BLUETOOTH SECURITY THREATS

Praveen Kumar Mishra
Department of Computer Science & Engineering
Ideal Institute Technology
Mahamaya Technical University, Noida, INDIA
amanpraveen@gmail.com

ABSTRACT

Bluetooth technology has become an integral part of this modern society. The availability of mobile phones, game controllers, Personal Digital Assistant (PDA) and personal computers has made Bluetooth a popular technology for short range wireless communication. However, as the Bluetooth technology becomes widespread, vulnerabilities in its security protocols are increasing which can be potentially dangerous to the privacy of a user's personal information.

The proliferation of the Bluetooth devices in the workplace exposes organizations to security risks. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attack, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. Preventing unauthorized users from secure communication is a challenge to the pairing process.

Keywords- Bluetooth Security, Privacy, PDA, man-in-the-middle attacks.

INTRODUCTION

Bluetooth 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 [1]. 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 [2]. Bluetooth is a combination of hardware and software technology. The hardware is riding on a radio chip. On the other hand, the main control and security protocols have been implemented in the software. By using both hardware and software Bluetooth has become a smart technology for efficient and flexible wireless communication system. Bluetooth radio chip supports communication among a group of electronic devices.

Some key benefits of Bluetooth technology are,

- Cable replacement. Bluetooth technology replaces a variety of cables, such as those traditionally used for peripheral devices (e.g., mouse and keyboard connections), printers, and wireless headsets and ear buds that interface with personal computers (PC) or mobile telephones.
- Ease of file sharing. A Bluetooth-enabled device can form a piconet to support file sharing capabilities with other Bluetooth devices, such as laptops.
- Wireless synchronization. Bluetooth provides automatic synchronization between Bluetooth-enabled devices. For example, Bluetooth allows synchronization of contact information contained in electronic address books and calendars.
- Internet connectivity. A Bluetooth device with Internet connectivity can share that access with other Bluetooth devices. For example, a laptop can use a Bluetooth connection to

  have a mobile phone establish a dial-up connection, so that the laptop can access the Internet through the phone.

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 [3]. 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 [4]. 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, Bluesnarf, etc [5, 6].

In this paper, we will provide some background information about Bluetooth system, its applications and various security issues involve in Bluetooth, mainly authentication, encryption, and key management. We will also describe vulnerabilities in Bluetooth technologies and threats against those vulnerabilities. Based on the common vulnerabilities and threats, recommendations for possible countermeasures that can be used to improve Bluetooth security are also made. This provides better understanding of the problem, current solution space, and future research scope to resolve various security issues involve in Bluetooth security.

Attacks on Bluetooth

As technology improves,these phone hackers, or "phreakers", only gain more of an advantage. Here is an abridged list of attacks that have been launched at Bluetooth :

SNARF Attack

This attack is typically only available when a phone is set in "discovery" or "visible" mode on the network. It was thought that setting the phone to "invisible" mode would cease these attacks, but recently, tools have appeared on the internet that can bypass even these settings. Attackers can now setup a SNARF attack on almost any phone. The only sure-fire way to avoid SNARF attacks is to disable Bluetooth on the phone when you do not absolutely need its functionality.

BACKDOOR Attack

The BACKDOOR attack is another security violation that works by establishing an illegal connection to the target's phone. This attack, however, works by actually establishing a trust relationship through Bluetooth's pairing mechanism, but removing the attacking device from the pair list after a connection is established. In this way, unless the owner of the device is watching the pair list at the exact moment a connection is made, it is unlikely they will notice that the enemy is still connected even though the pair has been removed from the list. The enemy will then have access to all material that a "trusted" link would entail, but without the owner permitting the use. This would again allow access permitted data on the phone as well as phone calls and instant messages. However, since this attack only grants access to information flagged for trusted connections, it is more limited than the SNARF attack.

BLUEBUG Attack

The BLUEBUG attack is an attack that creates a serial connection to the phone, allowing access to all the included AT commands. This allows the attacker to place phone calls, send and receive messages, connect to internet data services. It has also been discovered that if the phone is on a GSM network, it is possible to monitor conversations of nearby phones. This attack takes approximately 2 seconds to complete if implemented correctly, and it leaves almost no trace of its intrusion. An attacker can then route incoming calls to other devices.

BLUEJACKING

Unlike the previous attacks, BLUEJACKING does not allow and adversary access to any data. Instead, using a small loophole in the Bluetooth pairing process, it is possible to send a user a message. This is often harmless, as attackers merely used BLUEJACKING as a way to express themselves, present counter-culture propaganda, or simply prove they can accomplish the violation of a consumer's security.

WARNIBBLING

WARNIBBLING is an attack in which a phreaker attempts to find and access as many vulnerable Bluetooth phones as possible. They typically use laptops or PCs with high gain antennas and special software, such as Redfang, to sniff for accessible phones. Instead of remaining stationary, warnibblers will move around mapping as many phones a possible. Some drive, some move from café to café, but the results are the same – they often violate the security of large amounts of consumers.

Solutions of Bluetooth Security

The link layer security is usually used in wireless network. However, this kind of security can not satisfy the user's demand in upper layer. To meet with different requirements of data security in Bluetooth technology, Bluetooth technology provides three security modes to enforce the flexibility of its secure mechanism and the device manufacture determine which mode should be used.

The three modes are:

Mode1: non-secure

Mode2: Service-level security

Mode3: link-level security

Security Mode 1: Nonsecure mode

A device will not initiate any security procedures. In this nonsecure mode, the security functionality (authentication and encryption) is completely bypassed. In effect, the Bluetooth device in Mode 1 is in a promiscuous mode that allows other Bluetooth devices to connect to it. This mode is provided for applications for which security is not required, such as exchanging business cards.

Security Mode 2: Service-level enforced security mode

In the service-level security mode, security procedures are initiated after channel establishment at the Logical Link Control and Adaptation Protocol (L2CAP) level. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode, a security manager (as specified in the Bluetooth architecture) controls access to services and to devices. The centralized

security manager maintains polices for access control and interfaces with other protocols and device users. Varying security polices and trust levels to restrict access may be defined for applications with different security requirements operating in parallel. Therefore, it is possible to grant access to some services without providing access to other services. Obviously, in this mode, the notion of authorization – that is the process of deciding if device A is allowed to have access to service X – is introduced.

Security Mode 3: Link-level enforced security mode

In the link-level security mode, a Bluetooth device initiates security procedures before the channel is established. This is a built-in security mechanism, and it is not aware of any application layer security that may exist. This mode supports authentication (unidirectional or mutual) and encryption. These features are based on a secret link key that is shared by a pair of devices. To generate this key, a pairing procedure is used when the two devices communicate for the first time.

Bluetooth Key Generation from PIN

The link key is generated during an initialization phase, while two Bluetooth devices that are communicating are ”associated” or ”bonded.” Per the Bluetooth specification, two associated devices simultaneously derive link keys during the initialization phase when a user enters an identical PIN into both devices. The PIN entry, device association, and key derivation are depicted conceptually in Figure 1. After initialization is complete, devices automatically and transparently authenticate and perform encryption of the link. It is possible to create a link key using higher layer key exchange methods and then import the link key into the Bluetooth modules. The PIN code used in Bluetooth devices can vary between 1 and 16 bytes. The typical 4-digit PIN may be sufficient for some applications; however, longer codes may be necessary.

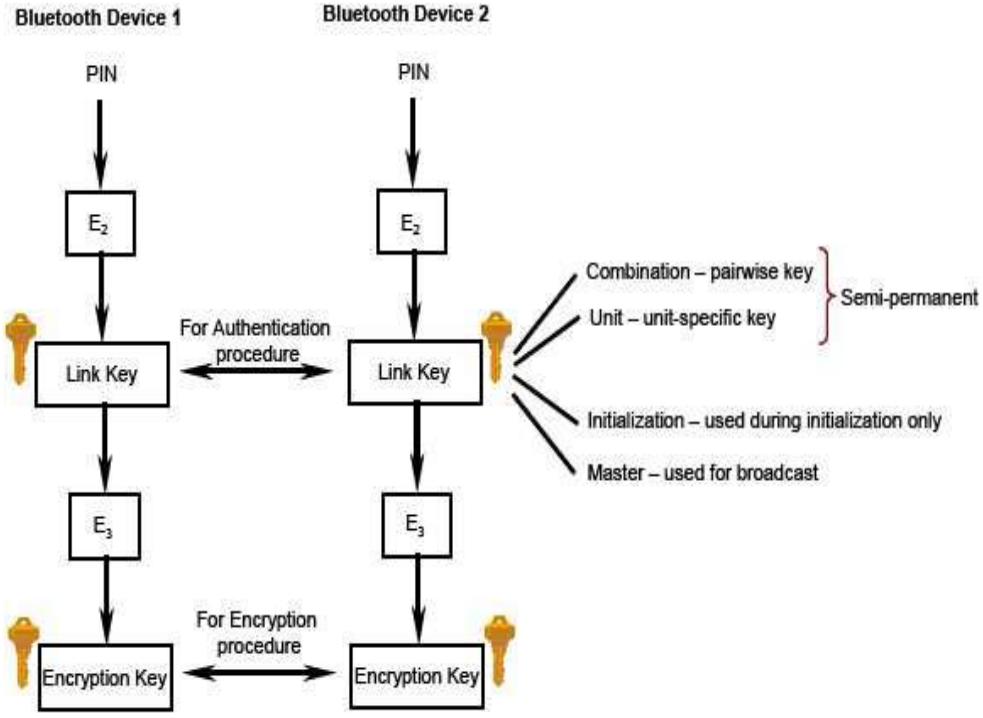

Figure 1: Bluetooth Key Generation from PIN

RISK MITIGATION AND COUNTERMEASURES

Organizations should applying countermeasures to address specific threats and vulnerabilities to Bluetooth network. First solution is to provide an adequate level of knowledge and understanding for those who will deal with Bluetooth-enabled devices. Organizations using Bluetooth technology should design and document security policies that address the use of Bluetooth-enabled devices and users' responsibilities. Organizations should also include awareness-based education to support staff to enhance their understanding and knowledge of Bluetooth.

Security Services:

Here, we will discuss three basic security services specified in the Bluetooth standard [2]:

- Confidentiality—Confidentiality ensures that only authorized devices can access and analysis data. It prevents information compromise caused by eavesdropping.
- Authentication—It deals with verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.
- Authorization—It allows the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

Security checklist with guidelines and recommendations:

Following section will provide a Bluetooth security checklist with guidelines and recommendations for creating and maintaining secure Bluetooth piconets:-

- Need to develop an organizational wireless security policy that addresses Bluetooth technology.
- Need to ensure that Bluetooth users on the network are made aware of their security-related responsibilities regarding Bluetooth use.
- Need to perform comprehensive security assessments at regular intervals to fully understand the organization's Bluetooth security posture.
- Need to ensure that wireless devices and networks involving Bluetooth technology are fully understood from an architecture perspective and documented accordingly.
- Users should be provided with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft.
- Change the default settings of the Bluetooth device to reflect the organization's security policy.
- Bluetooth devices should be set to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization.
- Choose PIN codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes.
- If Bluetooth device is lost or stolen, users should immediately unpair the missing device from all other Bluetooth devices with which it was previously paired.
- Need to install antivirus software on Bluetooth-enabled hosts that are frequently targeted by malware.
- Need to fully test and deploy Bluetooth software patches and upgrades regularly.
- Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images.

CONCLUSION

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. This paper discussed some background information about Bluetooth system, its applications and various security issues involve in Bluetooth. Vulnerabilities in Bluetooth technologies and threats against those vulnerabilities are also discussed. Few possible countermeasures are recommended that can be used to improve Bluetooth security are also made. 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 counter-measures against new attacks.

REFERENCES

[1] J. Dunning. Taming the Blue Beast: A Survey of Bluetooth Based Threats. IEEE Security & Privacy, 8(2):20–27,Mar-Apr. 2010.
[2] K. Scarfone and J. Padgette. Guide to Bluetooth Security. NIST Special Publication 800-121, Sep 2005.
[3] L. Carettoni, C. Merloni, and S. Zanero. Studying Bluetooth Malware Propagation: The BlueBag Project. IEEE Security & Privacy, 5(2):17–25,
[4] K. Haataja and K. Hypponen. Man-In-The-Middle attacks on Bluetooth: A Comparative Analysis, A Novel Attack, and Countermeasures. In 3rd International Symposium on Communications, Control and Signal Processing, ISCCSP'08, pages 1096–1102, March 2008.

[5] K. Haataja and P. Toivanen. Practical Man-in-the-Middle Attacks Against Bluetooth Secure Simple Pairing. In 4th International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM'08, pages 1–5, Oct. 2008.
[6] Mohamed Ghallali, Driss El Ouadghiri, Mohammad Essaaidi, and Mohamed Boulmalfm, ―Mobile phones security: the spread of malware via MMS and Bluetooth, prevention methods,‖ In Proceedings of the 9th International Conference on Advances in Mobile Computing and Multimedia (MoMM '11). ACM, New York, NY, USA, pp. 256-259, 2011.
[7] Bluetooth SIG. Bluetooth Technology in Hands of One Billion. Press release, http://www.bluetooth.com/ Bluetooth/SIG/Billion.htm, November 14, 2006.
[8] Adam Laurie, ―The Blue Bug‖, A.L. Digital Ltd. http://trifinite.org/trifinite_stuff_bluebug.html.
[9] John Oates, ―Virus attacks mobiles via Bluetooth‖, http://www.theregister.co.uk/2004/06/15/symbian_virus/
[10] F-Secure Article on Lasco.A Worm. http://www.fsecure.com/v-descs/lasco_a.shtml.
[11] Ford-Long Wong, Frank Stajano, Jolyon Clulow, ―Rep airing the Bluetooth pairing protocol‖. University of Cambridge Computer Laboratory. http://www.cl.cam.ac.uk/research/dtg/~fw242/publications/2005-WongStaClu-bluetooth.pdf
[12] Phone pirates in seek and steal mission", Cambridge Evening News. http://www.cambridgenews.co.uk/news/region_wide/ 2005/08/17/06967453-8002-45f8-b520-66b9bed6f29f.lpf
[13] "Going Around with Bluetooth in Full Safety‖, FSecure. http://www.securenetwork.it/ricerca/whitepaper/download/bluebag_brochure.pdf
[14] B. B. Gupta, R. C. Joshi, M. Misra, ―Defending against Distributed Denial of Service Attacks: Issues and Challenges,‖ Information Security Journal: A Global Perspective, vol. 18, issue 5, Taylor & Francis, UK, pp. 224-247, 2009.