A

Seminar report

On

"Bluejacking"

Submitted in partial fulfillment of the requirement for the award of degree
of Bachelor of Technology in Computer Science

SUBMITTED TO:
www.studymafia.org

SUBMITTED BY:
www.studymafia.org

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Preface

I have made this report file on the topic **Bluejacking**; I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to ……..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

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. 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 phone's contact interface, sends the message to the recipient, and remains in the vicinity to observe any reactions expressed by the recipient.

The messages tend to be anonymous since the recipient has no idea who has sent the bluejack, and the recipient has no information about the bluejacker, except for the name and model of the bluejacker's mobile phone. Because of Bluetooth's short-range networking capabilities, bluejacking can only occur between actors who are within 10 meters of each other, which makes this activity highly location-dependent. Contrary to what the name suggests, the bluejack recipient's phone is not hijacked; that is, the phone is at no time under the control of the bluejacker.

We 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.

We 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.

Bluejackers, however, ignore the conflict between the control exerted by the bluejacker and the lack of defensive measures that can be taken by the recipient when his or her possessional territory is violated. To gain a further understanding of why bluejackers would engage in a practice that disrupts the social conventions of public space, we ask the following research questions:

1. What are the characteristics of the public spaces in which bluejacking occurs?
2. What are the alternative social conventions that might arise from the practice of bluejacking?
3. What implications does this appropriation have for the design of mobile social systems?

1.1 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 cellphone 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.

2. BLUEJACKING TECHNOLOGY

As we 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.

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.

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.

The devices themselves are categorized into range ability. There are three classes of devices each covering a select range. Class 1 devices are mostly used in industrial cases and have a range of 100 to 300 meters. These devices take more power than the standard devices you and I are accustomed to in our daily routine and therefore are a bit more expensive. Class 2 devices are most commonly found in mobile devices and the most commonly used. Items such as cell phones and printers are Class 2 devices and have a range of 10 to 30 feet and use only 2.5 milli-Watts of power. Finally, Class 3 devices have the shortest range of up to 1 meter and include devices such as keyboards and a computer mouse. Class three devices therefore require the least amount of power and are in general the lease expensive.

Class	Maximum Permitted Power (mW)	Maximum Permitted Power (dBm)	Range (approximate)
Class 1	100 mW	20 dBm	~100 meters

Class 2	2.5 mW	4 dBm	~10 meters
Class 3	1 mW	0 dBm	~1 meter

2.1.1 Bluetooth Piconets

Let's say you have a typical modern living room with typical modern stuff inside. There's 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 it's 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.

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, it's 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 network's business.

2.1.2 The Bluetooth 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.

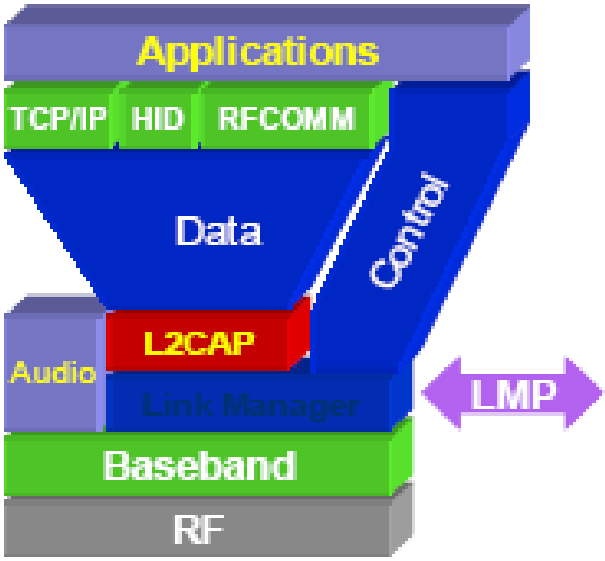

Figure 1:

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

number of piconets by providing each piconet with its own set of random hoping patterns.

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.

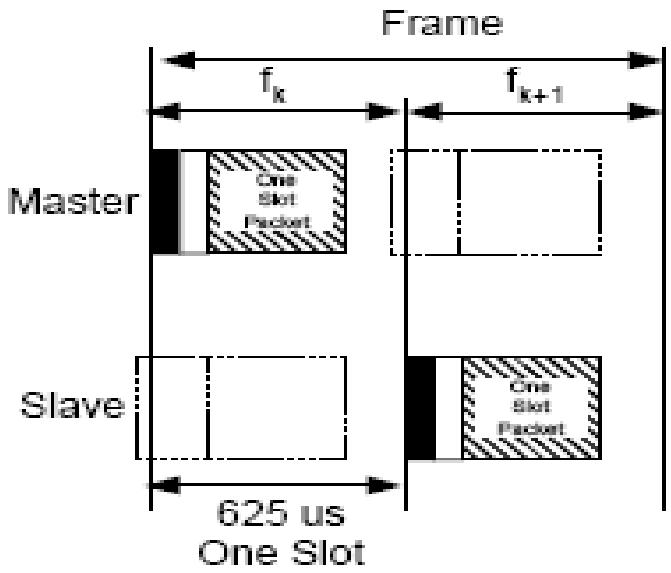

Figure 2:

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.

Usually, radios not connected to the piconet are in stand-by mode. While in stand-by mode, radios are listen for other radios to find them, which is called Inquiring, and are listening for a request to from a piconet, which is called Paging. In the event a radio issues an Inquire command, a listening radio will respond with an FHS packet that includes the devices Global ID and clock offset to give the inquiring radio at list of available Bluetooth radios within the local range.

A Bluetooth radio will page another radio with its Global ID to form a piconet. The radio that was paged will respond with its Global ID and the master radio will pass the radio that was paged and FHS packet. The radio that was paged loads the paging radio's Global ID and clock offset in order to join then master's piconet.

2.2 vCard file format

vCard is a file format standard for electronic business cards. vCards are often attached to e-mail messages, but can be exchanged in other ways, such as on the World Wide Web. They can contain name and address information, phone numbers, URLs, logos, photographs, and even audio clips.

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.

vCard is accompanied by a proposed standard for exchanging data about forthcoming appointments called vCalendar since superseded by iCalendar; the Internet Mail Consortium has issued a statement that it "hopes that all vCalendar developers take advantage of these new open standards and make their software compatible with both vCalendar 1.0 and iCalendar."

The following is an example of a VCard file containing information for one person:

BEGIN:VCARD
VERSION:2.1
N:Gump;Forrest
FN:Forrest Gump

ORG:Bubba Gump Shrimp Co.
TITLE:Shrimp Man
TEL;WORK;VOICE:(111) 555-1212
TEL;HOME;VOICE:(404) 555-1212
ADR;WORK:;;100 Waters Edge;Baytown;LA;30314;United States of America
LABEL;WORK;ENCODING=QUOTED-PRINTABLE:100 Waters Edge=0D=0ABaytown, LA 30314=0D=0AUnited States of America
ADR;HOME:;;42 Plantation St.;Baytown;LA;30314;United States of America
LABEL;HOME;ENCODING=QUOTED-PRINTABLE:42 Plantation St.=0D=0ABaytown, LA 30314=0D=0AUnited States of America
EMAIL;PREF;INTERNET:forrestgump@walladalla.com
REV:20080424T195243Z
END:VCARD

vCard defines the following property types: FN, N, NICKNAME, PHOTO, BDAY, ADR, LABEL, TEL, EMAIL, MAILER, TZ, GEO, TITLE, ROLE, LOGO, AGENT, ORG, CATEGORIES, NOTE, PRODID, REV, SORT-STRING, SOUND, URL, UID, VERSION, CLASS, and KEY .

vCard supports private extensions, with a "X-" prefix, a number of which are in common usage.

Some of these include:

Extension	**Used As**	**Data**	**Semantic**
extensions supported by multiple different programs			
X-ANNIVERSARY	property	YYYY-MM-DD	arbitrary anniversary, in addition to BDAY = birthday
X-ASSISTANT	property	string	assistant name (instead of Agent)
X-MANAGER	property	string	manager name
X-SPOUSE	property	string	spouse name

X-AIM	property	string	Instant Messaging (IM) contact information; TYPE parameter as for TEL (I.e. WORK/HOME/OTHER)
X-ICQ	property	string	"
X-JABBER	property	string	"
X-MSN	property	string	"
X-YAHOO	property	string	"
X-GADUGADU	property	string	"
X-GROUPWISE	property	string	"

introduced and used by Mozilla, also used by Evolution (software)

X-MOZILLA-HTML	property	TRUE/FALSE	mail recipient wants HTML email

introduced and used by Evolution (software)

X-EVOLUTION-ANNIVERSARY	property	YYYY-MM-DD	arbitrary anniversary, in addition to BDAY = birthday
X-EVOLUTION-ASSISTANT	property	string	assistant name (instead of Agent)
X-EVOLUTION-BLOG-URL	property	string/URL	blog URL
X-EVOLUTION-FILE-AS	property	string	file under different name (in addition to N = name components and FN = full name
X-EVOLUTION-MANAGER	property	string	manager name

X-EVOLUTION-SPOUSE	property	string	spouse name
X-EVOLUTION-VIDEO-URL	property	string/URL	video chat address
X-EVOLUTION-CALLBACK	TEL TYPE parameter value	-	callback phone number
X-EVOLUTION-RADIO	TEL TYPE parameter value	-	radio contact information
X-EVOLUTION-TELEX	TEL TYPE parameter value	-	Telegraphy#Telex contact information
X-EVOLUTION-TTYTDD	TEL TYPE parameter value	-	TTY (?) contact information

3. HOW TO BLUEJACK

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

Now, remember that Bluetooth only works over short distances, so if you are in the middle of Dartmoor then BlueJacking isn't going to work for you (unless the sheep have mobile phones these days!) so you 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 you 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.

You will now need to create a new Contact in your Phone Book - however rather than putting someone's name in the Name field you write your short message instead - so for example rather than creating a contact called Alan Philips you would write - "Hey, you have been BlueJacked!" instead (or whatever message you 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?

Your phone or PDA will start to search the airwaves for other devices that within range. If you are lucky you 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 you 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 you 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 you want to name your Phone so it appears as a name in the list on a BlueJackers phone see how to name our phone .You can build a library of contacts with predefined messages.

3.1 Mobile

The various steps involve in this are as follows:

1. First press the 5-way joystick down.

2. Then choose options.

3. Then choose "New contact"

4. Then in the first line choose your desired message.

5. Then press done.

6. Then go to the contact.

7. Then press options.

8. Then scroll down to send.

9. Then choose "Via Bluetooth"

10. Then the phone will be searching for enabled Devices.

11. Then press "Select"

3.2 Personal computers/laptops

1. Go to contacts in your Address Book program (e.g. Outlook)

2. Create a new contact

3. Enter the message into one of the 'name' fields

4. Save the new contact

5. Go to the address book

6. Right-click on the message/contact

7. Go to action

8. Go to Send to Bluetooth

9. Click on other

10. Select a device from the list and double click on it

3.3 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 you 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:

3.3.1 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 you 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 you put your 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.

3.3.2. Meeting point

Meeting point is the perfect tools to search for Bluetooth devices. You can set your meeting point to a certain channel and meet up with people you've not met before. Combine it with

any bluejacking tools and have lots of fun. This software is compatible with pocket PC, palm, Windows.

3.3.3 Freejack

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

3.3.4. Easyjacking (eJack)

Allows sending of text Messages to other Bluetooth enables devices.

3.3.5. Proximitymail

3.3.6. Freejack

4. 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

- Café/ 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. We 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. We 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.

4.1 Bluetooth location based system

In terms of location proximity detection for mobile phone users the obvious choice is Bluetooth which, despite previous predictions of its demise, is in fact increasing its growth and Nokia is predicting a year-on year increase of 65% in 2006. There are already a small number of mobile Bluetooth proximity applications in existence which are often described as mobile social software (MoSoSo) and can be viewed as evolutions of Bluejacking. Bluejacking was/is a phenomenon where people exploit the contacts feature on their mobile phone to send messages to other Bluetooth enabled devices in their proximity. Bluejacking evolved into dedicated software applications such as Mobiluck and Nokia Sensor which provided a simpler interface, and in the case of Nokia Sensor, individual profiles could be used to initiate a social introduction. In terms of this particular application it could be regarded as a business orientated application of the Bluejacking phenomenon.

Consumers are becoming increasingly aware of the use and benefits of Bluetooth as demonstrated in the widespread use of Bluetooth dongles through which the users can connect their desktop machines to these devices. Other initiatives for Bluetooth have been seen in the automotive and medical industries in that manufactures have begun to include Bluetooth access in cars and medical monitoring equipment. According to analysts [11], Bluetooth is currently present in 65% of all mobile phone handsets thus making a system such as the one described in this paper, a very practical and worthwhile scenario.

This location based system enables Bluetooth to be used as a means of targeting users with specialized content in a specific area at a given time. For example, users in a supermarket could be informed about a certain discount offer based upon their purchasing habits. Such messages can be sent to all the users in the area with a Bluetooth enabled mobile handset or PDA. In order that the system can service a diverse range of users and devices no client side application is required thus nothing has to be installed. The information is presented in a very familiar and simple form of a text message. Figure 3 shows the basic layout of a system for transmitting messages to all the devices in a given area.

The system uses object exchange protocol (OBEX) over Bluetooth to send the information to target devices. Licensed by Bluetooth SIG from IrDA, OBEX has become even more popular than during its original period as means of transferring business details. OBEX is transport neutral, as with the hypertext transfer protocol (HTTP), which means that it can work over

almost any other transport layer protocol. OBEX is defined as one of the protocols in Bluetooth and sits over RS232 serial cable emulation (RFCOMM) protocol. Moreover, OBEX is a structured protocol which provides the functionality to separate data and data attributes. A clear definition of each request can be given which helps distinguish one request from another. Use of other protocols such as RFCOMM or logical link control and adaptation protocol (L2CAP) require the applications sending and receiving information to know how the data is sent and when to send the reply. Like extensible markup language (XML) OBEX provides structure to the data being sent in contrast to other protocols such as RFCOMM which basically send bytes.

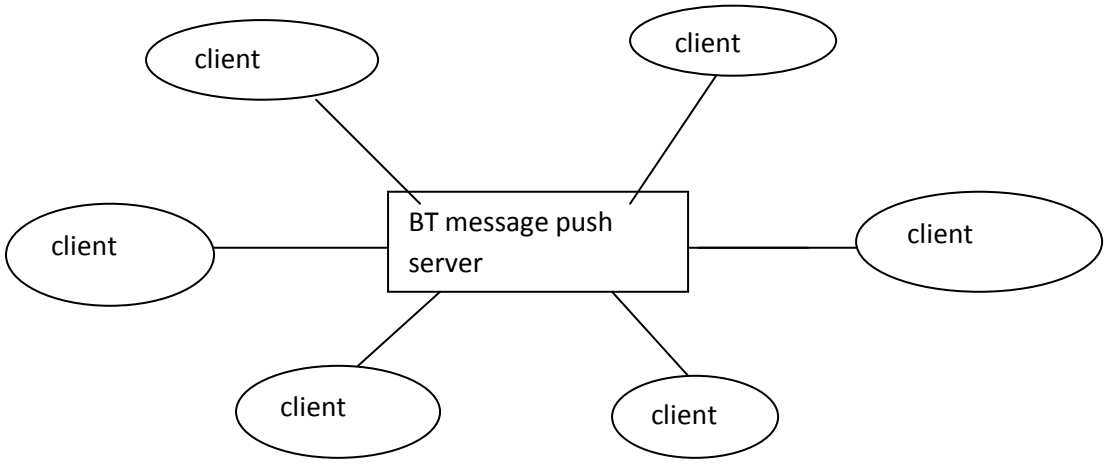

Figure3. Basic Bluetooth message system

4.2 Bluejacking as a market channel

Bluetooth offers a new communications channel to marketers. But the technology needs to be respected if they are to avoid alienating consumers according to a white paper from Rainier PR. Stephen Waddington, managing director of Rainier PR, turns wireless sleuth. The marketing industry is never slow to jump on a new communication channel and exploit it for its own ends. The telephone, email, SMS text messaging and the web have all become a standard part of the marketing toolkit, the latter having a marked impact on the way in which organizations communicate with their audiences.

Now there is a new mobile communication platform called Bluetooth and both the marketing and technology community are debating whether it offers a new opportunity to be exploited for marketing gain.

4.3 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. 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

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 café or pub

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 consumer's 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. Herein lies one of the key benefits of Bluetooth. Unlike any

other mobile communication mechanism it is absolutely free – there are no subscription charges and no costs associated with sending a message.

“The rise in text-based bluejacking couldn’t have been more timely for TagText’s launch. Not only can we capitalize on the trend, but using images adds a new dimension that even most bluejackers haven’t yet considered,” said Russell Buckley, director and founder of TagText.

Buckley admits that Bluejacking would not suit everyone, but for brands that want bleeding edge youth credibility, it’s certainly worth considering. “If you don’t shy away from other forms of guerrilla marketing like fly posting or giant image projection, you may want to think about this new medium,” he said.

5. 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 & 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

Other forms of message content included social interaction (19.4%) types of statements (Figure 3). This suggests that while bluejackers engage in this illicit messaging, they use social pleasantries to follow the conventions of acceptable small talk occasionally made by strangers in public places. Bluejackers often wanted to "spread the word" about bluejacking; 16.6% of the messages referred to the practice of bluejacking. They characterized this bluejacking-referential message type as a way to familiarize recipients about bluejacking in the hopes that those who received a bluejack would visit the Bluejackq website and eventually be inclined to try bluejacking in the future. The evangelical tone adopted by bluejackers suggests that they perceive this practice positively. We were interested in whether bluejackers engaged in harmful behavior through malicious message content, despite their framing of bluejacking as merely for fun. While bluejackers do not deny that there are prank-like aspects to their activities, there does seem to be a regulatory spirit among the posters on Bluejackq. As part of the "Guides and Facts" section of the site, the board moderators have posted a code of ethics, which include provisions that discourage the sending of executable files, libelous or pornographic pictures, and excessive messages. This explicit set of rules may explain the relative lack (2.7%) of malicious message content sent, which we defined as those banned by the Bluejackq code of ethics. It may, however, also be the case that those who do send malicious messages do not report them on Bluejackq for fear of censure by the community of posters.

We conceptualized bluejacking as the bluejacker's attempt to leave his or her mark on the recipient's 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%) sent 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 recipient's mobile phone. This lack of richer multimedia messages, when combined with the relatively large percentage of posts (23.4%) that did not indicate message content type, implies that bluejackers place less value on a carefully crafted message. The act itself and the description of the location in which the bluejack took place are the noteworthy portions of the practice when bluejackers share their stories of bluejacking.

6. RELATED CONCEPTS

The various concepts related to bluejacking are as follows:

6.1 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.

This weakness has since been patched by the Bluetooth standard. There seems to be no available reports of phones being Bluesnarfed without pairing, since the patching of the Bluetooth standard.

Bluesnarfing is much more serious in relation to Bluejacking, but both exploit others' Bluetooth connections without their knowledge. Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) may be susceptible to Bluejacking, and possibly to Bluesnarfing when and if Bluesnarfing of the current Bluetooth security becomes possible. By turning off this feature, the potential victim can be safer from the possibility of being Bluesnarfed; although a device that is set to "hidden" may be Bluesnarfable by guessing the device's MAC address via brute force. However, this is difficult because Bluetooth uses a 48-bit unique MAC Address, so there are over 280 trillion possible addresses to guess (although the first 24 bits are common to a manufacturer which, so only 24 bits need be guessed). Because Bluesnarfing is an invasion of privacy, it is illegal in many countries.

It is important not to confuse Bluesnarfing with Bluejacking. While Bluejacking is essentially harmless and does not result in the exposure of any data in the victim's handset, Bluesnarfing is the stealing of information from the victim's Bluetooth device.

6.2 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.

6.3 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. SECURITY ISSUE

As we 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.

Concerns about bluejacking were raised earlier this month when security firm AL Digital published a report that suggested there are a number of security problems with Bluetooth devices.

"Bluejacking promotes an environment that puts consumer devices at greater risk because of serious flaws in the authentication and/or data transfer mechanisms on some Bluetooth-enabled devices," it said.

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.

However, the report was later questioned in an article published on The Register, in which TDK Systems MD Nick Hunn said the research posed little cause for concern.

Hunn said the report was incorrect because in order for information to be duplicated, the devices would have to be paired. Bluejacking does not, as the report stated, require a password to be entered and therefore the two devices are not paired, he explained.

He said bluejacking doesn't hijack the phone or harvest information, but simply presents a message, which the recipient can delete, ignore or read.

Ajack agrees. “Bluejacking is not a security risk as Bluetooth is secured by design and one does not pair the two devices in order to bluejack. While it can be a nuisance, one can easily switch the Bluetooth off to avoid getting bluejacked.”

Clickatell key sales consultant Gary Cousins says that while he hasn't heard of any cases of bluejacking happening locally, “with more and more cellphones having Bluetooth functionality, it's just a matter of time”.

A Jacking Attack or Bluejacking is similar to the Windows netsend spam issue when XP was first released. Instead of receiving anonymous messages over the Windows network, a Bluetooth receives anonymous wireless business cards. Though this doesn’t put any of the user’s data at risk, this attack has the potential of a denial of service attack.

Denial of Service Attacks of Bluetooth is similar to 802.11. This is when an attacker uses his/her device to repeatedly request “pairing” with the victim’s device. This will in turn not allow the Bluetooth user to connect or transmit successfully with another Bluetooth device. This attack also drains the victim’s battery.

7.1 Counters-Measures

Knowing of potential problems of jacking and denial of service attacks of Bluetooth is the first step. Knowing that these things can occur may help a user think twice in when and where it is best to use their device. It will also make them insure that information they do not wish to use over the air is insured to get to the potential receiver.

The best solution is to turn off your Bluetooth device until you need to communicate with another user. Since we know that software can turn on and off Bluetooth a device, disabling it and leaving it on is not your best bet. If you must keep the device on, than the idea of the E2X bag may be your best option explained below

> One of the problems with blue tooth is applications can choose to start receiving or transmitting anytime they wish. So an obvious countermeasure is software that takes all these applications and shields your phone, PDA, or other devices for transmitting or receiving when you do not want to. This type of software applications exist but cost a lot.

Another option is to buy an E2X bag. Place your device in this bag and it blocks all transmissions and receiving signals from leaving the bag. This allows people to leave their device on instead of turning it off when they feel it not safe to use.

"Since Bluetooth is a wireless technology, it is very difficult to avoid Bluetooth signals from leaking outside the desired boundaries. Therefore, one should follow the recommendation in the Bluetooth standard and refrain from entering the PIN into the Bluetooth device for pairing as much as possible. This reduces the risk of an attacker eavesdropping on the pairing process and finding the PIN used.

Most Bluetooth devices save the link key in non-volatile memory for future use. This way, when the same Bluetooth devices wish to communicate again, they use the stored link key. However, there is another mode of work, which requires entering the PIN into both devices every time they wish to communicate, even if they have already been paired before. This mode gives a false sense of security! Starting the pairing process every time increases the probability of an attacker eavesdropping on the messages transferred. We suggest not to use this mode of work.

Finally, the PIN length ranges from 8 to 128 bits. Most manufacturers use a 4 digit PIN and supply it with the device. Obviously, customers should demand the ability to use longer PINs."[2]

8. FUTURE ASPECTS

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. We plan to do this as we 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.

9. 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.

Now a day new and new techniques are developing using Bluetooth. Some of the latest news is :

Bluetooth Technology Now Standard in Cars ,BlueParrott Bluetooth B100 Wireless Headset ,Motorola & Burton Launch Bluetooth Snowjackets ,Bluetooth shipment units 3m a week ,O'Neil Launches 'The Hub' Bluetooth Snowboard Jacket ,CellStar Launches Bluetooth Web Surfer ,Emergence of new Bluetooth usage_models ,Heart Monitor Sends Crucial Information to Cell Phones ,Impulsesoft Delivers Stereo Music Over Bluetooth ,TDK Systems builds on the benefits of Bluetooth ,Impulsesoft Delivers Stereo Music Over Bluetooth .

So we conclude that in future this technology become the key for advertising and to interact with world and to get the location messages on the phone when you are somewhere out. Bluejacks are location specific. We first wanted to determine the types of places where bluejacks took place. The data indicate that bluejacking is an activity that primarily occurs in public spaces, outside of the home. Bluejacks frequently occurred in public transportation locales (23.4%), stores and shopping malls (32.1%) and restaurants (9.8%), bars (11.2%) and cafes (7.3%) but almost never at home (0.7%). This suggests that bluejackers are targeting strangers, presumably taking advantage of anonymity, opportunities for interaction and available Bluetooth enabled devices afforded by densely populated public spaces.There are few security issue which can be minimized by taking some simple precaution like when you do not want to be blue jacked just off your Bluetooth.

10. REFERENCES

1. BluejackQ. http://www.bluejackq.com/ [referenced 4 Nov 2003].

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 47–54, 26–28 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, 26–27 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”, *IEEE*, Retrieved on 10.02.06 from: http://standards.ieee.org/announcements/802151app.html

6. Legg, Greg, (August 4, 2005) “The Bluejacking, Bluesnarfing, Bluebugging Blues: Bluetooth Faces Perception of Vulneability”, *TechOnLine*, Retrieved on 10.01.06 from: www.techonline.com./community/tech_topic/bluetooth/38467