BLUETOOTH SECU RITY ANALYSIS

[1] Priyanka B Murdeshwar, [2] Shruthi Tharanath Salian, [3] Surekha Reddy, [4]Sharath D S, [5]Dr. Manjunath Kotari.

Alvas Institute of Engineering and Technology

Abstract

Bluetooth is one of the advanced technology which replaced the complex technology of transferring information through wires and cables. Bluetooth is currently deployed in mobile phones, gaming consoles, laptops and wireless devices. Over a couple or more years many countries are using Bluetooth in field of defence. United States of America Department of Defence have begun to disclose the security failures of Bluetooth. There were no security features provided for Bluetooth before. Here we discuss how Bluetooth security works, and then move onto the security risks and requirements associated with designing and implementing Bluetooth based solutions for use in the Department of Defence. Further, open security problems that impact the future of Bluetooth use in the Department of Defence such as service-level security modes etc.

Keywords: *Bluetooth, piconet, Ethernet, Deffie Hellman, Encryption.*

I. INTRODUCTION

Advancing Information and Communication Technologies (ICT) have led to the creation of various communication channels to connect users anytime and anywhere. With many different electronic devices that have proliferated in recent times, consumers' expectations on instantaneous and continuous connectivity of multiple gadgets are high. Indeed, Bluetooth technology provides the very essence of such connectivity as its features and capabilities enable users to instantaneously establish connections with a wide range of Bluetooth-enabled devices without the need for a fixed infrastructure of physical cables.

Bluetooth is a wireless personal area network (WPAN) technology that was designed to replace cables used in various short-range data and voice applications. It is considered one of the most widely deployed wireless technologies with 2 billion devices shipped and counting (approximately 13 million Bluetooth devices are shipped per week)1. Bluetooth radios are integrated in many popular mobile devices including cell phones and laptops as well as smart card readers, mono/stereo headsets, gaming consoles and wireless keyboards/mice.

Bluetooth technology is the best option for short range communication rather than Infra-red communication which is done only with line of sight and also has lower data rates. The Bluetooth covers around 10 to 300 meters with 1Mbps data rate. A group of 8 Bluetooth networks connect to form a piconet. Two or more piconet joins to form a scatternet. One among the 8 devices of a piconet behaves as a master. All the others in the group are called slaves. If a slave works under two masters, then it should synchronize between both the masters. Bluetooth uses fast frequency hopping to decrease interference and increase security where it makes use of 79 frequencies in 1MHZ intervals[1]. It has short data packets and gives fast acknowledgements.

A study analyzing the BT presence in mobile devices, focusing on their security problems. We address this important aspect by analyzing common mobile attacks using BT and how to prevent them. The special attention is paid to the most critical security problems affecting BT, which are BlueSnarf, BlueSnarf++ and BlueBug. BT is a common entry point for many attack methods in mobile phones, and the information presented in this paper can be useful to educate and raise the awareness of mobile users in order to follow best practices.

II. LITERATURE REVIEW

Bluetooth Features- Bluetooth was initially developed for portable devices with limited battery power that needed to establish wireless connections within short ranges. It is a short-range wireless communication system that allows devices to communicate within close physical proximity of each other. It uses radio frequency technology that requires minimal power and embeds relatively small footprint or digital trace in other devices. As specified by the IEEE 802.15, it is a point-to-point or point-to-multipoint wireless technology that can handle both data and voice simultaneously within a transmission range of 10 meters (m) and a power usage of 2.5 milliwatt (mW). It can establish a network connection of a maximum of eight Bluetooth-compatible devices in an active state creating an instant Personal Area Network (PAN) in which one acts as the master device and the seven others as slaves. The Bluetooth network is called a piconet, which is automatically initiated by the devices where the master device solely controls the access of the slave all operating on the same channel and frequency]. Now at version 4, it provides both synchronous and asynchronous links with a data rate ranging from 1 up to 24 Megabits per second (Mbps), depending on the speed configuration . As the demand for the technology increases, various manufacturers have now incorporated Bluetooth into the development of their products and services, making it to be a globally accepted technology.

Bluetooth Applications- Bluetooth has supported a diverse range of services, and amongst the most common Bluetooth applications are as follows:

1) Device Connection: The main objective is to connect Bluetooth-compatible devices with ease, without the difficulty of cable installation .Once connected, it encourages the usage of hands-free devices such as a car kit or a wearable accessory like a headset.

2) Network Connection: It allows a device, such as a mobile phone, to function as a wireless modem providing the laptop user with a mobile Internet.

3) Synchronization: Once the connections have been established, synchronizing of data such as personal phone contacts, calendar, email entries, and notes between Bluetooth-compatible equipments can take place.

4) File Transfer: This is the wireless transmission of data, multimedia or program files (e.g., ringtones, documents, photos, and videos) between Bluetooth-compatible devices. Invoking file transfer comes into two ways - uploading files where the device user becomes the sender and downloading files where the device user becomes the recipient.

Bluetooth Security Threats- Most of the users do not consider Bluetooth technology's security threats and even do not consider the consequences of such attacks as major concerns. Noting that the severity of the consequences can only be measured once the attacks start causing enormous data loss, financial loss and even compromising the victim's identity or safety , it is thus a concern such security threats are taken lightly. At least seven Bluetooth security threats have been identified, and it is essential that one should be aware of them.

1) Virus Infection: It is similar to computer virus.The threat aims to create chaos amongst the users by paralyzing and wrecking the entire network system.

2) BlueBugging: The attacker creates an unauthenticated serial connection to the phone commands of a targeted mobile device without the acknowledgement of the user.

3) Information Theft: Once an unauthorized access is obtained into a particular device, residing confidential data can be at risk of information theft. A common form of information theft is BlueSnarfing that attacks specific groups of mobile devices and enables the attacker to steal sensitive data without the victim's knowledge.

4) Service Theft: Mobile network services like sending of text messages, downloading of multimedia content, and initiating phone calls are being hacked by the attacker without the victim's consent. 5) 5)Denial of Service (DoS): A nonparticipating device launches a DoS attack that affects the piconet by throwing some devices out of the network or disrupting the master device from supporting the connection .

6) BlueJacking: The threat begins with the sending of short, unsolicited, and deceitful messages to mobile devices. The short messages, in the form of anonymous business cards, can grant an attacker authorized access without the victim's knowledge and can proceed to over-write information like calendar appointments, phonebook entries, and mobile residing files.

7) BluePrinting: It is a process of discovering the fingerprint of Bluetooth-supported devices that comprises details uniquely identifying a particular device (i.e., make, model, and unique address of the equipment), just like the human fingerprint.

III. SECURITY IN BLUETOOTH

The essential security services provided by Bluetooth include authentication, encryption, and authorization. Authentication is performed so that a device can verify the identity of a remote device based on a mutually established symmetric key, called a link key. Identity is provided by a 48-bit Bluetooth device address (BD_ADDR) which is similar to an Ethernet MAC address. Pairing occurs when two devices generate and agree on the aforementioned link key used for authentication and encryption key generation. Whether or not pairing or any security mechanism is required for a particular connection depends on the security mode of the participating devices

The worldwide spread of mobile phones with BT and the decision to use it in situations not foreseen when the BT protocol was developed, attracted the attention for security problems. To address these security problems, in 2007 BT version 2.1 (the fifth release) had more security features than all the other versions, affecting a huge number of security related aspects. Below are the most relevant:

- **Encryption Pause and Resume**: This feature pauses the encryption when the link key connection needs to be changed and when the master and slave roles of the devices need to be switched. After these changes, the encryption resumes.
- **Secure Simple Pairing (SSP)**: Created to simplify the pairing process and improve the BT security. The two main security aspects are to protect against passive eavesdropping and man-in-the-middle attacks. It uses the Elliptic Curve Diffie Hellman (ECDH) public key cryptography as a means to prevent passive eavesdropping attacks.
- **Security Mode 4:** Used for SSP.

IV. BLUETOOTH SECURITY THREATS

As with all wireless communication, a risk analysis of Bluetooth must include a discussion of attacks which can be performed over-the-air. Passive eavesdropping is a key concern with wireless technologies due to its open medium. 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.

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).

Table 1: Bluetooth Attacks

Attack Classification	Threats
Surveillance	Blueprinting, bt_audit, redfang, War-nibbling, Bluefish, sdptool, Bluescanner, BTScanner

Range Extension	BlueSniping, bluetooone, VeraNG
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

V. PROBLEM STATEMENT

The major challenges faced in Bluetooth networks are PIN usages, the man in the middle attack and to detect any changes in the alteration of messages. Once when as soon as two Bluetooth nodes comes in the range of contact, they get connected by pairing. It uses only a fixed PIN (Personal Identification Number) value and the number of digits used in PIN is also very less. Hence it is easier to crack them and also random numbers used are also not good as it makes the attackers easy track the information.

VI. PROPOSED SOLUTION

In order to overcome the challenges faced in Bluetooth networks, 'Security framework' is proposed. Here authentication via trusted third party and digital signature are done. Bluetooth Firewalls are also used to reduce the threats or risks from the attackers and to reduce the risks the user of the Bluetooth should follows the practices like:

- Turn BT off when not in use.
- Change the default security settings to a more restrict mode whenever possible.
- Remove trusted devices that will not be used.
- Change the default name of the Bluetooth device to something unidentified and without meaning.
- Use a PIN code whenever pairing with another Bluetooth device.
- Select PIN codes that are comfortable and long. Avoid static and weak PINs, such as PINs consist of all 0's or 1's.

VII. OBJECTIVES

Bluetooth, a short ranged communication system which is intended to allow devices within physical proximity of each other to communicate. Bluetooth is used in almost every device. Bluetooth has severe security issues and the user doesn't seem to care much. But when the attack cause a severe loss to the user it becomes threat .The objective of this paper is the security issues of Bluetooth and the solution to these problems to prevent harmful security breaches that may affect data and financial loss as a consequence of identity theft.

VIII. METHODOLOGY

Symmetric Encryption- The symmetric method will look little similar to the PIN methods.

Asymmetric Encryption- This uses two different keys i.e. public key and private for encryption

IX. BLUETOOTH SECURITY RELATED WORK

1. Bluetooth Security and Vulnerabilities: Bluetooth technology is a wireless substitute to data cables by exchanging data using radio -transmissions. Bluetooth technology was created as an open standard to authorize connectivity and collaboration between disparate products and industries. Like any wireless technology, Bluetooth also has a number of security vulnerabilities. These vulnerabilities may comprise the device or the networks that the device connects to. However if the common Bluetooth security features are used properly, it should provide adequate security.

2. Mechanism of Bluetooth Security: When devices connect to each other, Bluetooth creates a link which uses optional pre-shared key authentication and algorithms which is considered to be strong when used correctly. The strength of the Bluetooth security mainly relies on the randomness and the length of the passkey used at the time of their first connection. Discoverability and connectability settings also play an important role in determining the security strength. These settings control whether the device can searched by other Bluetooth devices and how it can be connected. Also optional user authorization for connection requests provides extra security.

3. Bluetooth Vulnerabilities: Through design, Bluetooth uses peer-to-peer technology. Bluetooth has a very complex specification and provides support for a lot of services. Some of these services include input output devices like keyboard and mouse, headphones, speakers, networking, file transfer and printing. In order for these service to work and communicate with devices, designers and programmers implements Bluetooth for a wide variety for operating systems, chipsets and devices. Settings like discoverability, connection preferences and security of the interface are not always the same and depend on the programmer. Due to this, Bluetooth is open to a lot of security vulnerabilities.

X. CONCLUSION

It is alarming to note that these users are not taking precautions to mitigate the possible harm that “re-engineered” Bluetooth can expose them to various security vulnerabilities and risks. In this paper we analyzed BT security and the most common attack procedures: BlueSnarf, BlueSnarf++, and BlueBug.

Users of BT enabled devices should follow best practices, like turn off BT when not in use, restrict BT settings, remove trusted devices when no longer needed. However, BT devices should provide by default a safety barrier protecting their users, instead of relying on them to follow the best practices. The use of digital signature and authentication via the trusted third party is seen to enhance the security in Bluetooth Networks.

With the plethora of commercial products available today, it is apparent that Bluetooth use in the DoD has the potential to reach - and perhaps exceed - the usage levels of other wireless technologies such as IEEE 802.11 and cellular. Fortunately, effort has been invested by experienced Bluetooth personnel over the past couple of years to

provide a set of requirements that will ensure the technology can be used with DoD information systems in a low risk, secure fashion.

XI. REFERENCES

1. BLUETOOTH SECURITY IN THE DOD John D. Padgette Booz Allen Hamilton Herndon, VA.

2. ENHANCING SECURITY IN BLUETOOTH NETWORKS Sharon Priyank.S SENSE, VIT University Chennai, India sharon.priyanka2013@vit.ac.in B.Nagajayanthi Asst. Professor (SR), SENSE VIT University, Chennai, India nagajayanthi.b@vit.ac.in

3. AN ANALYSIS OF BLUETOOTH SECURITY VULNERABILITIES Creighton T. Hager and Scott F. Midkiff Bradley Department of Electrical and +Computer Engineering Virginia Polytechnic Institute and State University Blacksburg, Virginia 24061 USA {chager, midkiff}@vt.edu

4. BLUETOOTH SECURITY ANALYSIS FOR MOBILE PHONES João Alfaiate, José Fonseca UDI – Research Unit for Inland Development of Guarda Polytechnic Institute, Portugal jc.alfaiate@gmail.com, josefonseca@ipg.pt

5. A SIMPLE WAY TO IMPROVE THE SECURITY OF BLUETOOTH DEVICES Peter Dell Curtin University of Technology P.T.Dell@curtin.edu.au Khwaja Shan-ul-Hasan Ghori Curtin University of Technology K.Ghori@curtin.edu.au

6. AN INVESTIGATION OF BLUETOOTH SECURITY THREATS Tan Nanyang Technological University Singapore mtan@ntu.edu.sg. Kathrine Aguilar Masagca Nanyang Technological University Singapore.