International Journal of Advanced Research in

Computer Networking,Wireless and Mobile Communications

Volume: 2 Issue: 1 09-Apr-2015,ISSN_NO: 2320-7248

Securing A Bluetooth Device

Mrs. Dhanashri D. Dhokate[1] , Mr. Milind C. Butale[2] , Mr. Babasaheb S. Patil[3]
Assistant Professor, Information Technology, PVPIT, Budhgaon , India [1].
Associate Professor, Electronics Department, PVPIT, Budhgaon , India [2]
Associate Professor, Electronics Department, PVPIT, Budhgaon , India [3]

ABSTRACT: *The purpose of this study is to introduce the various security levels for connecting two Bluetooth devices. Bluetooth devices form Scatter net network for personal area networking. These Scatternet concepts and security issues related to Scatternet are explained here. This article is based on study of different aspects of Bluetooth security. Various weaknesses involved in Bluetooth transfer between devices and steps to overcome these weaknesses are also included. The purpose of this document is to let the reader's know the basic technology used for data transfer through Bluetooth. The aim of our study is to evaluate security threats in Bluetooth-enabled systems.*

Keywords - Bluetooth, Bluetooth security, Radio Frequency, Scatternet, security analysis.

1. INTRODUCTION:

Bluetooth operates at 2.4 GHz frequency in the free ISM-band (Industrial, Scientific, and Medical) by using frequency hopping. Bluetooth frequency hopping uses a maximum of 79 different Baseband frequencies to avoid channels that suffer from interference. It also enables a large number of Bluetooth devices to operate in the same 2.4 GHz ISM-band. The use of wireless communication systems and their interconnections via networks have grown rapidly in recent years. Because RF (Radio Frequency) waves can penetrate obstacles, wireless devices can communicate with no direct line-of-sight between them. This makes RF communication easier to use than wired or infrared communication, but it also makes eavesdropping easier.

Bluetooth and WLAN are wireless RF communication systems, our work focuses on the security of Bluetooth technology. Bluetooth is a wireless networking technology specifically developed for personal area networking and other short range applications. Bluetooth is a technology for short range wireless data and real time two-way voice transfer providing data rates up to 3 Mb/s. It can be used to connect almost any device to another device. Bluetooth-enabled devices, such as mobile phones, headsets, PCs, laptops, printers and keyboards are widely used all over the world. The Bluetooth special interest group (SIG) works for Bluetooth related developments and other aspects. Security issues in wireless ad-hoc networks are much more complex than those of more traditional wired or centralized wireless networks. Moreover, Bluetooth networks are formed by radio links, which means that there are additional security aspects whose impact is not yet well understood.

Since Bluetooth is a wireless communication system, there is always a possibility that the transmission could be deliberately jammed or intercepted, or that false or modified information could be passed to the picante devices. To provide protection for the picante, the system can establish security at several protocol levels. Bluetooth has built-in security measures at the link level. The basic Bluetooth security configuration is done by the user, who decides how a Bluetooth device will implement its connect ability and discoverability options.

2. THE BLUETOOTH SECURITY:

The different combinations of connect ability and discoverability capabilities can be divided into three categories, or security levels: **1. Silent:** The device will never accept any connections. It simply monitors Bluetooth traffic. **2. Private**: The device cannot be discovered, i.e. it is a so-called non-discoverable device. Connections will be accepted only if the BD_ADDR (Bluetooth Device Address) of the device is known to the prospective master. A 48-bit BD_ADDR is normally unique and refers globally to only one individual Bluetooth device. **3. Public**: The device can be both discovered and connected to. It is therefore called a discoverable device.

In Bluetooth technology, a device can be in only one of the following security modes at a time: **1. No secure**: The Bluetooth device does not initiate any security measures. **2. Service- level enforced security mode:** Two Bluetooth devices can establish a No secure ACL link. Security procedures, namely authentication, authorization and optional encryption, are initiated when an L2CAP CO or an L2CAP CL channel request is made. **3. Link-level enforced security mode:** Security procedures are initiated when an ACL link is established. 4. Service-level enforced security mode: This mode is similar to mode 2, except that only Bluetooth devices using SSP can use it.

3. SECURITY ANALYSIS TOOLS:

3.1 On-line pin cracking script -

On-line PIN Cracking attack is successfully performed by using: CATC Protocol Analyzer System 2500H: It is flexible and efficient integrated environment provider that provides 512 MB of recording memory, Hi-Speed USB 2.0 Interface to host PC/laptop, upgradeable firmware/ Bus Engine/Baseband, and support for plug-in modules.

Bluetooth Analyzer and Test Generator Plug-In Module: LeCroy Bluetooth 1.1 compatible radio unit is used as a plug-in module for the CATC Protocol Analyzer System 2500H. Nokia's Wireless Headset HDW-2: The Bluetooth 1.1 compatible Nokia HDW-2 acts as a victim device. It has a fixed 4-digit PIN code.

LeCroy BTTracer/Trainer v2.2 software: A LeCroy BTTracer/Trainer v2.2 software is to be installed to the laptop, which is connected to the CATC Protocol Analyzer System 2500H via a USB cable. On-Line PIN cracking script: CATC Scripting Language is used to create On-Line PIN Cracking script, which makes the On-Line PIN Cracking attack possible.

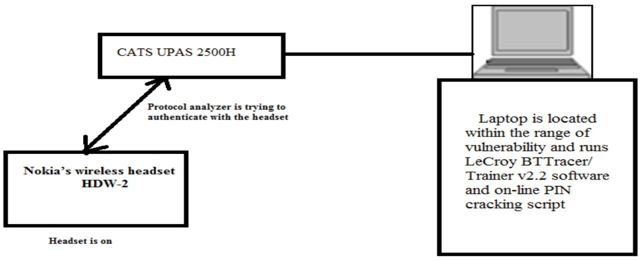
CATS UPAS 2500H
Protocol analyzer is trying to authenticate with the headset
Nokia's wireless headset HDW-2
Headset is on
Laptop is located within the range of vulnerability and runs LeCroy BTTracer/ Trainer v2.2 software and on-line PIN cracking script

Fig.1: An example of the On-Line PIN Cracking

3.2, Brute-Force BD ADDR Scanning script -

The Brute-Force BD ADDR Scanning is successfully performed by using: The CATC Protocol Analyzer System 2500H.

A Bluetooth Analyzer and Test Generator Plug-In Module: A LeCroy Bluetooth 1.1 compatible radio unit is used as a plug-in module for the CATC Protocol Analyzer System 2500H.

A Nokia 6310i [6] mobile phone: An unmodified Bluetooth 1.1 compatible Nokia 6310i mobile phone is the victim device. The LeCroy BTTracer/Trainer v2.2 software. A Brute-Force BD ADDR Scanning script: The CATC Scripting Language is used to create Brute-Force BD ADDR Scanning script, which makes the Brute-Force BD ADDR Scanning attack possible.

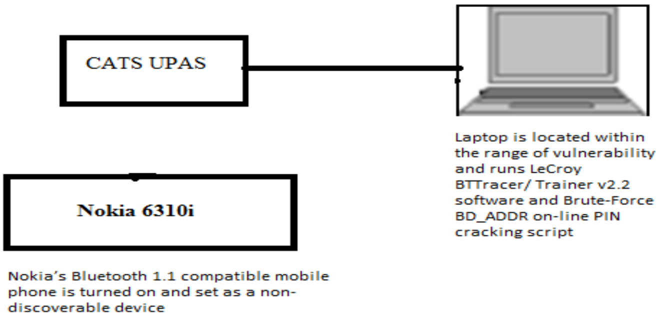
CATS UPAS
Laptop is located within the range of vulnerability and runs LeCroy BTTracer/ Trainer v2.2 software and Brute-Force BD_ADDR on-line PIN cracking script
Nokia 6310i
Nokia's Bluetooth 1.1 compatible mobile phone is turned on and set as a non-discoverable device

Fig 2: An example of the Brute-Force BD ADDR Scanning.

3.3, BTKeylogging attack:

The BTKeylogging attack is performed by using: The CATC Protocol Analyzer System 2500H. A Bluetooth Analyzer and Test Generator Plug-In Module: LeCroy Bluetooth 1.1 compatible radio unit is a plug-in module for the CATC Protocol Analyzer System 2500H.

A Microsoft Bluetooth keyboard and a Microsoft Bluetooth USB Transceiver: Microsoft's Bluetooth 2.0 compatible keyboard and Microsoft's Bluetooth 2.0 compatible USB dongle are used in the victim device (PC). The LeCroy BTTracer/Trainer v2.2 software. An On-Line PIN cracking script: An On-Line PIN cracking script to discover the PIN code of the keyboard.

A protocol analyzer intercepts all required information (IN RAND, LK RAND, AU RAND, SRES and EN RAND) for the attack. After that keyboard is used as a key logger for intercepting all key presses, and finally all intercepted information is successfully decrypted.

4. THE SCATTERNET:

Scatternet formation is the foundation for large scale Bluetooth ad-hoc networks and it is therefore a very important concept. Scatternet are formed by interconnecting piconets through gateways, or bridge nodes. Inter-piconet bridges are necessary since each piconet restrict the membership to a single master and up to seven slaves. Piconets are interconnected using common slaves, or bridge nodes. These devices participate in two piconets and schedule their participation in each piconet during disjoint time-slots. The Bluetooth slotted Time-Division Duplex (TDD) allocation scheme works in such a way that each slave is addressed in a round-robin fashion, and slaves are only permitted to transmit during the directly following slot(s) after being addressed by a master. Therefore, it is possible for bridge nodes to switch piconets and listen for transmissions from the other master during idle periods.

Bluetooth is a wireless networking technology specifically developed for Personal Area Networking and other short range applications. Bluetooth devices can be networked together by forming piconets of up to eight devices, where a single device is the master and the rest are slaves. These piconets can further be interconnected to create a Scatternet. A Scatternet is formed by allowing bridge nodes to operate in multiple piconets by interleaving their membership.

5. BLUETOOTH PRELIMINARIES

At the physical layer, Bluetooth operates in the globally available 2.4 GHz ISM (Industry, Scientific, and Medical) frequency band. The main advantage of the ISM frequency band is that it makes Bluetooth universally accepted worldwide. Bluetooth utilizes a frequency-hopping spread spectrum (FHSS) scheme. The Bluetooth Special Interest Group was originally founded in 1998 and promoted by industry leaders such as Ericsson, Intel, IBM, Toshiba and Nokia, among others.

Devices stay synchronized to a piconet by following the pseudo random frequency-hopping sequence (FHS) across 79 channels. Therefore, multiple piconets can coexist with each other and other types of devices without too much interference. Any Bluetooth device can either act as a master or as a slave since roles are not pre assigned. They can be interconnected into a piconet, which is the basic Bluetooth networking unit. A piconet can contain up to 8 active devices, where one device operates as the master and the others as slaves. The Master/Slave configuration places a restriction on the ad-hoc networking topology, since devices are clustered into relatively small piconets. The master can be viewed as a cluster head of the piconet, much like ad-hoc clusters in. All communication within the piconet goes through the master, and therefore there are no direct links between slaves. The master controls all intra-piconet communication and addresses each slave individually in a round-robin fashion. Each slave is only permitted to respond in the directly following slot(s) after being addressed by the master. This eliminates contention and collisions within the piconet, and allows a slave to enter sleep mode when it is not being addressed.

The master determines the frequency-hopping sequence for the piconet, which all slaves must follow in order to communicate. A Bluetooth device is classified as either a master or a slave. Each device has a unique 48-bit BD ADDR. It is similar to an IEEE 802 MAC address, but is divided into three parts; a 24-bit Lower Address Part (LAP), an 8-bit Upper Address Part (UAP), and a 16-bit Non-significant Address Part (NAP). The UAP and NAP together identifies the company that manufactured the device, and the LAP is a company assigned value. All Bluetooth devices have a permanent BD ADDR. Within a piconet, each slave is also assigned a 3-bit AM ADDR by the master. Thus, a slave can determine from the packet header whether the packet is addressed to it and if it should continue to listen to the transmission.

Bluetooth packets can be either one of two types: Asynchronous connectionless (ACO) or synchronous Connection-oriented (SCO). Once a device is connected and a Master/Slave link is formed, ACL packets can be exchanged without any other setup procedures. ACL links are primarily used for time-insensitive data and can be retransmitted as needed. An SCO link is a synchronous link that is used for time-sensitive packets. Prior to data transmission, the peers must establish an SCO link and reserve slots. for transmission of SCO packets. This type of link is used for voice and multimedia packets that have strict time bounds and are never retransmitted.

6. SCATTERNET BLUETOOTH SECURITY:

Most Bluetooth devices have limited processing power and battery capacity. Therefore, a general purpose security mechanism must adhere to strict resource constraints. For instance, private key cryptography uses the same key for both encryption and decryption secret keys. The Bluetooth specification defines the SAFER+ block cipher algorithm for encryption and link key generation. Bluetooth authentication keys are 128-bits in length. Keys are generated for encryption and authentication procedures using several different algorithms. A key can either be temporary, valid only during a session, or semi-permanent. A semi-permanent key is seldom changed and stored in non-volatile memory.

7. SECURITY MODELS:

The following two scenarios to be suitable for a Scatternet and benefit from efficient security solutions: Conference room scenario: A large group of participants (more than 8 connected devices) need to form a secure Scatternet based on a predetermined shared secret. Personal Area Network scenario: An individual requires that his/her personal devices form secure connections, while still maintaining connectivity to a non-secure public Scatternet.

First scenario the entire Scatternet share a common secret is assumed. For example, at a Bluetooth enabled medical center a group of surgeons meet in a conference room. Each surgeon keeps all his/her patient's journals in a Bluetooth enabled PDA. If a participant wants to share confidential medical information they have to ensure that no adversary outside the room is eavesdropping and can intercept it. It would not be practical for each contributing surgeon to walk around and securely transfer the journal to each of his/her colleagues. Therefore, the obvious solution is to form a Scatternet that connects all PDAs in the room. In this type of environment they could simply write a password on the white board and use it as the PIN. Regardless of how the PIN is communicated, the underlying assumption is that the shared secret exists. The second scenario is somewhat different, but also important for Bluetooth Scatternet. As Bluetooth devices become more and more prevalent, we foresee that an individual will carry several Bluetooth enabled devices. Thus, each individual assumes that his/her devices can communicate securely amongst each other while maintaining connectivity to the rest of the (insecure) Scatternet.

For example, suppose that our networked person wanted to add funds to his/her digital wallet. The notebook computer, which is equipped with a custom authentication hardware module and has sufficient processing power, connects to an Internet bank through a nearby Bluetooth access point. The transaction is insecure at the Bluetooth link layer to the access point, but is protected by application level strong authentication and encryption. After successfully completing the transaction, the user transfers the funds to his/her digital wallet over a secure link layer Bluetooth connection. The basic idea is that the individual's devices are connected in a secure piconet, which we call a Private PAN. These Private PANs are then connected to the Scatternet through a regular bridge node. We define a Private PAN as a secure piconet connected to an insecure Scatternet.

8. WEAK POINTS IN BLUETOOTH SECURITY:

8.1 Encryption mechanisms:

When two Bluetooth devices negotiate the parameters for encryption, the length of the encryption key is restricted by the Bluetooth device that has the shorter maximum encryption key length. For example, if one Bluetooth device can support only a 32-bit encryption key, the other Bluetooth device has to adjust to the situation and also use a 32-bit encryption key otherwise encryption cannot be used at all.

8.2 Device configuration :

The default settings of Bluetooth devices usually provide no security at all: the device is set as discoverable (i.e. public security level) and non-secure (i.e. non secure security mode). Therefore, an attacker can discover the BD_ADDR of the target device in a few seconds and perform various attacks against it. It is worth noting that Bluetooth is rarely switched on by default, so a user has to switch it on from the device's settings before any Bluetooth attacks against that device are possible. Moreover, many users want to save the batteries of their Bluetooth devices so Bluetooth is often switched off when there is no need to use it for a long time. It is very important that users know how to configure their Bluetooth devices correctly to achieve the best available level of security.

8.3 PIN code selection :

The PIN code can be as long as 128 bits (16 bytes), so it can contain up to sixteen 8-bit characters. However, long PIN codes are quite hard to remember, so users usually use only four digits. This makes an eavesdropper's work much easier, because she needs to go through only 10000 possible PIN values and witness the initial pairing process between the target devices in order to get all the required information for various attacks. It is worth noting that the attacker needs only an average of 5000 PIN guesses to find out the correct value when a four-digit PIN code is used. On the other hand, if the user decides to use sixteen 8-bit characters, it is very likely that she will write down the PIN code on a piece of paper. This is another weak point, because this piece of paper must be kept secret.

9. SECURE BLUETOOTH IMPLEMENTATION RECOMMENDATIONS:

Organizations should use the strongest Bluetooth security mode available for their Bluetooth devices.

1. Organizations using Bluetooth technology should address Bluetooth technology in their security policies and change default settings of Bluetooth devices to reflect the policies.
2. Organizations should ensure that their Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use.

10. CONCLUSION:

This study is performed to understand the details about Bluetooth security analysis tools (On-Line PIN Cracking script and Brute-Force BD ADDR Scanning script) and attacks (BTKeylogging attack and BTVoiceBugging attack). To know about the Scatternet formation and its related security issues. This report also lists the weaknesses in current Bluetooth transfers. Some useful steps that can be followed for secure transfer of data are also included.

REFERENCES

[1]Keijo M.J. Haataja- Detailed descriptions of new proof-of-concept Bluetooth security analysis tools and new security attacks ; Report B/2005/1

[2] Karen Scarfone John Padgette– Guide to Bluetooth Security Recommendations of the National Institute of Standards and Technology ; NIST Special Publication 800-121 September 2008

[3] Keijo Haataja- Security Threats and Countermeasures in Bluetooth-Enabled Systems ; Kuopio University Publications H. Business and Information Technology 13. 2009

[4] Karl E Persson and D. Manivannan-Secure Connections in Bluetooth Scatternets ; Computer Science Department University of Kentucky 2002

[5] Christian Gehrmann- Bluetooth™ Security White Paper; Bluetooth SIG Security Expert Group 2002 .