A

Seminar-II Report

on

BLUEJACKING

Submitted in Partial Fulfillment of
the Requirements for the Degree
of

Bachelor of Engineering

in

Computer Engineering

to

North Maharashtra University, Jalgaon

Submitted by

Vrushali S. Patil

Under the Guidance of

Mr. Manoj E. Patil

DEPARTMENT OF COMPUTER ENGINEERING
SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY,
BAMBHORI, JALGAON - 425 001 (MS)

2016 - 2017

SSBT's COLLEGE OF ENGINEERING AND TECHNOLOGY, BAMBHORI, JALGAON - 425 001 (MS)

DEPARTMENT OF COMPUTER ENGINEERING

CERTIFICATE

This is to certify that the Seminar-II entitled *Bluejacking*, submitted by

Vrushali S. Patil

in partial fulfillment of the degree of *Bachelor of Engineering* in *Computer Engineering* has been satisfactorily carried out under my guidance as per the requirement of North Maharashtra University, Jalgaon.

Date: October 4, 2016
Place: Jalgaon

Mr. Manoj E. Patil
Guide

Prof. Dr. Girish K. Patnaik
Head

Prof. Dr. K. S. Wani
Principal

Acknowledgements

I would like to extend our deep gratitude to almighty God, who has enlightened us with power of knowledge. I wish to express my sincere and deep gratitude to Dr. Kishor S. Wani Sir(Principal, SSBT's COET Bambhori, Jalgaon) for giving me such a great opportunity to develop this report. Inspiration and Guidance are invaluable in all aspects of life especially on the fields of gratitude and obligation and sympathetic attitude which I received from respected Dr. Girish K. Patnaik Sir (Head of computer department, COET, Jalgaon) whose guidance and encouragement contributed greatly to the completion of this report.

I wish to express my sincere and deep gratitude to Mr. Manoj E. Patil whose guidance and encouragement helps in completion of this report.

I would like to thanks to all faculty members of Computer Engineering Department. I would like to thanks to my parents and all friends for their co-operation and supports in making this seminar report successful. I acknowledge my sincere gratitude to all who have directly or indirectly helped me in completing this report successfully.

Vrushali S. Patil

Contents

List of Figures

Abstract

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 meters on mobile phones, but laptops can reach up to 100 meters with powerful transmitters. Bluejacking allows phone users to send business cards anonymously using Bluetooth wireless technology. Bluejacking does not involve the removal or alteration of any data from the device. Bluejackers often look for the receiving phone to ping or the user to react. In order to carry out a bluejacking, the sending and receiving devices must be within 10 meters of one another. Phone owners who receive bluejack messages should refuse to add the contacts to their address book. Devices that are set in non-discoverable mode are not susceptible to bluejacking. Mobile phones have been adopted as an everyday technology, and they are ubiquitous in social situations as users carry them around as they move through different physical locations throughout the day. As a communicative device, the mobile phone has been gradually taken up in ways that move beyond merely providing a channel for mediated conversation. One such appropriation is bluejacking, the practice of sending short, unsolicited messages via vCard functionality to other Bluetooth-enabled phones. To choose the recipients of bluejacks, senders complete a scan using their mobile phones to search for the available Bluetooth-enabled devices in the immediate area.

Chapter 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 meters on mobile phones, but laptops can reach up to 100 meters with powerful transmitters. Bluejacking allows phone users to send business cards anonymously using Bluetooth wireless technology. Bluejacking does not involve the removal or alteration of any data from the device.[1]

Figure 1.1: Bluetooth transmition

Bluejackers often look for the receiving phone to ping or the user to react. In order to carry out a bluejacking, the sending and receiving devices must be within 10 meters of one another. Phone owners who receive bluejack messages should refuse to add the contacts to their address book. Devices that are set in non-discoverable mode are not susceptible to bluejacking.Mobile phones have been adopted as an everyday technology, and they are ubiquitous in social situations as users carry them around as they move through different physical locations throughout the day. As a communicative device, the mobile

phone has been gradually taken up in ways that move beyond merely providing a channel for mediated conversation. One such appropriation is bluejacking, the practice of sending short, unsolicited messages via vCard functionality to other Bluetooth-enabled phones. To choose the recipients of bluejacks, senders complete a scan using their mobile phones to search for the available Bluetooth-enabled devices in the immediate area. A bluejacker picks one of the available devices, composes a message within a body of the phones contact interface, sends the message to the recipient, and remains in the vicinity to observe any reactions expressed by the recipient.

In this chapter, to give Introduction about bluejacking. In Section 1.1 learn about the Bluejacking technology and their Marketing opportunity. With their subpoint.

1.1 Marketing opportunity

This mechanism by which messages can be sent between Bluetooth devices - predominantly mobile phones - has provoked discussion within the marketing community as to whether Bluetooth could be used as a promotional communication channel.

Bluejacking offers three distinct opportunities for marketers:

1.1.1 Viral communication

Exploiting communication between consumers to share content such as text, images and Internet references in the same way that brands such as Budweiser, Honda, Trojan Condoms and even John West Salmon, have created multimedia content that has very quickly been circulated around the Internet.

1.1.2 Community activities

Dating or gaming events could be facilitated using Bluetooth as a channel to communicate between participants. The anonymous nature of bluejacking makes is a superb physiological tool for communication between individuals in a localized environment such as a caf or pub.

1.1.3 Location based services

Bluejacking could be used to send electronic coupons or promotional messages to consumers as they pass a high street shop or supermarket. To date SMS text messaging has been used with mixed success as a mechanism to send consumers location based information Rainier PR believes that viral communication and to a lesser extent event based activities offer the greatest opportunity for bluejacking as a marketing mechanism. Already companies are looking at ways of exploiting the technology in these two areas. London, UK-based TagText

has made available a series of urban avatars available free for consumers to send each other. The company is tight lipped about its ultimate product and goals but has done a superb job of raising its profile by making available a series of free media properties. What is clear is that TagText wants consumers to send TagText characters to each other and raise the profile of the company.[2]

1.2 Summary

In this chapter the introduction of Bluejacking. It described its How to send unsolicited massege over the Bluetooth to Bluetooth enable device. In the next chapter is literature survey will discuss.

Chapter 2

Literature survey

This bluejack phenomenon started after a Malaysian IT consultant named “Ajack” posted a comment on a mobile phone forum. Ajack told IT Web that he used his Ericsson cellphone in a bank to send a message to someone with a Nokia 7650.[3]

In this chapter, discuss about the literature survey and the history in Section 2.1. In Section 2.2 learn about the Bluejacking technology. With their subpoint. Also explain there related concept in Section 2.3.

2.1 Origin

This bluejack phenomenon started after a Malaysian IT consultant named “Ajack” posted a comment on a mobile phone forum. Ajack told IT Web that he used his Ericsson cell phone in a bank to send a message to someone with a Nokia 7650. Becoming bored while standing in a bank queue, Ajack did a Bluetooth discovery to see if there was another Bluetooth device around. Discovering a Nokia 7650 in the vicinity, he created a new contact and filled in the first name with ‘Buy Ericsson!’ and sent a business card to the Nokia phone. “A guy a few feet away from me suddenly had his 7650 beep. He took out his 7650 and started looking at his phone. I couldn’t contain myself and left the bank”, he says. Ajack then posted the story on a mobile Web site and other people started trying it out. “I gave it the name bluejacking (taken from the words Bluetooth and hijacking) and it has just taken off from there”. He says bluejacking is common in Malaysia and is happening everywhere there are lots of Bluetooth devices. Bluejacking has become popular among young people wanting to play practical jokes. A 13-year-old named Ellie from Surrey in the UK has started a dedicated bluejacking site called bluejackq. The site explains what bluejacking is and also has forums where people can share their bluejacking experiences.

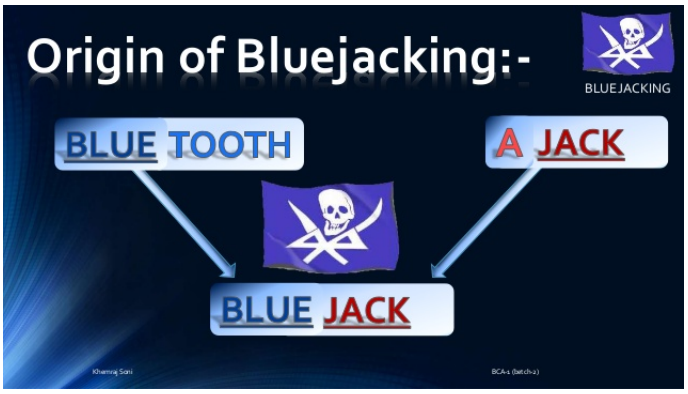

Figure 2.1: Origin of Bluejacking

Conceptualize bluejacking as a violation of possessional territory. Inspired by Goffman, we propose that the mobile phone is a possessional territory as a result of the intimacy and continued contact between mobile phone users and their phones. A possessional territory, in our usage, is an object that engenders attachment and defense by those who perceive possession and can be referred to as a "personal effect". Possessional territories function "egocentrically"; that is, they move around with their owners who maintain and exert regulatory control, such as the definition of settings. Since we characterize the mobile phone as a possessional territory, we adapt the category of violation, defined as a temporary incursion where gaining control is not necessarily the goal as a likely and appropriate category of infringement in this context.[3] Also propose that bluejackers are attempting to personalize their experience of public space by engaging in the violation of others possessional territories through the act of illicit and anonymous messaging. Visitors to public spaces can engage in habitual behaviors at a specific location, such as picking a favorite parking spot that one can return to on each successive visit, to gain a sense of familiarity to locations that are frequently re-visited. These physical environments then hold enough significance to inspire defense among those who inhabit them and defensive behaviors, which can range from defining a personal space within a conversation or while using a tabletop work-surface. Typically, an inhabitant of a public place tends to personalize a location if he or she feels that the social conventions of a space allow one the license to mark a territory.

2.2 Bluejacking Technology

As know that 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. So bluejacking is based on Bluetooth technology which is explained bellow.[4]

Figure 2.2: Bluejacking technology

2.2.1 Bluetooth technology

Bluetooth Technology was developed to solve the simple problem of eliminating the connector cable. The idea is to replace the cables that are needed to accompany portable devices carried by many mobile travelers with a low-cost, secure, robust RF link. Originally Bluetooth marketed to small handheld devices such as cell phones and laptops. As the Bluetooth standard emerged successfully into society, the world demanded more. It is reported on Lets Go Digital in an article written by Ilse Jurrien that three new Bluetooth products are qualified every day and 10 million Bluetooth units are shipped per week. Bluetooth is so efficient, effective, and secure that even the IEEE approved the 802.15.1 Standard for Wireless Person Area Networks based on the Bluetooth specification.

What is Bluetooth?

Bluetooth is defined as a wireless technology that provides short-range communications intended to replace the cables connecting portable and/or fixed devices while maintaining high levels of security. There are three key features of Bluetooth; robustness, low power, and low cost. The Bluetooth standard provides a uniform structure enabling a wide variety of devices to seamlessly, and wirelessly, connect and communication with each other. Bluetooth devices connect and communicate via RF link through short-range piconets. Bluetooth devices have the ability to connect with up to seven devices per piconet. Each of these devices can also be simultaneously connected to other piconets. The piconet itself is established dynamically and automatically as Bluetooth enables devices enter and leave the range in which its radio operates. The major pro of Bluetooth is the ability to be full duplex and handle both data and voice transmission simultaneously. The differentiation of Bluetooth

from other wireless standards such as Wi-fi is that the Bluetooth standard gives both link layer and application layer definitions which support data and voice applications. Bluetooth comes in two core versions; Version 2.0 + Enhanced Data Rate and Version 1.2. The primary differences being Bluetooth 2.0 has a data rate of 3 Mega byte per second whereas Version 1.2 has only a 1 Mega byte per second data rate. Both are equipped with extended Synchronous Connections (eSCO), which improves voice quality of audio links by allowing retransmissions of corrupted packets.[5]

Figure 2.3: Bluetooth technology

Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. Bluetooth is modulated using adaptive frequency hopping (AFH). This modulation has the capability to reduce interference between wireless technologies sharing the ISM band. It does this by having the ability to detect other devices using the ISM band and use only frequencies that are free. The signal itself hops between ranges of 79 frequencies at 1 Megahertz intervals to minimize interference

2.2.2 Bluetooth Piconets

Lets say you have a typical modern living room with typical modern stuff inside. Theres an entertainment system with a stereo, a DVD player, a satellite TV receiver and a television; there's also a cordless telephone and a personal computer. Each of these systems uses Bluetooth, and each forms its own piconet to talk between the main unit and peripheral.

The cordless telephone has one Bluetooth transmitter in the base and another in the handset. The manufacturer has programmed each unit with an address that falls into a range of addresses it has established for a particular type of device. When the base is first turned on, it sends radio signals asking for a response from any units with an address in a particular range. Since the handset has an address in the range, it responds, and

a tiny network is formed. Now, even if one of these devices should receive a signal from another system, it will ignore it since its not from within the network. The computer and entertainment system go through similar routines, establishing networks among addresses in ranges established by manufacturers. Once the networks are established, the systems begin talking among themselves. Each piconet hops randomly through the available frequencies, so all of the piconets are completely separated from one another.[6]

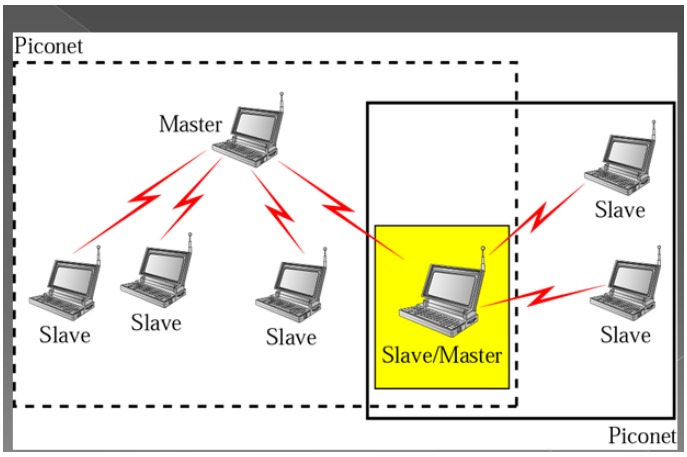

Figure 2.4: piconet

Now the living room has three separate networks established, each one made up of devices that know the address of transmitters it should listen to and the address of receivers it should talk to. Since each network is changing the frequency of its operation thousands of times a second, its unlikely that any two networks will be on the same frequency at the same time. If it turns out that they are, then the resulting confusion will only cover a tiny fraction of a second, and software designed to correct for such errors weeds out the confusing information and gets on with the networks business.

2.3 Related Concepts

The various concepts related to bluejacking are as follows:

2.3.1 Bluesnarfing

Snarfing is information theft or data manipulation in wireless, local networks (WLAN). The word snarf probably is a portmanteau from snort and scarf and derived as a rather malicious form of sniffing. It is also an extremely likely that the term was coined from cartoon characters in American pop-culture. In the US-American animated television series Thundercats (1980's) and Trollz (2000's) there are animated characters named "Snarf". In Thundercats lore, Snarf, an intelligent cat-like creature of the Snarf race, served as a loyal

sidekick (mascot) to Lion-O and the other ThunderCats. While a snarf is incapable of evil, their virtuous attributes were outweighed by their penchant for being nosey and annoying (hence, one who "snarfs" is nosey and annoying). In Trollz lore, The Snarf usually is a neat, small dog with a very sensitive tracking nose, but it can turn into a cureless hungry monster, which is able to overcome large obstacles for foraging. I.e. a dog-like creature that is a "malicious sniffer". Transferred to information technology, snarfing means that wireless devices are detected and then will be attacked by using vulnerabilities. The "Snarfer" can simulate an internet exchange point by a man-in-the-middle attack for example and gather information or data. Snarfing occurred firstly at Bluetooth devices where the term bluesnarfing is in use. Snarfing can be made difficult drastically with appropriate security measures at hard- and software. Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages and on some phones users can steal pictures and private videos. Currently available programs must allow connection and to be 'paired' to another phone to steal content. There may be other programs that can break into the phones without any control, but if they exist they are not made publicly available by the developer. One instance of Bluesnarfing software that was demonstrated (but never made available for download) utilized weaknesses in the Bluetooth connection of some phones.

2.3.2 Bluecasting

Although arguably neologism "bluecasting" is gradually gaining ground as a common term for the provision of any small digital media to suitable media provisioning enabled devices over Bluetooth via the OBEX protocol. Where by "small digital media" does not exclusively mean advertisements but could include photos, podcast style audio content, video, mobile ticketing, text messages, games (especially those written in J2ME) or even other applications. A bluecast is generally provisioned by a Bluetooth Kiosk a physical server provisioning the digital media over Bluetooth to interested devices. Bluetooth Kiosks are generally located in public spaces such as malls, bars or mass-transit terminals. In India there are some temples which offer ringtones, wallpapers of gods and some other content using bluecasting. Bluecasting is also used by many companies to advertise about various offers by them.

2.3.3 Bluebugging

Bluebugging is a form of Bluetooth attack. In progression of discovery date, Bluetooth attack started with bluejacking, then bluesnarfing, and then bluebugging. Bluebugging was discovered by German researcher Herfurt. His Bluebug program allows the user to take

control of a victim's phone to call the user's phone. This means that the Bluebug user can simply listen to any conversation his victim is having in real life. Initially, Bluebugging was carried out using laptops. With the advent of powerful PDAs and mobile devices, Bluebugging can now be carried out using these devices. Further developments of Bluebugging tools has allowed Bluebugging to "take control" of the victim's phone. Not only can they make calls, they can send messages, essentially do anything the phone can do. It should be noted that Bluebugging, like Bluesnarfing, is illegal in most countries.[7]

2.4 Summary

In this chapter the history and related work about the Bluejacking is related a where is developed over the Bluetooth-bluetooth enable devices such as an mobile, laptop, PDA'S,etc. The next section contains the methodology of the system.

Chapter 3

Methodology

In this chapter, It consist of architecture of bluejacking. In section 3.2 the working of the bluejack are discussed.In the working see how to bluejack via mobile, personal laptop's and the software tool in respectively section 3.2.1, 3.2.2 an so on.

3.1 Architecture

The Bluetooth architecture is divided into two specifications: the core and the profile specifications. The core specification discusses how the technology works while the profile specification focuses on how to build interoperating devices using the core technologies[7]

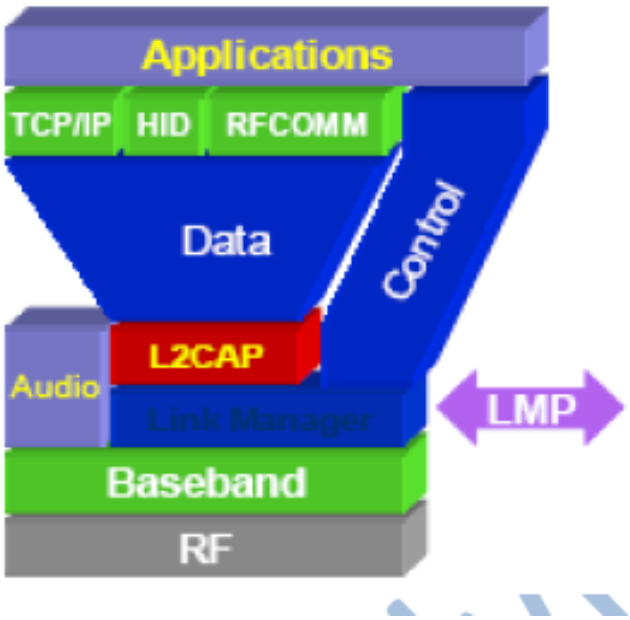

Figure 3.1: Architecture

- The RF Layer

The Bluetooth air interface is based on a nominal antenna power of 1mW (0dBm) with extensions for operating at up to 100 mW (20dBm) worldwide. The nominal link range is 10 centimeters to 10 meters, but can be extended to more than 100 meters by increasing the transmit power to 100 mW.

- The Bluetooth Baseband

The basic radio is a hybrid spread spectrum radio that operates in a frequency hopping manner in the ISM band. As stated earlier, the band is divided into 79 one Megahertz channels that the radio randomly hops through while transmitting and receiving data. A piconet is formed when one Bluetooth radio connects to another Bluetooth radio. Both radios then hope together throughout the 79 channels. The Bluetooth radio system supports a large 11 number of piconets by providing each piconet with its own set of random hoping patterns.

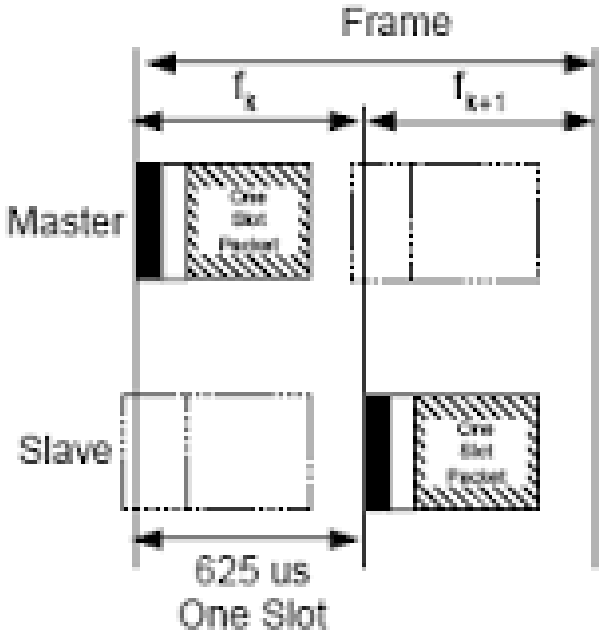

Figure 3.2: Bluetooth baseband

The Bluetooth frame consists of a transmit packet followed by a receive packet. Each packet can be composed of multiple slots (1, 3, or 5) of 625 us. Below is a single slot frame. Multi-slot frames allow higher data rates because of the elimination of the turn-around time between packets and the reduction in header overhead. The method which Bluetooth radios connect to each other in a piconet is fairly simple. IT is called a master/slave design. The master radio can be connected up to seven slave radios at any given time. Any Bluetooth radio can become a master or a slave radio. At the time of formation the piconet configuration is determined. Usually, the connecting radio will become the master, although, most devices have a "master/slave swap" function that allows the roles to be reversed. In order for

the piconet to be established by a Bluetooth Radio, the radio must have two parameters available, that is, the hopping pattern of the radio it is to be connected to and the phase within that pattern. All Bluetooth radios have a "Global ID" which is unique to the system. The master radio shares its Global ID with other radios. The other radios that receive the Global ID become slaves and provide all other radios with the correct hopping pattern. IT is the master who provides the clock offset with the slaves in the piconet, providing the offset into the hopping pattern.

3.2 Working

Try one at random and look around to see who grabs their phone and then looks perplexed when they read users message. If user want to name your Phone so it appears as a name in the list on a BlueJackers phone see how to name our phone. User can build a library of contacts with predefined messages.

3.2.1 HOW TO BLUEJACK

Assuming that now have a Bluetooth phone in your hands, the first thing to do is to make sure that Bluetooth is enabled. User will need to read the handbook of the particular phone (or PDA etc) that have but somewhere in the Menu item user will find the item that enables and disabled Bluetooth. Now, remember that Bluetooth only works over short distances, so if user are in the middle of Dartmoor then BlueJacking isn't going to work for user (unless the sheep have mobile phones these days!) so user need to find a crowd. BlueJacking is very new so not everyone will have a Bluetooth phone or PDA so the bigger the crowd the more likely user will have of finding a 'victim'. The Tube (yes, Bluetooth works underground), on the train, in a Cafe or standing in line are all good places to start.[8] User will now need to create a new Contact in user's Phone Book - however rather than putting someones name in the Name field you write your short message instead - so for example rather than creating a contact called Alan Philips user would write - "Hey, user have been BlueJacked!" instead (or whatever message user want to send) Now select the new contact and from the Menu of the phone choose "Send via Bluetooth". This is a facility available within the Mobile Phone that was designed to send a Contact to someone else - useful in Business when trading names and addresses, however we are now going to use it to send our message that was contained in the Name field of the contact - clever eh? User's phone or PDA will start to search the airwaves for other devices that within range. If user are lucky user will see a list of them appear, or it will say that it cannot find any. If the latter happens then relocate to another crowd or wait a while and try again. If user have a list of found devices then let the fun

begin. Unfortunately, almost every Bluetooth enabled device will not yet be configured with a useful name - so user are going to have to guess. Some devices will be called by their Phone manufacturer (e.g. Nokia, Sony) or maybe a random string. Try one at random and look around to see who grabs their phone and then looks perplexed when they read your message. If user want to name user's Phone so it appears as a name in the list on a BlueJackers phone see how to name our phone. User can build a library of contacts with predefined messages.

3.2.2 Mobile

The various steps involve in this are as follows:

- First press the 5-way joystick down.
- Then choose options.
- Then choose "New contact".
- Then in the first line choose your desired message.
- Then press done.
- Then go to the contact.
- Then press options.
- Then scroll down to send.
- Then choose "Via Bluetooth".
- Then the phone will be searching for enabled Devices.
- Then press "Select".

3.2.3 Personal computers/laptops

- Go to contacts in your Address Book program (e.g. Outlook)
- Create a new contact
- Enter the message into one of the 'name' fields
- Save the new contact
- Go to the address book
- Right-click on the message/contact

- Go to action
- Go to Send to Bluetooth
- Click on other
- Select a device from the list and double click on it

3.2.4 Software tools

The procedure for bluejacking as stated or explained earlier are very long and confusing. To avoid this we have developed some software to do bluejacking in an easier way. So by downloading that software on your personal computer or on your Bluetooth configured mobile phone user can do it directly by just searching the enabled Bluetooth device and send unsolicited messages to them. There are many software tools available in the market and there name is according to their use. Some of them are as follows:

- *Bluespam*

BlueSpam searches for all discoverable Bluetooth devices and sends a file to them (spams them) if they support OBEX. By default a small text will be send. To customize the message that should be send user need a palm with an SD/MMC card, then you create the directory /PALM/programs/BlueSpam/Send/ and put the file (any type of file will work .jpg is always fun) you would like to send into this directory. Activity is logged to /PALM/programs/BlueSpam/Log/log.txt. BlueSpam also supports backfire, if user put user's palm into discoverable and connectable mode, BlueSpam will intercept all connection attempts by other Bluetooth devices and starts sending a message back to the sender.

- *Meeting point*

Meeting point is the perfect tools to search for Bluetooth devices. User can set user's meeting point to a certain channel and meet up with people user have not met before. Combine it with any bluejacking tools and have lots of fun. This software is compatible with pocket PC, palm, Windows.

- *Freejack*

Freejack is compatible to java phone like Nokia N-series.

- *Easyjacking (eJack)*

Allows sending of text Messages to other Bluetooth enables devices.

- *Proximitymail*
- *Freejack*

3.3 Summary

In above chapter, see the architecture and working of bluejacking technology. Here, see the overall working of bluejacking how it's done via bluetooth technology. The next chapter, discuss about usage of bluejacking, code of ethics, etc.

Chapter 4

Discussion

In this chapter, in Section 4.1 the usage of bluejacking are discussed. The code of ethics about bluejacking are discussed in Section 4.2. In Section 4.3 the security issues related bluejack are discussed. The future aspects of bluejack are discuss in Section 4.4.

4.1 Usage Of Bluejacking

Bluejacking can be used in many fields and for various purposes. The main fields where the bluejacking is used are as follows:

- Busy shopping centre
- Starbucks
- Train Station
- High Street
- On a train/ tube/ bus
- Cinema
- Cafe/ restaurant/ pub
- Mobile phone shop
- Electronics shop (e.g. Dixons)

The main use of bluejacking tools or bluejacking is in advertising purpose and location based purpose. Advertising on mobile devices has large potential due to the very personal and intimate nature of the devices and high targeting possibilities. And introduce a novel B-MAD system for delivering permission-based location-aware mobile

advertisements to mobile phones using Bluetooth positioning and Wireless Application Protocol (WAP) Push. Present a thorough quantitative evaluation of the system in a laboratory environment and qualitative user evaluation in form of a field trial in the real environment of use. Experimental results show that the system provides a viable solution for realizing permission-based mobile advertising.

This Section discuss about Advantages pill camera. The next Section 8.2 discuss about Disadvantages and application.

4.2 Code Of Ethics

a) The 'bluejacker' is the individual carrying out the bluejack.
b) The 'victim' is the individual receiving the bluejack.
The various codes of ethics are as follows:

1. Bluejackers will only send messages/pictures. They will never try to 'hack' a device for the purpose of copying or modifying any files on any device or upload any executable files. By hacking a device you are committing 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 mobile devices including phones.

2. Any such messages or pictures sent will not be of an insulting, libelous or pornographic nature and will be copyright free or copyrighted by the sender. Any copyright protected images/sound files will only be sent with the written consent of the copyright holder.

3. If no interest is shown by the recipient after 2 messages the bluejacker will desist and move on.

4. The bluejacker will restrict their activity to 10 messages maximum unless in exceptional circumstances e.g. the continuous exchange of messages between bluejacker and victim where the victim is willing to participate, the last message being a final comment or parting sentiment (perhaps include www.bluejackq.com web address).

5. If the Bluejacker senses that he/she is causing distress rather than mirth to the recipient they will immediately deceases all activity towards them.

6. If a bluejacker is caught 'in the act' he/she will be as co-operative as possible and not hide any details of their activity (honesty is the best policy).

7. Social practices of bluejacking.

Conceptualized bluejacking as the bluejackers attempt to leave his or her mark on the recipients mobile phone through violation of possessional territory, which leads us to wonder if the bluejackers would want to leave an identifiable imprint, similar to the tag of a graffiti artist. Only a small percentage of bluejackers 4.7 persent multimedia files, such as a signature camera phone image or a theme song, suggesting that for most bluejackers, simply sending a largely anonymous text-only bluejack was sufficient to mark the recipients mobile phone. This lack of richer multimedia messages, when combined with the relatively large percentage of posts 23.4 percent that did not indicate message content type, implies that bluejackers place less value on a carefully crafted message.

4.3 Security Issue

As know that bluejacking is elated to Bluetooth therefore all the security issue related to Bluetooth are also related to bluejacking.

In Bluetooth, there are three security modes:

Security Mode 1 In this mode, the device does not implement any security procedures, and allows any other device to initiate connections with it.

Security Mode 2 In mode 2, security is enforced after the link is established, allowing higher level applications to run more flexible security policies.

Security Mode 3 In mode 3, security controls such as authentication and encryption are implemented at the Baseband level before the connection is established. In this mode, Bluetooth allows different security levels to be defined for devices and services.

It stated that the phonebook and calendar can be obtained, anonymously, and without the owner's knowledge or consent, from some Bluetooth-enabled mobile phones. It also claimed that the complete memory contents of some mobile phones can be accessed by a previously trusted paired (a direct connection accessed through a password) device that has since been removed from the trusted list. This data could include the phonebook, calendar, pictures and text messages.

4.4 Future Aspect

The Bluetooth positioning system needs to be made more reliable. To achieve this, the inquiry timeout should be made longer. This would make the positioning latency longer but more predictable. To shorten the latency the Bluetooth Sensor should not wait for the inquiry to time out before sending the device addresses of found devices but send them as soon as they

are discovered. Guessing user location based on his/her previous locations could be another possibility. Architecturally the Ad Server is not cohesive. If mapping device addresses to location information would be separated from the advertisement sending logic, Bluetooth positioning could be used with other location-aware applications as well. And plan to do this as incorporate Bluetooth positioning to the SmartRotuaari service platform. Advertisements should be profiled for each user. Possible profiling factors are gender, age, language, interests, mood, advertising frequency etc. The system could also learn user preferences by placing options like "more ads like this" and "less ads like this" in each advertisement. WAP Push is not the only possible advertisement content delivery channel. For example, the Bluetooth object exchange protocol could be used for that purpose, although it does not give the user the option to download and view the advertisements when he/she sees fit. However, in a heterogeneous mobile environment, multiple delivery channels should be considered. Also, in a mobile environment it is easier to take advantage of two-way communication, which should be thought of as well. The field trial provided evidence supporting favorable user acceptance. However, a much more extensive and longer lasting user study would be needed to provide real assessment of the acceptance of mobile advertisements. Further, a larger scale deployment would require a thorough validation of the underlying candidate business models.

4.5 Summary

In this chapter discussed the usage of bluejack, code of ethics, their security issues and future aspect. In the next chapter is conclusion.

Conclusion

Bluejacking is technique by which we can interact with new people and has ability to revolunerise market by sending advertisement about the product, enterprise etc. on the Bluetooth configured mobile phone so that the people get aware about them by seeing them on the phone. Now a day it is used in sale promotion or sale tools and in dating. This technique is used in many fields like cinema, train station, shopping malls, mobile phone shops etc. now a days there are new tools available in the markets by which bluejacking can be done. The basic technology behind bluejacking is similar to Bluetooth because we can do bluejacking in the mobile or PADs or computers or laptop configured with Bluetooth.

Bibliography

[1] BluejackQ. http://www.bluejackq.com/ [referenced 4 Aug 2016].

[2] Clemson H, Coulton P, Edwards R, Chehimi F (2006) Mobslinger: the fastest mobile in the west. In: 1st world conference for fun n games, Preston, UK, pp 4754, 2628 June 2006 (in press)

[3] Chehimi F, Coulton P, Edwards R (2006) Mobile advertising: practices, technologies and future potential. In: The 5th international conference on mobile business (ICMB 2006), Copenhagen, Denmark, 2627 June 2006

[4] T. Bunker. Serious Flaws in Bluetooth Security Lead to Disclosure of Personal Data, 2006. http: //www.thebunker.net/security/bluetooth.htm.

[5] Gifford, Ian, (January 2, 2007) IEEE Approves IEEE 802.15.1 Standard for Wireless Personal Area Networks Adapted from the Bluetooth Specification,

[6] Legg, Greg, (August 4, 2005) The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulneability.

[7] Bialoglowy, Marek, Bluetooth Security Review, Part 1, http://www.symantec.com/connect/articles/bluetooth-security-review-part-1 access date on 22 august 2016

[8] Fuller, John, How Bluetooth Surveillance Works, http://electronics.howstuffworks.com/bluetooth-surveillance1 access date on 22 august 2016.

[9] C.C. Chang.Pink Tentacle.The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulneability..updated on June 2013.

[10] Sidhu RR, McAlindon MEME, Sanders DSDS, Thomson MM. Bluetooth Faces Perception of Vulneability. Current Opinion in Pediatrics. March 2007.