BLUEJACKING Technology

Srimathy R[1] Mr. Fahad Iqbal[2]
[2]Assistant Professor
[1,2]Department of Computer Science and Engineering
[1,2]Saveetha School of Engineering, Saveetha University, Thandalm, Chennai.

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 blue dating or blue chat) 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 user 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.
Keywords: Bluejacking, Bluetooth, bluejacker.

I. INTRODUCTION

A. BLUETOOTH

Bluetooth is a system for short-range wireless communication and is intended to allow devices within physical proximity of each other to communicate. As it is becoming universal among mobile devices, and as almost everybody has a mobile device, most people have a Bluetooth device in their possession most of the time. The prevalence of Bluetooth devices makes possible a wide range of applications, such as proximity-based location services [1], mobile commerce applications such as 'eWallets' [2], and even triggering face-to-face interactions that would not otherwise occur [3]. However, as has been the experience with Internet-based e-commerce [4], the development of such applications would be hindered by problems with the underlying Bluetooth communication medium. Security problems, either real or perceived, can be a significant barrier to new technologies as they contribute to people's reluctance to use such systems.

ATTACK	DESCRIPTON
Information theft	The most common form of this attack is known as BlueSnarfing. Examples of software to conduct these attacks are Bloover, which attacks phones supporting J2ME, and HeloMoto, which attacks some Motorola V-Series phones. Further, many attacks can be devised using the standard tools available in Linux.
Service Theft	Service theft Using the victim's device to access network services such as telephony or SMS. An example of this attack is the Mosquito virus, which sends SMS messages from the victim's device
Denial of Service	Deliberately consuming resources on the victim's device so as to prevent legitimate use. An example is the BlueSmack tool, which can immediately disable a range of Bluetooth devices.
BlueJacking	BlueJacking involves sending short, unsolicited messages to the target device. While not particularly serious, this attack could potentially be used to over-write information in the victim's phonebook. BlueJack is also the name of a tool commonly used to perform this kind of attack.
BluePrinting	BluePrinting Tools such as BlueStumbler, RedFang and BluePrint can be used to identify details such as the make, model and unique address of a Bluetooth device. While not an attack in itself, identifying these details can facilitate subsequent attacks of other types.
Bluebugging	BlueBugging In BlueBug attacks the attacker creates a serial connection to the victim's device without the need for authentication. The connection can subsequently be used to conduct information and service theft attacks. Many tools can be used to conduct this kind of attack, including Gnokii, a suite of open-source Bluetooth utilities.

B. BLUEJACKING TECHNOLOGY

Bluejacking is the sending of either a picture or a message from one user to an unsuspecting user through Bluetooth wireless technology. Common applications include short messages, *e.g.*, "You've just been bluejacked!" Bluejacking does not involve the removal or alteration of any data from the device.] Bluejacking can also

involve taking control of a mobile device wirelessly and phoning a premium rate line, owned by the bluejacker.

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.

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:

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

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.

C. 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.

D. MOBILE

The various steps follow are:-

- 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"

E. PERSONAL COMPUTER AND LAPTOPS

The various steps are:-
Go to contacts in your address book program (eg.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

II. SOFTWARE TOOLS

The procedural 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 earlier way. So by downloading that software on your 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 follow:

A. BLUESPAN

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.

B. MEETING POINT

Meeting point is the perfect tools to search for Bluetooth device. You can see your meeting point to a certain channel and met up with the people you have not met before. Combine it with any Bluejacking Tools and have a lot of fun. This software is compatible with pocket PC, Palm, Windows.

C. FREEJACK

Freejack is compatible to java phone like Nokia N-SERIES

D. EASYJACKING (eJack)

Allows sending of text Messages to other Bluetooth enable devices.

E. PROXIMITYMAIL

G. FREEJACK

III. 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.

A. 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.

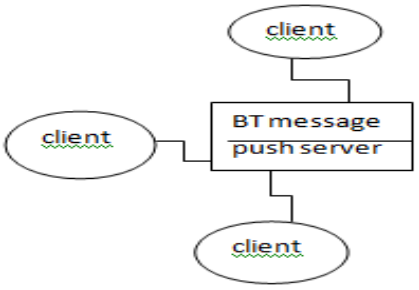

Fig. 3**:** Basic Bluetooth message system

B. 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.

IV. 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:

A. 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

B. 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

C. 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 Tag Text'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 Tag Text.

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.

V. 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:

- 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.
- 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.
- If no interest is shown by the recipient after 2 messages the bluejacker will desist and move on.
- 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).
- If the Bluejacker senses that he/she is causing distress rather than mirth to the recipient they will immediately deceases all activity towards them.

- 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).
- 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 Bluejacking for fear of censure by the community of posters.

VI. 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.

A jack 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."

Click a tell 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 net send 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.

VII. 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 using 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]

VIII. 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 , Impulse soft Delivers Stereo Music Over Bluetooth ,TDK Systems builds on the benefits of Bluetooth ,Impulse soft 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.

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
[7] Seminarsonly.com/computer science/Bluejacking.php

