Overview, Working style and Safety Measures for Bluetooth Hacking

Author 1:	Author 2:	Author 3:
Devendra Vashi Lecturer, Institute of Technology, Nirma University Email: devendra.vashi@nirmauni.ac.in	Divya Brahmabhatt Student, Institute of Technology, Nirma University Email: D4divu@yahoo.com	Kamesh Jungi Student, Institute of Technology, Nirma University Email: kameshworld@yahoo.com

ABSTRACT

Bluetooth has shown promise as a wireless ad hoc networking protocol and will only continue to spread as more and more consumers cut the wires from their everyday lives. On the other side of the coin, Bluetooth has also shown the difficulties and pitfalls that exist when implementing a network such as this. Clearly, Bluetooth is not a perfect standard in any way, but it is a step in the right direction. It will be interesting to see what changes and improvements come about in future implementations of Bluetooth. For now, Bluetooth offers convenience and access to a broader base of information, but one must remember that there are people out there with malicious intent, and they can violate Bluetooth security. As long as everyone is aware of this and does their best to maintain some security, then Bluetooth can act as a sufficient step towards a world of secure ad hoc networks.

1. INTRODUCTION

Technology grows rapidly, and it will enhance the ways to doing something. Bluetooth technology similarly does that, but technology brings advantage as well as some limitation. Bluetooth hacking now is becoming popular. People are unaware that their PCs and mobiles and not secure may be it can be happened that someone is reading your massages on your mobile right now. There are lots of things can be done via Bluetooth hacking, the question is your mobile is safe or not?

Bluetooth technology was developed to replace cumbersome wires in portable and personal electronic devices. The protection of a consumer's valuable information and the contents of their communications have remained at the forefront of Bluetooth development.

Unfortunately, security vulnerabilities have remained an increasing problem as attackers have developed more sophisticated ways of violating Bluetooth security, and the problem only promises to become worse as Bluetooth devices permeate everyday life.

2. BLUETOOTH TECHMOLOGY

[BLUETOOTH TECHNOLOGY]

Bluetooth is a new technology named after the 10th century Danish king Harald Bluetooth Blatand who ruled part of Scandinavia in 960 AD .He helped unite his part of the world.

Bluetooth device is the revolutionary device launched by L.M Ericsson, to integrate its phone with all Internet enabled devices. This technology provides a way to connect and exchange

information between devices like personal digital assistants (PDAs), mobile phones, laptops, PCs, printers and digital cameras via a secure, low cost, globally available short-range radio frequency.

[Personal digital assistants (PDAs), mobile phones, laptops, PCs, printers]

Simply Bluetooth technology is wireless connect to

- Wireless headsets
- Handhelds
- Personal computers
- Printers
- Mobile phones
- Digital pens
- Automobiles etc.

3. WHY BLUETOOTH HACKING?

- People do hacking for fun
- Many time hacking take place because of profit motive
- Some people want to satisfy their Psychological Needs
- Some time reasons behind hacking is Extortion
- Bluetooth hacking is take place with view to taking Revenge
- To show and get benefit of Technical Reputation people do Bluetooth hacking
- It is a nice way to Exposing System Weakness and its improvement

4. HOW IT WORKS?

4.1 Bluetooth Authentication

_Like most wireless communication protocols, Bluetooth provides a way to authenticate connecting devices. This is accomplished through a system of shared secret keys. In Bluetooth, these are called link keys. Link keys are 128-bit secret keys that only the two devices know. This key is generated during the "pairing" portion of the communication setup between the two devices. Two connected Bluetooth devices are said to share a common link key. However, to complicate matters, Bluetooth allows for two types of keys: combination keys and unit keys.

4.2 Link Keys

Combination keys are the safer method of authenticating a device because these keys are only used between a pair of devices. This means that each connection using combination keys in a Bluetooth network has a distinct link key.

On the other hand, unit keys are simpler to maintain, but offer less security. Unit keys are link keys that are used by a device for each connection it makes. However, in order to add some small sense of security, only one device in a pair is allowed to use a unit key. The other device must use a combination key. Unit keys are typically used by devices which are unable to maintain large amounts of unique key pairs. The Bluetooth SIG has released an official recommendation that unit keys be used as little as possible. Sometimes, the device classified as the "master" device wants to transmit data to more than one recipient. To do this, something called a master key is created which temporarily replaces the link key. The master key informs the receivers that the data being transmitted to them is being sent to multiple devices as well as stating who the information is from. The generation of these keys will be discussed later.

4.3 Device Pairing

When two devices do not yet share a link key, they must perform a process known as "device pairing". The protocol begins when one of the devices—known as the "initiator"—transmits a random number to the other device, called the "responder". The responder then replies with a message indicating it received the random number. The two devices then proceed to calculate an initial key, Kinit, using the device address of the responder and the random number. This creation technique will be covered in a later section. Sometimes the responder has a fixed PIN that is uses to connect to other devices. In this case, when it receives the random number challenger from the initiator, it will generate a new random number and send it back to the initiator. The initiator then sends a response message accepting the challenge. The

devices then continue on in the protocol by calculating Kinit. The other case that may occur during the pairing process is one where both devices have fixed PINs that are required when pairing. In this case, after the responder replies to the initiator with its own random number, the initiator will see that the responder has a fixed PIN and reject the pairing. It also sends a message to the responder notifying it of the rejection. Once the devices have calculated Kinit, they then create a link key to use for their subsequent communications. This link key will be either a combination key or one of the device's unit keys. However, as stated previously, unit keys are not secure and are typically avoided unless absolutely necessary.

4.4 Key Generation

The Bluetooth protocol provides three different key generation algorithms. One algorithm is used for authentication (discussed later), one is used to produce keys, and one is used for encryption. Both Kinit and the link keys (either unit or combination keys) mentioned earlier are produced using variations of the same algorithm, known as E2. This algorithm is more complicated than is necessary for analysis in this overview of Bluetooth, so a short summary is sufficient.

Both modes produce 128-bit keys as was mentioned in an earlier section, so the more interesting portion is the different input each mode uses. To produce unit and combination keys, the algorithm uses the random number challenge and the Bluetooth device address to create the key. This makes sense since link keys pair to at least one device (unit key) and more often to a unique pair of devices (combination).

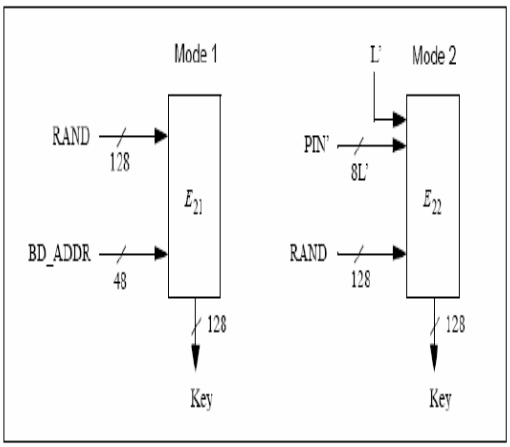


Figure 2 - Key generating algorithm E_2 and its two modes. Mode 1 (E_{21}) is used for unit and combination keys, while Mode 2 (E_{22}) is used for K_{init} and K_{master}. [1]

[Key Generation Algorithm E2 and its mode 1 & Mode2]

combination keys, while Mode 2 (E22) is used for Kinit and Kmaster. [1]

In Mode 2, the key generation algorithm uses the PIN (which is some number of octets in length) as well as the random number challenge. Also used as an input is the number of octets in the PIN (maximum of 16 octets). This design agrees with the previous statement that the purpose of the PIN is to assist in the initial communication setup of two devices, which is where Kinit plays a role. Once the keys have been created, authentication can begin.

4.5 Authentication Process

The process of authenticating a connecting device takes the form of the following protocol. (It is important to note that not all Bluetooth devices require authentication when connecting to other devices.)

A Bluetooth authentication(Figure 2) begins with the connecting device (Device_A) issuing a challenge to the device it would like to authenticate with (Device_B). This challenge takes the form of a 128-bit random number. This is often called the "authentication random number" and forms the base of the authentication algorithm.

Next, Device_B computes a 32-bit response which is called the "sign response". The sign response is calculated through the use of the E1 algorithm. Device_B takes the 128-bit challenge, its 48-bit Bluetooth address, and the link key being used by the devices and applies the E1 algorithm. This produces a 128-bit cipher, of which the 32 most significant bits are used as the sign response.

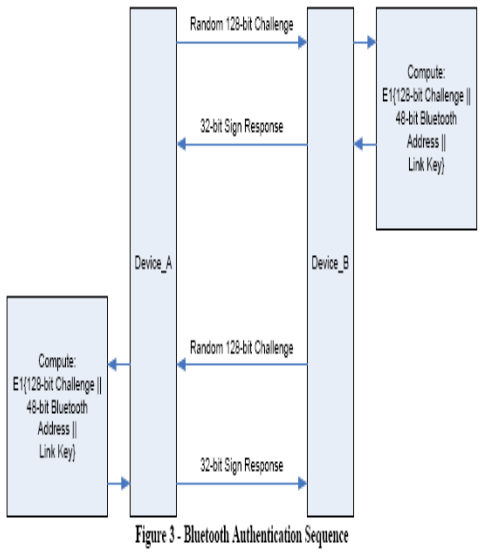


Figure 3 - Bluetooth Authentication Sequence

[Bluetooth Authentication Sequence]

Device_B then transmits the sign response to Device_A, who has performed the same calculation as Device_B. Device_A then compares the results, and if there is a match, then authentication has taken place.

The process is then repeated going the other direction (Device_A authenticating Device_B), and if this is successful as well, then mutual authentication has been completed, and the devices can begin their communication.

4.6 Encryption

The final piece of the Bluetooth security puzzle is data encryption. Encryption occurs at the packet level where groups of packets, called payloads, are encrypted before transmission. Encryption is accomplished using the E0 algorithm at its core. The basic structure of Bluetooth encryption can be found in Figure 4. Bluetooth encryption uses 4 linear shift registers (LSR) whose outputs pass through a finite state machine which produces an "encryption stream". The E0 algorithm must initialize the LSRs at the beginning of encryption, and it accomplishes this using an encryption key, known as Kc, a clock input, and a 48-bit device address. E0 outputs a cipher, Kcipher, which is then XOR'd with the transmitting data.

This encryption scheme assumes that Kcipher is difficult to guess, otherwise, the XOR function is extremely weak.

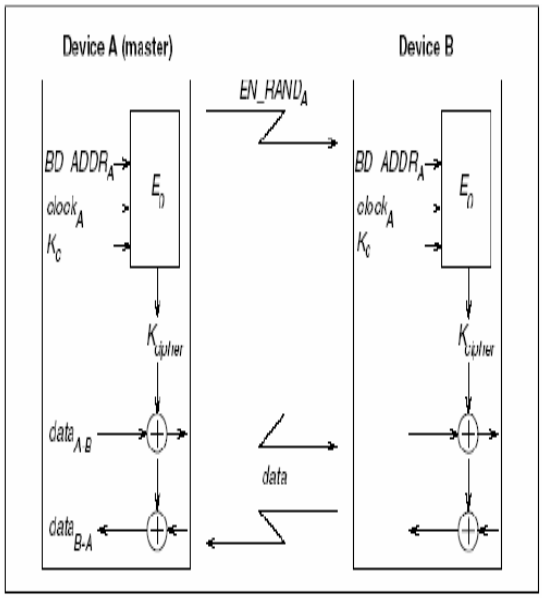


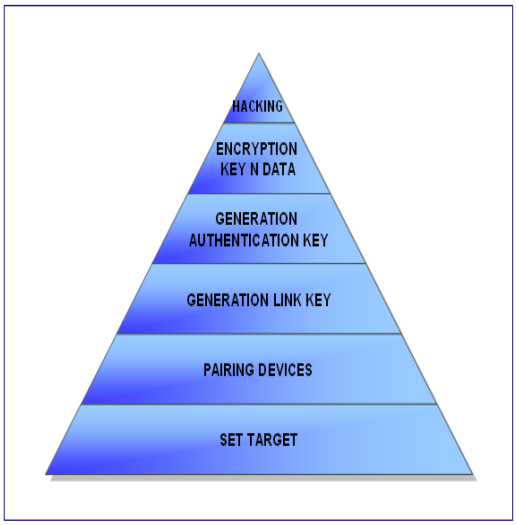
Figure 4 - Functional description of the encryption procedure [1]

[Functional Description of the encryption procedure]

Bluetooth supports many different encryption modes. First of all, if a unit or combination link key is used in communication, no broadcast data is encrypted. However, encryption can be enabled for individually specified traffic. If a master key is used in the communication, then three modes are available for encryption:

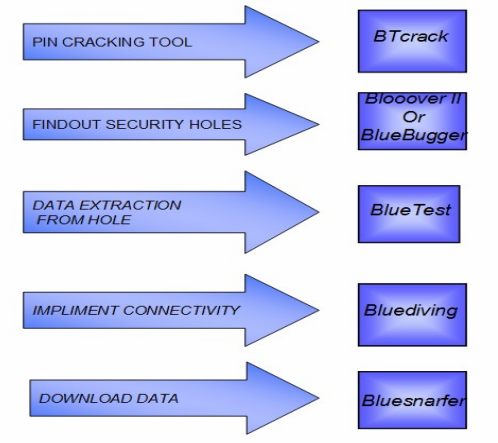
1. Mode 1 – Nothing is encrypted
2. Mode 2 – Broadcast traffic is not encrypted, but individually specified traffic is encrypted using the master key
3. Mode 3 – Everything is encrypted using the master key

This allows for flexibility depending on the application of Bluetooth. Clearly, most users will not require their Bluetooth mice to transmit encrypted data, but most consumers want their phones to work with full encryption.



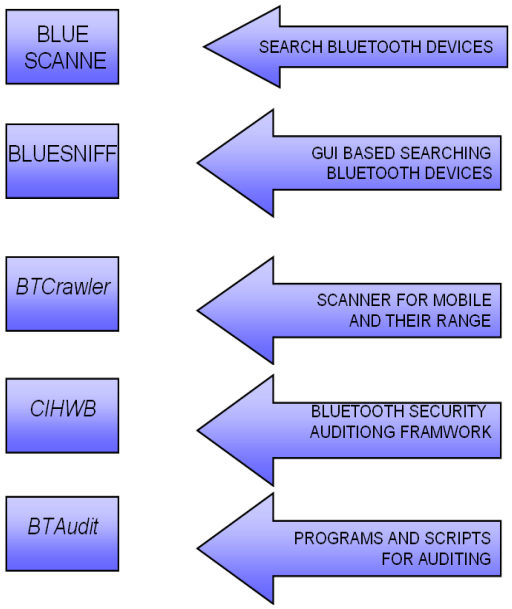
[PROCESS OF HACKING BLUETOOTH]

4. LUETOOTH HACKING TOOLS:



[Process of the Bluetooth]

Today Bluetooth hacking tools are being accepted which are used to perform different activities. They basically refer to one of the process of the Bluetooth mentioned above. Some of them are as follows.



[Process of the Bluetooth]

6. ATTACKS ON BLUETOOTH

- **BtScanner:** Extract as much information as possible from a Bluetooth phone without requiring a pairing.
- **BlueStumbler:** Monitoring and log all visible Bluetooth devices, and identify manufacturer from MAC address lookup
- **BlueBrowse:** Display available services on a selected device.
- **BlueJack:** Send anonymous message to a target device.
- **BlueSnarf :** Copy data from target device.
- **BlueBug :** Set up cover serial channel to device
- **RedFang:** Allows the discovery non-discoverable Bluetooth device through brute-forcing the last six digits of the device address.

7. SAFETY TIPS

- When you don't working on Bluetooth – STAY OFFLINE
- If you don't want to show your Id to other – STAY INVISIBLE
- Don't accept or run attachment from any unknown devices.
- Always use password protection with your device hence it can prevent Bluetooth hacking up to some extent and also keep your password always of more digits.

8. Conclusion

Unfortunately, even with all the security, authentication, and encryption designed into Bluetooth, it has proved to be a difficult system to keep secure. There continue to be new attacks launched at Bluetooth devices, especially cell phones, and this problem will only get worse.

Currently, there is no one solution that can protect a consumer from the vulnerabilities currently found in Bluetooth. However, there are a few things that users can do to reduce the chances of a security violation

- Do not worry about devices such as mice, keyboards, and other simple Bluetooth devices. These are unlikely to be the target of an attack.
- Only enable Bluetooth on cell phones when it is absolutely necessary Otherwise, keep it disabled.
- Do not open mysterious messages that appear on the phone. This can prevent attackers from spreading malicious content through BLUEJACKING.
- Bluetooth is beginning to be implemented in automobiles, but it has been shown that is it possible to transmit viruses to cars through Bluetooth— BEWARE!

9. REFERENCE

[1] Bluetooth Special Interest Group, "Specification of the Bluetooth System," 5 November 2003

[2] Gehrmann, Christian et al, "Bluetooth Security White Paper," Bluetooth SIG Security Expert Group, 19 February 2002

[3] Kardach, James, "Bluetooth Architecture Overview," Intel Technology Journal, 2000

[4] Kurose, James F. and Keith W. Ross, "Computer Networking: A Top-Down Approach Featuring the Internet, 3rd ed. (Boston: Addison Wesley, 2005)

[5] Laurie, Adam and Ben Laurie, "Serious flaws in Bluetooth security lead to disclosure of personal data," The Bunker,

[6] http://www.thebunker.net/security/bluetooth .htm (22 February 2005)[security tips]

[7] Newitz, Annalee, "They've Got Your Number…" Wired December S2004, 92.

[8] Vainio, Juha T. “Bluetooth Security,” Helsinki University of Technology, 25 May