. A hop selection mechanism of up to 1600 hops/sec is employed to avoid the interference from external or other piconets. An automatic output power adaptation scheme is also included in the standard for the low power consumption of light-weight mobile devices, which can reduce the radio spread range for data transmission exactly according to requirements based on the detected intensity.

2.1. Basic Definitions

A total of three different information security objectives are to be reached one or all. Confidentiality means that the data can only be used by authorized users and/or parties. Integrity means that the data cannot be modified during transfer and stored by adversaries. Availability means that the data is always available for authorized use. Typical attacks to a wireless network include DoS (Denial-of-Service), man-in the- middle, spoofing, impersonating, session hijacking, eavesdropping, *etc*. Bluetooth launches three main techniques to achieve security features.

- **Confidentiality:** The first goal of Bluetooth is confidentiality or privacy. This service prevents an eavesdropper from reading critical information. In general, with this security service only the authorized user can access the data. The process of transforming data into a form that it cannot be understood without a key. Both data and control information can be encrypted.

- **Authentication:** Providing identity verification of the communicating devices is the second goal of Bluetooth. Authentication allows the communicating devices able to recognize each other; hence communication aborts if the user is not authorized. The process of verifying ‘who’ is at the other end of the link. Authentication is performed for both devices and users.

- **Authorization:** The third goal of Bluetooth is to control access to the resources. This is achieved by determining the users who are authorized to use the resources The process of deciding if a device is allowed to have access to a service. Authorization always includes authentication.

2.2. Modes of Security

Each Bluetooth device can operate on one of the 3 security modes. Mode 1 is a non secure mode in which a Bluetooth device shall never initiate any security procedure. Mode 2 is service-level enforced security where a device does not initiate security procedures before channel establishment at L2CAP level, and whether to initiate or not depends on the security requirements of the requested channel or service. Mode 3 is a link-level enforced security in which a Bluetooth device shall initiate security procedures before the link set-up at the LMP level is completed. Accordingly, two levels of Bluetooth security scheme can be identified, as follows:

- Link-level security, corresponding to security mode 3. The Bluetooth device initiates security procedures before the channel is established. This is the built in security mechanism and it is not aware of service/application layer security.

- Service-level security, corresponding to security mode 2. The Bluetooth device initiates security procedures after the channel is established, *i.e.*, at the higher layers. This is a kind of add-in mechanism and is regarded as a practical issue.

2.3. The Levels of Security

Bluetooth allows different security levels to be defined for devices and services. Two security levels can be defined for a device. A trusted device has unrestricted access to all or some specific services. Basically this means that the device has been previously authenticated and marked as “trusted”. An entrusted device has restricted access to services. Usually the device has been previously authenticated but has not been marked as “trusted”. An unknown device is also an entrusted device. Three levels of service security are allowed to be defined so that the requirements for authorization, authentication, and encryption can be set independently, including services that require authorization and authentication, services that require authentication only, and services open to all devices. These three security levels can be described by using the following three attributes.

- Authorization Required: access is only granted after an authorization procedure. Only trusted devices would get automatic access.

- Authentication Required: the remote device must be authenticated before being able to connect to the application.

- Encryption Required: the link between the two devices must be encrypted before the application can be accessed.

3. Security Modes of Bluetooth

3.1. Security Mode 1: Non Secure Mode

This is the most insecure security mode in which the Bluetooth device does not initiate any security procedure, allowing other Bluetooth devices to initiate connections with it.

3.2. Security Mode 2: Service-level Enforced Security Mode

This mode enforces security after establishment of the link between the devices at the L2CAP level. This mode allows the setting up of flexible security policies involving application layer controls running in parallel with the lower protocols.

3.3. Security Mode 3: Link-level Enforced Security Mode

This mode enforces security controls such as authentication and encryption at the Baseband level itself, before the connection is set up. The security manager usually enforces this onto the LMP. Bluetooth allows security levels to be defined for both devices and services. For devices there are two possible security levels. A remote device could either be trusted device-Such a device would have access to all services for which the trust relationship has been set or untrusted device-Such a device would have restricted access to services. Typically such devices would not share a permanent relationship with the other device.

4. Authentication

The Bluetooth authentication scheme uses a challenge response strategy as shown in Figure 1, where a protocol is used to check whether the other party knows the secret key. The protocol uses symmetric keys, so a successful authentication is based on the fact that both participants share the same key. The Authenticated Ciphering Offset (ACO) is computed and stored in both devices and is used for cipher key generation later on. The verifier sends the claimant a random number to be authenticated. Then, both participants use the authentication function E1 with the random number, the claimants Bluetooth Device Address and the current link key to get a response. The claimant sends the response to the verifier, who then makes sure the responses match. The used application indicates who is to be authenticated. So the verifier may not necessarily be the master. Some of the applications require only one-way authentication, so that only one party is authenticated. This is not always the case, as there could be a mutual authentication, where both parties are authenticated in turn. If the authentication fails, there is a period of time that must pass until a new attempt at authentication can be made. The period of time doubles for each subsequent failed attempt from the same address, until the maximum waiting time is reached. The waiting time decreases exponentially to a minimum when no failed authentication attempts are made.

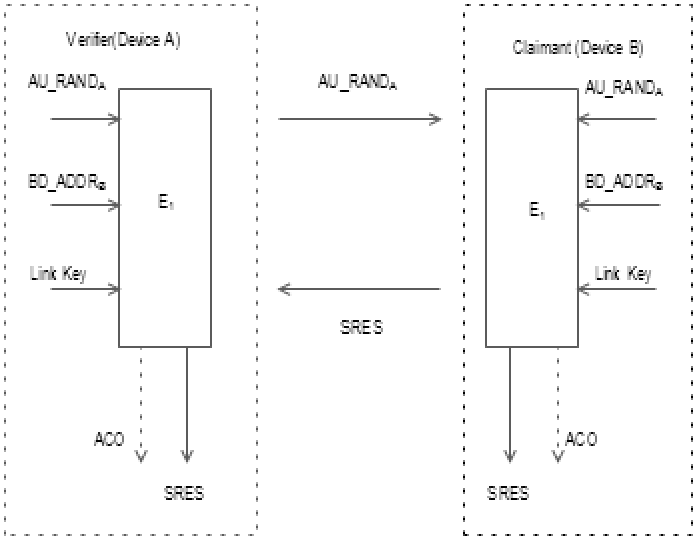

Figure 1. Challenge response for Bluetooth

5. Key Management

Prepare all security transactions between two or more parties are handled by the link key. The link key is a 128- bit random number. It is used in the authentication process and as a parameter when deriving the encryption key. The lifetime of a link key depends on whether it is a semi-permanent or a temporary key. A semi-permanent key can be used after the current session is over to authenticate Bluetooth units that share it. A temporary key lasts only until the current session is terminated and it cannot be reused. Temporary keys are commonly used in point-to- multipoint connections, where the same information is transmitted to several recipients. The length of the Personal Identification Number (PIN) code used in Bluetooth devices can vary between 1 and 16 octets. The regular 4-digit code is sufficient for some applications, but higher security applications may need longer codes. The PIN code of the device can be fixed, so that it needs to be entered only to the device wishing to connect. Another possibility is that the PIN code must be entered to the both devices during the initialization as shown in Figure 2.

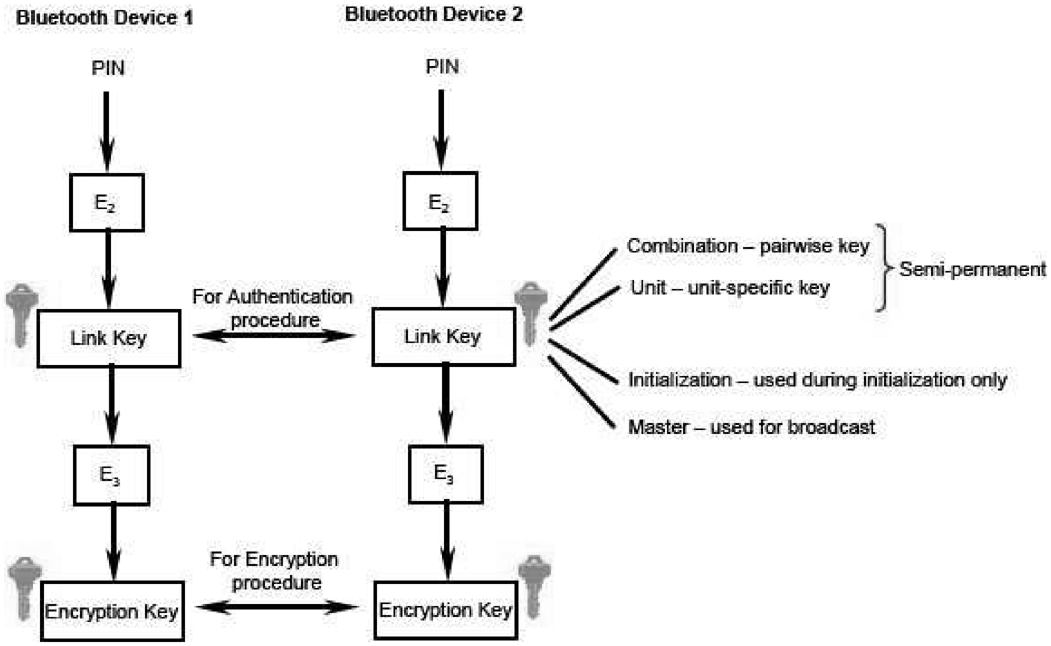

Figure 2. Bluetooth Key Generations from PIN

6. Conclusions

Bluetooth is a wireless technology which can do much more than just replace data cables between devices. Bluetooth version 4.0 supports higher data rates, greater range and safer security measures. In this paper, we discussed the security issues related to wireless Bluetooth. We designed a security architecture that protects from an attacker that has full control over the Bluetooth wireless link between the wireless Bluetooth and device. Bluetooth is a relatively new wireless technology and therefore new attacks against Bluetooth security are likely to be found. Therefore, in future, we will investigate Bluetooth security weaknesses and propose countermeasures against new attacks.

References

[1] Bluetooth Special Interest Group. Bluetooth wireless technology surpasses one billion devices. http://www.bluetooth.com/Bluetooth/Press/SIG/BLUETOOTH WIRELESS TECHNOLOGY SURPASSES ONE BILLION DEVICES.htm, **(2006)**.

[2] Bluetooth Special Interest Group. Specification of the Bluetooth system. http:// www.bluetooth.com/NR/rdonlyres/1F6469BA-6AE7-42B6-B5A1-65148B9DB238/840/Core v210 EDR.zip, **(2004)**.

[3] J. Dunning, “Taming the Blue Beast: A Survey of Bluetooth Based Threats”, IEEE Security & Privacy, vol. 8, no. 2, **(2010)** March-April, pp. 20-27.

[4] K. Scarfone and J. Padgette, “Guide to Bluetooth Security”, NIST Special Publication, **(2005)** September, pp. 800-121.

[5] L. Carettoni, C. Merloni and S. Zanero, “Studying Bluetooth Malware Propagation: The BlueBag Project”, IEEE Security & Privacy, vol. 5, no. 2, pp. 17-25.

[6] K. Haataja and K. Hypponen, “Man-In-The-Middle attacks on Bluetooth: A Comparative Analysis, A Novel Attack, and Countermeasures”, 3rd International Symposium on Communications, Control and Signal Processing, ISCCSP’08, **(2008)** March, pp. 1096-1102.

[7] K. Haataja and P. Toivanen, “Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing”, 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM’08, **(2008)** October, pp. 1-5.

[8] M. Ghallali, D. El Ouadghiri, M. Essaaidi and M. Boulmalfm, “Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods”, Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia (MoMM '11). ACM, New York, NY, USA, **(2011)**, pp. 256-259.

[9] J. McCune, A. Perrig and M. Reiter, “Seeing-is-believing: Using camera phones for human-verifiable authentication”, Proc. IEEE S&P, **(2005)**.

[10] N. Saxena, J.-E. Ekberg, K. Kostiainen and N. Asokan, “Secure device pairing based on a visual channel”, Proc. IEEE S&P, **(2006)**.

[11] M. Goodrich, M. Sirivianos, J. Solis, G. Tsudik and E. Urzun, “Human-verifiable authentication based on audio”, Proc. ICDCS, **(2006)**.

[12] S. Laur and K. Nyberg, “Efficient mutual data authentication using manually authenticated strings”, Proc. CANS, **(2006)**.

[13] B. Blanchet, “From secrecy to authenticity in security protocols”, In Proc. SAS, **(2002)**.

[14] B. Blanchet, “Automatic proof of strong secrecy for security protocols”, Proc.IEEE S&P, **(2004)**.

Authors

Bijoy Kumar Mandal, currently, associated with Computer Science and Engineering Department, Faculty of Engineering and Technology, NSHM Knowledge Campus – Durgapur, as an Assistant Professor. He is pursuing Ph.D. (Computer Science and Engineering) in NIT, Durgapur. He received M. Tech(CSE) from Jadavpur University, B.Tech from Govt. College of Engineering and Ceramic Technology and Diploma in Computer Science and Technology from Central Calcutta Polytechnic College. He has six years teaching experience. He published 14 Research papers in international Journals and Conferences.

Debnath Bhattacharyya, M.Tech (CSE), Ph.D. (Tech.), currently, associated with Computer Science and Engineering Department, Faculty of Engineering and Technology, NSHM Knowledge Campus – Durgapur, as a Professor and Head. Dr. Bhattacharyya has 17 years of experience in Teaching and Research. He published more than 135 research papers in international Journals and Conferences. He published 4 Text Books for B. Tech, and MCA, so far. He is also associated with West Bengal University of Technology, University of Calcutta and many leading National and International Universities as the Ph.D. Supervisor.

Tai-hoon Kim, M.S., Ph. D (Electricity, Electronics and Computer Engineering), currently, Professor of Sungshin Women's University, Korea. His research interests include Multimedia security, security for IT Products, systems, development processes, operational environments, etc. He has 18 Years of experience in Teaching & Research. He has already got distinctive Academic Records in international levels. He has published more than 300 Research papers in International & National Journals and Conferences.