International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 02 Issue: 03 | June-2015 www.irjet.net p-ISSN: 2395-0072

Review Paper on Novel Communication Technique: BLUEJACKING

Pankaj Gakare[1], Yogita Dhole[2]

[1] *Asst. Professor, Department of E & TC, DMIETR, Maharashtra, India*
[2] *M. Tech. Student, Department of CSE,* AMR Institute of Technology, Adilabad

---

Abstract - *This research paper is about the technology used for sending unsolicited messages over Bluetooth to Bluetooth to Bluetooth-enabled devices such as cell phones, laptops or computers, called Bluejacking. Range of Bluetooth is limited and hence the range of bluejacking is also limited. This technology allows phone users to send business cards i.e. vCards, anonymously using Bluetooth wireless technology using OBEX (Object Exchange) protocol. Receiver does not know who has sent the message, but it has the name and the model of the phone of a bluejacker. Devices that are set in non-discoverable, hidden or invisible mode are not susceptible to Bluejacking. Many people are still not aware of this technology. This paper discusses about Bluejacking and is written to make people aware of it, its use, its misconceptions, prevention measures and also considers its advantages, disadvantages and future aspects.*

Key Words: bluejacking, bluejacker, OBEX, vCards

1. INTRODUCTION

Blue jacking is an attack conducted on Bluetooth compatible devices, such as smart phones, laptops and PDAs. Blue jacking is instigated by an attacker (termed as bluejacker or blue jack addict) who forwards unsolicited messages to a user of Bluetooth-enabled device. When the connection goes through, the bluejacker tries to send a message to the recipient. The actual message sent to the user's device does not cause detriment but is used to inveigle the user to counter react in some manner or add the new contact to the device's address book. This message-transmitting attack resembles spam and phishing attacks conducted against email users. Blue jacking can be perceived as either infuriating or amusing, though it is relatively risk-free since the recipient has the option to decline. Blue jacking sure makes for an interesting wake-up call in close-knit environments like underground metro trains, buses, malls and cinemas.

Blue jacking was allegedly first conducted by a Malaysian IT consultant, 'Ajack' (his username a Sony Ericsson online forum), who used his Bluetooth-enabled phone to publicize Sony Ericsson. He also coined the name, which is an amalgam of Bluetooth and hijacking. While standing in a bank queue, Ajack turned on his Bluetooth, discovered a Nokia 7650 in the vicinity, created a new contact with 'Buy Ericsson!' as the first name, and sent that business card to the Nokia phone. The recipient of the Nokia phone standing a few feet away from him was startled to see such an 'advertisement'. Ajack posted this story on Sony Ericsson forum and other people started trying it out. Blue jacking has become a rage amid young people keen to play practical jokes. A 13-year-old girl named Ellie from Surrey, UK has created a website called 'bluejackq' where people can share their blue jacking experiences.

2. BLUEJACKING TECHNOLOGY

The Bluetooth port of the mobile phones is subject to threat of blue jacking attack. Bluejacker carefully crafts the identification that devices exchange during association and then transmits short, deceitful text messages into authentication dialogs. Thus, bluejacker tricks the user and gains access to user's phone book, calendar, or file residing on the device. Blue jacking is based on following technologies:

2.1 *BLUETOOTH TECHNOLOGY:*

1) Bluetooth as a Wireless Technology: Bluetooth, the latest development in wireless communications technology is a wireless standard that is designed for very short-range (less than 10 meters). It is a de facto standard, as well as a specification short range radio links. It is most appropriate for communication between computers or mobile devices and peripheral devices, such as to connect a wireless keyboard or mouse to a desktop PC, to send print jobs wirelessly from a portable PC to a printer, or to connect a mobile phone to an earpiece.

2) Usage of Bluetooth: Since Bluetooth devices automatically recognize each other when they get within transmission range, handheld/desktop PC's and mobile devices can always be networked wirelessly when they are within range. Bluetooth signals can transmit through clothing and other non-metallic objects, so a mobile phone or other device in a pocket or briefcase can connect with the user's Bluetooth headset, without having to be removed from the pocket or briefcase. Some industry experts predict that major household appliances will be Bluetooth-enabled in the future, resulting in an automatic, always connected, smart home.

3) Bluetooth Frequency Specification and Operating Principle: Bluetooth works using radio signals in the frequency brand of 2.4GHz, the same as Wi-Fi, and supports data transfer rates of up to 3Mbps. Once two Bluetooth- enabled devices come within range of each other, their software identifies each other (using their unique identification numbers) and establishes a link. Because there may be many Bluetooth devices within the range, up to 10 individual Bluetooth networks (called Piconets) can be in place within the same physical area at one time. Each Piconet can connect up to eight devices, for maximum of 80 devices within any 10-meter radius.

4) Bluetooth as Cable Replacement Technology: Bluetooth is competent of transmitting voice, data, video and still images. It can be used to wirelessly synchronize and transfer data among devices and can be thought of as a cable replacement technology.

5) Future Trends in Bluetooth Technology: The Bluetooth Special Interest Group is an industry group consisting of leaders in the telecommunications, computing, and networking industries that are driving development of the technology and bringing it to market.

6) *Advantages of Bluetooth:*

a) The main advantage of Bluetooth is that it can be full duplex mode.
b) It can handle both data and voice. Bluetooth standard uses both data link layer and application layer and hence supports both data and voice applications.
c) It's a very cheap, in fact free and easy way to send data.
d) It does not depend on the network provider or on your phone number.
e) It is robust.

7) *Disadvantages of Bluetooth:*

a) It is also a doorway to various techniques like Blue jacking, Blue snarfing (also called Bluetooth hacking).
b) As the same band is used for all the Bluetooth connections in an area, so it is prone to hack.

2.2 OBEX PROTOCOL:

1) OBEX as the heart of Bluetooth files transfer: 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. The Open OBEX project at http://openobex.sf.net/offers the most ubiquitous open source implementations of the protocol.

2) Usage of OBEX: 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 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) Devices supported by OBEX:

a) All Palms since Palm III, except the Palm Pre, Palm Pre Plus, Palm Pixi and Palm Pixi Plus.
b) Most Sharp, Motorola, Samsung, Sony Ericsson, HTC and Nokia phones with infrared or Bluetooth port.
c) LG EnV Touch (VX11000).
d) Many other PDAs since 2003.

2.3 VCARD FUNCTIONALITY:

1) vCard as a Standard of Communication: Address Book exchanges contact information with other programs primarily through vCards. vCard is short for virtual business card. More and more email programs send and receive these electronic business cards, which can be identified by their .vcf filename extensions.

2) History: The vCard standard has been around since 1996 and the current version, version 3.0, is specified by the IETF. The vCard or Versitcard was originally proposed in 1995 by the Versit consortium, which consisted of Apple Computer, AT&T Technologies (later Lucent),IBM and Siemens. In December 1996 ownership of the format was handed over to the Internet Mail Consortium, a trade association for companies with an interest in Internet e-mail.

3) vCard Features:

a) vCards are structured blocks of text data that provide what is more or less an electronic business card. The data can include name, address, telephone numbers (home, business, fax, pager, cellular, ISDN, voice, data, video), e-mail addresses and related internet URLs.
b) vCards can also include graphics and multimedia, including photographs, company logos, audio clips, along with geographic and time-zone information.
c) vCards are also designed to support multiple languages and are transport and operating system independent.

4) Applications of vCards:

a. Infrared Exchange
b. Bluetooth Exchange
c. Internet Mail
d. Computer/Telephony Applications
e. Video and data conferencing

3. PROCESS OF BLUEJACKING

The fundamental course of action of blue jacking is quite concise, trouble-free and effortless. It can be implemented by using the following steps:

Step 1: Go to contacts in the phone book (if using mobile) or address book program like Outlook (if using PCs/laptops).

Step 2: Choose the "New Contact" option. Consecutively, create a new contact.

Step 3: Enter the desired message into the 'name' field with which one wants to blue jack the other device. Messages like 'you have been blue jacked!' startle the victim.

Step 4: Press Done/OK option. Save this new contact in the phone/address book of mobile phone/laptop respectively.

Step 5: Click on the contact created. Go to action. Choose "via Bluetooth" or "Send to Bluetooth" option.

Step 6: Click the 'Search' option for discovering active Bluetooth devices. Select a device from the list.

Step 7: After the selection of the device, the message would be transmitted to it. Henceforth, the device would be bluejacked.

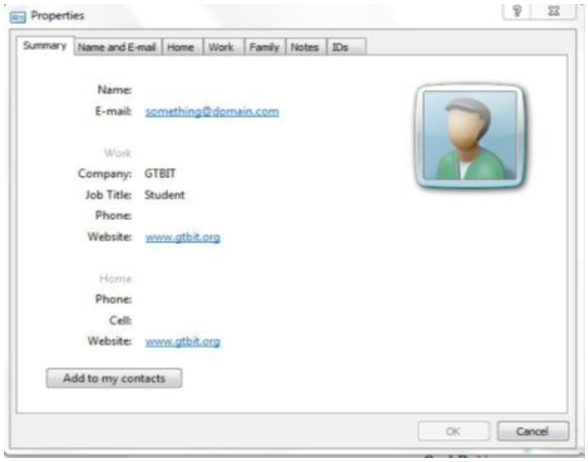

Fig. - 1: vCard saved in vcf format, viewed using 'Windows Contacts' application, shows various parameters along with 'Add to my contacts' option.

4. ADVANTAGES

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.

5. DISADVANTAGE

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

2. These may even cause irritation in any person as these are just unwelcomed messages or some joke.

6. APPLICATIONS

It can be used at many places, in many fields and for various purposes. Various main fields where it is used are:

1. It can be used in malls for advertisement purposes. As you cross their shop, you can get a message or any latest scheme they are providing on that day, etc.

2. They can be used at railway station to give you information about various general rules and about train timings, etc. Someone can even annoy you by sending useless messages. So, it is advisable to keep it off at these public places.

3. It can also be used at café, restaurant, cinema, mobile phone shop or at any electronic shop (e.g. Dixons) to provide you various information regarding them but any other random person can also send you the Blue jack messages and hence can even annoy you.

4. Viral interaction: Blue jacking can be utilized to exploit the communication paradigm between consumers and producers to share content such as text, images, videos and Internet references. Certain brands have already created multimedia content that has very rapidly been circulated around using blue jacking technology. Thus, blue jacking has replaced the conventional advertising via standardized broadcasting medium.

5. Community Activities: Social Networking or gaming events can be facilitated using Bluetooth as a channel for potential participants to converse.

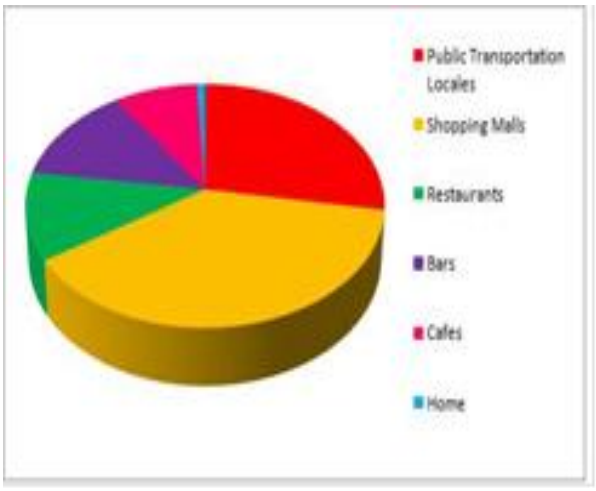

Fig. - 2: Comparison of Different applications of Bluejacking

7. MISCONCEPTIONS

Some people say that this term is originated by a user named Ajack on esato.com. Several people have said that blue jacking comes from Bluetooth plus hijacking. That obviously sounds logical but actually a bluejacker does not hijack anything.

1. Blue jacking doesn't give the sender any personal data. Your device remains absolutely safe from any sort of data modification.

2. It actually just creates annoyance.

3. A bluejacker just simply sends a contact to the recipient's device. Both of them, i.e. sender and receiver have complete control onto their devices, and he will not be able to get control of your device and hence, would not be able to steal any of your personal information.

4. Blue jacking is actually harmless, but because blue jacked people don't know what is happening, they think 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. So, this is a very interesting technology and such misconceptions about it must be removed from our minds.

Hence blue jacking is not actually harmful. It can provide you with lots of information as well as you pass by. You may not notice all such things when you are going through any road, etc. but now by just looking at your phone you can get all the latest information, latest schemes going on in any shop, etc. without even entering that. But obviously for some People, it is only something for fun and only those people are making inefficient use of it and hence making its name bad.

8. FUTURE ASPECTS

Looking at its current use and misuse also by few people, it is expected that in the future, it may have the following aspects:

1. Either it will be used extensively or people would be able to get all the necessary information on their devices if they have their Bluetooth on.

2. Or people will stop using Bluetooth even and only bluejackers will be playing with each other.

3. 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.

4. Bluejackers would only be able to send messages/pictures. They will never even try to hack any device for copying or modifying any files on any device or upload any executable files there. By hacking a device, you are supposed to commit an offence under the computer misuse act 1990, which states it is an offence to obtain unauthorized access to any computer. Changes in this law soon will cover all the mobile devices only.

9. CONCLUSION

Bluetooth is a great technology with many useful applications. At the same time, variety of Bluetooth hacking tools and techniques are available, Blue jacking being the most vulnerable of the lot, which makes it a little riskier to use this technology. Bluetooth is not going to go away because of a few security flaws; instead it can be secure if configured properly and used carefully with a proper understanding of this wonderful technology. Best practices to mitigate the Blue jacking 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. Many users take privacy for granted. Unfortunately, the Bluetooth system wasn't intended for confidential purposes. Although improvement in the domain of Bluetooth security has been made, one should never assume that information being sent using a Bluetooth connection is private. Attachments, if sensitive, should be encrypted before they are sent across. Blue jacking first showed up in popular use in 2003 or so when Bluetooth devices gained popularity. It has hitherto been used for advertising purposes by vendors. It is the modus operandi by which we can network with new people and has the ability to revolutionize market by propelling advertisements about the products, services, enterprises, etc. on the Bluetooth-configured devices. Blue jacking is more of a prank than an attack, and unquestionably an annoying one at that, but at the same moment its future prospects in the field of advertising and marketing are vividly dazzling.

REFERENCES

[1] Information Security Management Handbook, Sixth Edition. Edited by Harold F. Tipton, Micki Krause..
[2] Do You Speak American? Words That Shouldn't Be? Sez Who? Cyberspace | PBS.
[3] http://en.wikipedia.org/wiki/OBject_EXchange#Supported_devices, Devices supported by OBEX protocol.
[4] Ariadn Web Magazine for Information Professionals Overview of content related to 'vcard'.
[5] Mining Bluetooth Attacks in Smart Phones, Seyed Morteza Babamir, Reyhane Nowrouzi, Hadi Naseri.
[6] https://www.bluetooth.org/apps/content/, *Bluetooth Special Interest Group.*
[7] Guide to Bluetooth Security, Special Publication 800-121, National Institute of Standards and Technology, U.S. Department of Commerce
[8] Bluejacking 'a harmless prank' By Stephen Whitford, IT Web Journalist.
[9] PocketMagic. Bluetooth BlueJacking. By Radu Motisan. September 16th, 2008.
[10] Bluetooth group drops ultra wide band, eyes 60 GHz, Report: Ultra wide band dies by 2013, Incisor Magazine November 2009

