BLUEJACKING: ITS OVERVIEW, PROCESS OF BLUEJACKING AND PREVENTIVE MEASURES

MRS. AKVINDER KAUR,

MCA, Assistant Professor in Computer Science,

Govind National College, Narangwal, Ludhiana, Punjab, India.

Abstract: Bluejacking is probably the most common form of Bluetooth hacking. This happens when a hacker searches for discoverable devices in the area and then sends spam in the form of text messages to the devices. This form of hacking is rather childish and harmless.It was once used mainly to prank people in the past when mobile devices came with Bluetooth that was automatically set to discoverable. Bluejacking is used today for spam messaging and the hackers who use this do it just to frustrate others. The method does not give hackers access to your phone or the information on it.Bluejacking involves Bluetooth users sending messages to other Bluetooth users within range. Although sensitive information may not be revealed, unwanted messages may show up on your device.

IndexTerms: Hijack, OBEX, bluesnarfing, Wi-Fi, PDA.

1. INTRODUCTION:

Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.

Bluetooth has a very limited range, usually around 10 metres (32.8 ft) on mobile phones, but laptops can reach up to 100 metres (328 ft) with powerful (Class 1) transmitters.

Bluejacking is usually harmless, but because bluejacked people generally don't know what has happened, they may think that their phone is malfunctioning. Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well. Bluejacking has been used in guerrilla marketing campaigns to promote advergames.

Bluejacking was reportedly first carried out between 2001 and 2003 by a Malaysian IT consultant who used his phone to advertise Ericsson to a single Nokia 7650 phone owner in a Malaysian bank. He also invented the name, which he claims is an amalgam of Bluetooth and *ajack*, his username on Esato, a Sony Ericsson fan online forum. *Jacking* is, however, an extremely common shortening of hijack, the act of taking over something.

2. BLUETOOTH BLUEJACK

Bluetooth technology operates by using low-power radio waves, communicating on a frequency of 2.45 gigahertz. This special frequency is also known as the ISM band, an open, unlicensed band set aside for industrial, scientific and medical devices. When a number of Bluetooth devices are switched on in the same area, they all share the same ISM band and can locate and communicate with each other, much like a pair of walkie talkies tuned to the same frequency are able to link up.Bluetooth technology users take advantage of this ability to network with other phones and can send text messages or electronic business cards to each other. To send information to another party, the user creates a personal contact name in his or her phone's address book -- the name can be anything from the sender's actual name to a clever nickname.

Bluejackers have devised a simple technique to surprise their victims: Instead of creating a legitimate name in the address book, the bluejacker's message takes the place of the name. The prank essentially erases the "from" part of the equation, allowing a user to send any sort of comment he wishes without indentifying himself.For instance, if you're sitting in a coffee shop and notice a fellow Bluetooth user sitting down to enjoy a cup of iced coffee, you could set up a contact under the name "Is your coffee cold enough?" After choosing to send the text via Bluetooth, the phone will search for other enabled Bluetooth devices; selecting one will send the unsolicited message to that device. A bluejacker's crowning moment comes, of course, when the victim receives the message and expresses a mild mix of confusion and fear that he's under surveillance.

Bluejacking is imprecise, however. Searching for other Bluetooth-enabled hardware might turn up a list of devices labeled with a series of numbers and letters. Unless the bluejacker's target has chosen to publicly identify his or her phone, or it's the only Bluetooth phone in the area, the bluejacker may have a hard time messaging his or her target on the first try.

3. OBEX PROTOCOL:

The heart of file transfer over Bluetooth is called Object Exchange, or OBEX protocol, a binary file transfer protocol run over not merely Bluetooth but also Infrared and even generic TCP/IP. It is a session layer protocol designed to enable systems of various types to exchange data and commands in a resource sensitive standardized fashion. The OBEX protocol is optimized for ad-hoc wireless links and can be used to exchange all sorts of objects, like files, pictures, calendar entries, and business cards. It also provides some tools to enable the objects to be recognized and handled intelligently on the receiving side. 3) OBEX‟s operating functionality and resemblance to HTTP: OBEX is designed to provide push and pull functionality in such a way that an application using OBEX does not need to get involved in managing physical connections. The application only takes an object and sends it to the other side in a "point-and-shoot" manner. This is similar to the the role that HTTP serves in the Internet protocol suite, although HTTP is designed more for data retrieval, while OBEX is more evenly balanced for pushing and pulling data.

4. HOW TO BLUEJACK:

First Assume that you now have a Bluetooth phone in your hands, the thing is to make sure that Bluetooth is enabled. Then you will need to read the handbook of the particular phone (or PDA etc) that you have but somewhere in the Menu item then you will find the item that may enables and disabled Bluetooth.

Steps are as follows:

(i) Bluetooth devices only work over short distances, so we need to find a big crowd. Bluejacking is a very new technology so not everyone will have a Bluetooth phone or PDA. So the bigger the crowd the more we may find a 'victim'.

(ii) (ii) We now need to create a new Contact in our Phone Book - rather putting someone's name in the Name field we must write short message like - "Hey, you have been BlueJacked!" .

(iii) Press done/ok option. Save this new contact in the phone/address book of mobile phone/laptop respectively.

(iv) Then click on the contact created. Go to action. choose "via Bluetooth" or "Send to Bluetooth" option.

(v) Click the "Search‟ option for discovering active Bluetooth devices. Select a device from those list.

(v) After the selection of the particular device, the short message would be transmitted to it. Thus, the device Wouldbe bluejacked.

5. ADVANTAGES OF BLUEJACKING :

1.Usually, a bluejacker will only send a text message, but with modern phones it's possible to send images or sounds as well .

2.People can send any image or sound but not insulting.

3.Any copyright sound files will only be sent with the written consent of the copyright holder.

4.We can easily transfer data from mobile to laptop or from mobile to mobile in a short period.

5.We can even enjoy music by wireless headphones through Bluejacking.

6. DISADVANTAGES OF BLUEJACKING :

1.But with the increase in the availability of Bluetooth enabled devices, these devices have become vulnerable to virus attacks and even complete takeover of devices through a

Trojan horse program. These may even cause irritation in any person as these are just unwelcomed messages or some jokes.

2.They can annoy anyone very easily.

7. HOW TO PREVENT BLUEJACKING:

Bluejacking is mostly used by people as a way to market their products and services. However, this is not an advisable and efficient way as it confuses the receiver, making him think that his device is malfunctioning. Although harmless, bluejacking can get annoying at times, as the recipient doesn't know who the message sender is. There are certain ways by which it can be prevented on our devices, few of which have been mentioned below:

Setting the Bluetooth on the Right Mode

If you happen to use the Bluetooth connection more often, putting it off/on can be a chore. Adjust the setting of Bluetooth to non-discoverable mode. The non-discoverable mode hides the device from attackers or unknown people.

Factory Reset of the Phone

If your device was perpetrated at some point, it means that the attacker's device has already been added as a trusted device on your phone. Reset the phone to take off all the devices from the trusted list.

Keep Away from Strangers

Make it a point to decline any messages or connection requests from unknown devices. Most attacks happen due to accepting connection requests from strangers who then get added as trusted devices.

Keep the Device Updated and Password Character Strong

Make sure you maintain strong passwords and change them at regular intervals. Keep your devices up-to-date with the latest technology.

Putting off the Bluetooth When Not in Use

If you don't use the Bluetooth connection frequently, keep it off to avoid your device from being listed in the sender's device search list. This method keeps the device safe from perpetrators who try to gain access to others' phones using Bluetooth.

Set Password for Bluetooth

It is very simple to secure your device by setting a pin or a password for your Bluetooth connection. This will prompt a password from anyone trying to pair with your device. Remember to keep this password secure by sharing it only with trusted people.

One advantage of using latest technology gadgets like as iPhone or iPad is that bluejacking is restricted on them. Perpetrators, besides sending unsolicited messages, can also hack into confidential data from a victim's device, thus, rendering him helpless. This is a much harmful form of hijacking, which is called bluesnarfing.

Almost everyone today has a smartphone and one of the features that comes standard is Bluetooth capability. Since your device has Bluetooth capabilities, it also has the capability to be hacked.If your smartphone is hacked via Bluetooth connection, you are potentially at risk of losing your phone's data, pictures, videos, messages, contacts, and other information compromised. Today if you own a smartphone, you are walking around with a small computer in your pocket.

8. BLUETOOTH SECURITY:

- In any wireless networking setup, security is a concern. Devices can easily grab radio waves out of the air, so people who send sensitive information over a wireless connection need to take precautions to make sure those signals aren't intercepted.
- Bluetooth technology is no different — it's wireless and therefore susceptible to spying and remote access, just like WiFi is susceptible if the network isn't secure. With Bluetooth, though, the automatic nature of the connection, which is a huge benefit in terms of time and effort, can also be a benefit to people looking to send you data without your permission.

- Bluetooth offers several security modes, and device manufacturers determine which mode to include in a Bluetooth-enabled gadget. In almost all cases, Bluetooth users can establish "trusted devices" that can exchange data without asking permission. When any other device tries to establish a connection to the user's gadget, the user has to decide whether or not to allow it. Service-level security and device-level security work together to protect Bluetooth devices from unauthorized data transmission.

- Security methods include authorization and identification procedures that limit the use of Bluetooth services to the registered user and require that users make a conscious decision to open a file or accept a data transfer. As long as these measures are enabled on the user's phone or other device, unauthorized access is unlikely. A user can also simply switch his Bluetooth mode to "non-discoverable" and avoid connecting with other Bluetooth devices entirely. If a user makes use of the Bluetooth network primarily for syncing devices at home, this might be a good way to avoid any chance of a security breach while in public.

- Still, early cell-phone virus writers took advantage of Bluetooth's automated connection process to send out infected files. However, since most phones use a secure Bluetooth connection that requires authorization and authentication before accepting data from an unknown device, the infected file typically doesn't get very far. When the virus arrives in the user's cell phone or smartphone, the user has to agree to open it and then agree to install it. This has, so far, stopped most cell-phone viruses from doing much damage.

9. FUTURE ASPECTS OF BLUEJACKING :

Looking at its current use and misuse also by few people, it is expected that in the future, it may have the following aspects. Either it will be used extensively and people would be able to get all the necessary information on their devices if they have their Bluetooth on, Or people will stop using Bluetooth even and only bluejackers will be playing with each other, Or some new way could be developed in order to find the location of the device sending a blue jack request and their location can be traced. If they keep send annoying messages, we can find them out and can register a complaint against them. By this way, Bluetooth will be made more reliable.

10. CONCLUSION:

In conclusion, it can be said that bluejacking is not at all harmful. By it, we can interact with new people. The only thing it can do at worst is to irritate you or annoy you by sending unsolicited messages but you can still prevent yourselves from these messages by changing the visibility of your Bluetooth to invisible or non-discoverable mode.

It can be helpful as well by providing you with lots of useful information as well. So, use this technology properly as it is intended and get best of it, rather than just making wrong use of it and irritating othersBest practices to mitigate the Bluejacking threats against the Bluetooth are: user awareness, disable device when not in use, use an unidentifiable device name, employ security mode 3 or 4, disable unused services and profiles, set device to non-discoverable mode when not in use, use non-guessable PIN codes of at least 12 or more alphanumeric characters and perform pairing only when absolutely required.

11. REFERENCES:

- Ariadn Web Magazine for Information Professionals Overview of content related to 'vcard'.

- Mining Bluetooth Attacks in Smart Phones, Seyed
- Morteza Babamir, Reyhane Nowrouzi, Hadi Naseri.
- Bluejacking by Jonathan Samuel, First Edition: 1997 by
- Tata McGraw Hill.
- Bluetooth Special Interest Group (SIG) (Oct. 21, 2019) http://www.bluetooth.com
- Bluetooth SIG. "Bluetooth Core Specification v5.1." Jan. 21, 2019. (Oct. 28, 2019). https://www.bluetooth.org/docman/handlers/downloaddoc.ashx?doc_id=457080
- Bluetooth SIG. "Understanding Bluetooth Range." (Oct. 27, 2019) https://www.bluetooth.com/bluetooth-technology/range/
- Fleishman, Glenn. "Inside Bluetooth 2.0." Macworld.com. Feb. 9, 2005. (Oct. 21, 2019) http://www.macworld.com/news/2005/02/09/bluetooth2/index.php
- Mobile Resource Group. "Lions and tigers ... and Bluesnarfing." Credentialed Mobile Device Security Professional. 2019. (Oct. 28, 2019) https://cmdsp.org/2019/08/12/lions-and-tigers-and-bluesnarfing/