Bluejacking Technology: Overview, Key Challenges and Initial Research

Ratika Bali

Department of Computer Science and Engineering
Guru Tegh Bahadur Institute of Technology
New Delhi, India

***Abstract*—The mobile phone technology has developed tremendously in the past forty years since its invention in 1973 owing to its unique, wiring sans and fixation free networked system. Mobile phones have been espoused as an everyday technology, omnipresent at every physical location. Initially used merely as a communicative device to facilitate a channel for mediated conversation, the usage of mobile phones has been diversified progressively. One such appropriation is bluejacking, the technique of relaying anonymous, unwanted and unsolicited short messages via vCard functionality over Bluetooth to Bluetooth-enabled devices using the OBEX (OBject EXchange) protocol. This paper provides an overview of the Bluejacking Technology.**

***Keywords*— Bluejacking, Bluejackaddict, Bluetooth Exchange, OBEX, vCard.**

I. Introduction

Bluejacking is an attack conducted on Bluetooth-compatible devices, such as smart phones, laptops and PDAs. Bluejacking is instigated by an attacker (termed as bluejacker or bluejackaddict) who forwards unsolicited messages to a user of Bluetooth-enabled device. When the connection goes through, the bluejacker tries to send a message to the recipient. The actual message sent to the user's device does not cause detriment, but is used to inveigle the user to counter react in some manner or add the new contact to the device's address book. [1] This message-transmitting attack resembles spam and phishing attacks conducted against email users. Bluejacking can be perceived as either infuriating or amusing, though it is relatively risk-free since the recipient has the option to decline. Bluejacking sure makes for an interesting wake-up call in close-knit environments like underground metro trains, buses, malls and cinemas.

II. History

Bluejacking was allegedly first conducted by a Malaysian IT consultant, 'Ajack' (his username a Sony Ericsson online forum), who used his Bluetooth-enabled phone to publicize Sony Ericsson. He also coined the name, which is an amalgam of Bluetooth and hijacking. While standing in a bank queue, Ajack turned on his Bluetooth, discovered a Nokia 7650 in the vicinity, created a new contact with 'Buy Ericsson!' as the first name, and sent that business card to the Nokia phone. The recipient of the Nokia phone standing a few feet away from him was startled to see such an 'advertisement'. Ajack posted this story on Sony Ericsson forum and other people started trying it out. Bluejacking has become a rage amid young people keen to play practical jokes. A 13-year-old girl named Ellie from Surrey, UK has created a website called 'bluejackq' where people can share their bluejacking experiences. [2]

III. Bluejacking Technology

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

A. Bluetooth Technology

1) *Bluetooth as a Wireless Technology:* Bluetooth, the latest development in wireless communications technology is a wireless standard that is designed for very short-range (less than 10 meters). It is a de facto standard, as well as a specification short range radio links. It is most appropriate for communication between computers or mobile devices and peripheral devices, such as to connect a wireless keyboard or mouse to a desktop PC, to send print jobs wirelessly from a portable PC to a printer, or to connect a mobile phone to an earpiece.
2) *Usage of Bluetooth:* Since Bluetooth devices automatically recognize each other when they get within transmission range, handheld/desktop PC's and mobile devices can always be networked wirelessly when they are within range. Bluetooth signals can transmit through clothing and other non-metallic objects, so a mobile phone or other device in a pocket or briefcase can connect with the user's Bluetooth headset, without having to be removed from the pocket or briefcase. Some

industry experts predict that major household appliances will be Bluetooth-enabled in the future, resulting in an automatic, always connected, smart home.

3) *Bluetooth Frequency Specification and Operating Principle:* Bluetooth works using radio signals in the frequency brand of 2.4GHz, the same as Wi-Fi, and supports data transfer rates of up to 3Mbps. Once two Bluetooth- enabled devices come within range of each other, their software identifies each other (using their unique identification numbers) and establishes a link. Because there may be many Bluetooth devices within the range, up to 10 individual Bluetooth networks (called Piconets) can be in place within the same physical area at one time. Each Piconet can connect up to eight devices, for maximum of 80 devices within any 10-meter radius.
4) *Bluetooth as Cable Replacement Technology:* Bluetooth is competent of transmitting voice, data, video and still images. It can be used to wirelessly synchronize and transfer data among devices and can be thought of as a cable replacement technology.
5) *Future Trends in Bluetooth Technology:* The Bluetooth Special Interest Group is an industry group consisting of leaders in the telecommunications, computing, and networking industries that are driving development of the technology and bringing it to market. [6]

B. OBEX Protocol

1) *OBEX as the heart of Bluetooth file transfer*: The heart of file transfer over Bluetooth is called Object Exchange, or OBEX protocol, a binary file transfer protocol run over not merely Bluetooth but also Infrared and even generic TCP/IP. The OpenOBEX project at http://openobex.sf.net/ offers the most ubiquitous open source implementations of the protocol.
2) *Usage of OBEX*: It is a session layer protocol designed to enable systems of various types to exchange data and commands in a resource-sensitive standardized fashion. The OBEX protocol is optimized for ad-hoc wireless links and can be used to exchange all sorts of objects, like files, pictures, calendar entries, and business cards. It also provides some tools to enable the objects to be recognized and handled intelligently on the receiving side.
3) *OBEX's operating functionality and resemblance to HTTP*: OBEX is designed to provide push and pull functionality in such a way that an application using OBEX does not need to get involved in managing physical connections. The application only takes an object and sends it to the other side in a "point-and-shoot" manner. This is similar to the role that HTTP serves in the Internet protocol suite, although HTTP is designed more for data retrieval, while OBEX is more evenly balanced for pushing and pulling data.
4) *Devices supported by OBEX*:
   i. All Palms since Palm III, except the Palm Pre, Palm Pre Plus, Palm Pixi and Palm Pixi Plus.
   ii. Most Sharp, Motorola, Samsung, Sony Ericsson, HTC and Nokia phones with infrared or Bluetooth port.
   iii. LG EnV Touch (VX11000).
   iv. Many other PDAs since 2003. [3]

C. vCard Functionality

1) *vCard as a Standard of Communication:* Address Book exchanges contact information with other programs primarily through vCards. vCard is short for virtual business card. More and more email programs send and receive these electronic business cards, which can be identified by their .vcf filename extensions.
2) *History:* The vCard standard has been around since 1996 and the current version, version 3.0, is specified by the IETF. The vCard or Versitcard was originally proposed in 1995 by the Versit consortium, which consisted of Apple Computer, AT&T Technologies (later Lucent), IBM and Siemens. In December 1996 ownership of the format was handed over to the Internet Mail Consortium, a trade association for companies with an interest in Internet e-mail. [4]
3) *vCard Features:*
   i. vCards are structured blocks of text data that provide what is more or less an electronic business card. The data can include name, address, telephone numbers (home, business, fax, pager, cellular, ISDN, voice, data, video), e-mail addresses and related internet URLs.
   ii. vCards can also include graphics and multimedia, including photographs, company logos, audio clips, along with geographic and time-zone information.
   iii. vCards are also designed to support multiple languages and are transport and operating system independent.
4) *Applications of vCards:*
   i. Infrared Exchange
   ii. Bluetooth Exchange
   iii. Internet Mail
   iv. Computer/Telephony Applications
   v. Video and data conferencing

IV. Process Of Bluejacking

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

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

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

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

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

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

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

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

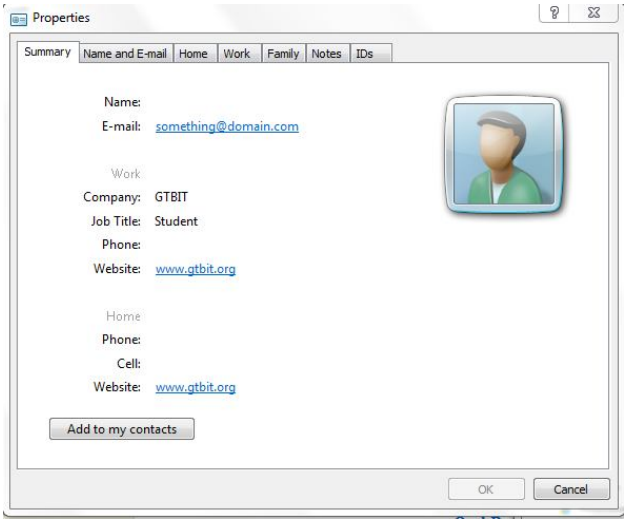


Fig. 1 vCard saved in .vcf format, viewed using 'Windows Contacts' application, shows various parameters along with 'Add to my contacts' option.

V. Bluejacking Tools

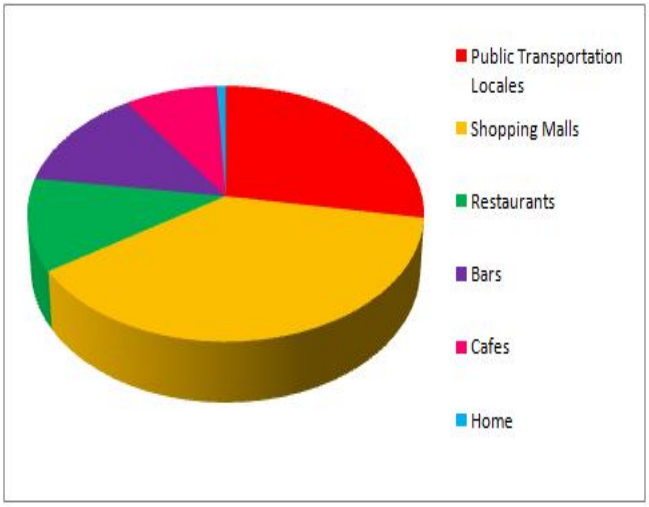
Bluetooth wireless technology has suffered some bad press and in particular has been associated with a new buzz word 'Bluejacking' which has emerged as a potential security issue due to its facilitation of unauthorized access to confidential information. The very phenomenon of Bluejacking has evidently exhibited that Bluetooth is amply vulnerable to attacks. Furthermore, the availability and continuous development of bluejacking tool intensifies the Bluetooth security paradigm. Some of the prime bluejacking tools are:

1) *RedFang:* A small proof-of-concept application used to find undiscoverable Bluetooth devices.
2) *Bluesniff:* A proof-of-concept tool for a Bluetooth wardriving.
3) *Meetingpoint*: Meeting point is the perfect tool to search for Bluetooth devices. One can set the meeting point to a certain channel and combine it with any bluejacking tool. This software is compatible with pocket PC, palm, Windows.
4) *Freejack*: Freejack is compatible with java phones like Nokia N-series.
5) *Btscanner:* A Bluetooth scanning program that can perform inquiry and brute-force scans, identify Bluetooth devices that are within range, and export the scan results to a text file and sort the findings.
6) *BlueBug:* A tool that exploits a Bluetooth security loophole on some Bluetooth-enabled cell phones. It allows the unauthorized downloading of phone books and call lists, and the sending and reading of SMS messages from the attacked phone.

VI. Applications Of Bluejacking

The insecure "discoverable" mode of Bluetooth provides a vehicle for bluejacking propagation. Amongst the various diversified applications of bluejacking, its use is in advertising domain is significantly popular. Advertising on mobile devices has a momentous potential due to the intimate nature of the devices and the high targeting likelihood. It is an endorsement communiqué conduit.

1) *Viral interaction:* Bluejacking can be utilized to exploit the communication paradigm between consumers and producers to share content such as text, images, videos and Internet references. Certain brands have already created multimedia content that has very rapidly been circulated around using bluejacking technology. Thus, bluejacking has replaced the conventional advertising via standardized broadcasting medium.
2) *Community Activities:* Social Networking or gaming events can be facilitated using Bluetooth as a channel for potential participants to converse.



The anonymous nature of bluejacking makes is a

splendid physiological instrument for interaction between individuals in a close-knit environment such as a café.

Fig. 3 Go to Contacts Option

Fig. 4 Choose 'New Contact' Option

Fig. 5 Create a new contact with 'You Are Bluejacked' as the name

Fig. 6 Contact with name field 'You Are Bluejacked' has been created. Choosing 'Share Contact' -> 'Via Bluetooth' -> message will trasmit to victim's mobile

Fig. 7 After discovering active Bluetooth devices, the victim's device can be bluejacked easily.

VII.

VII. Related Concepts

1) *Bluebugging*: A bluebug susceptibility authorizes admission to the mobile phone's set of AT commands, which facilitate an attacker utilize the phone's service, including placing outgoing calls, sending, receiving/deleting text, diverting calls, and so on.
2) *Bluebump Attack*: This attack seizes benefit of a flaw in the managing of Bluetooth link keys, granting devices that are no longer sanctioned the capability to exploit services as if still paired. It can pilot to the situation of data larceny or to the mistreatment of mobile Internet connectivity services such as Wireless Application Protocol and General Packet Radio Services.
3) *HelloMoto Attack*: This attack is amalgamation of the bluesnarf attacks and bluebug attacks. The name originates from the piece of evidence that it was formerly discovered on Motorola mobile phones.
4) *Bluedump Attack*: This attack prompts a Bluetooth device to abandon its amassed link key, generating an opening for key- swapping sniffing or for an additional pairing to take place with the attacker's device of preference.
5) *Bluechop Attack*: This is DoS attack that can interrupt any recognized Bluetooth network (Piconets) via a device that is not involved in it, if the Piconets master sustains numerous associations.

VIII. Conclusion

Bluetooth is a great technology with many useful applications. At the same time, variety of Bluetooth hacking tools and techniques are available, Bluejacking being the most vulnerable of the lot, which makes it a little riskier to use this technology. Bluetooth is not going to go away because of a few security flaws; instead it can be secure if configured properly and used carefully with a proper understanding of this wonderful technology.

Best practices to mitigate the Bluejacking threats against the Bluetooth are: user awareness, disable device when not in use, use an unidentifiable device name, employ security mode 3 or 4, disable unused services and profiles, set device to non-discoverable mode when not in use, use non-guessable PIN codes of at least 12 or more alphanumeric characters and perform pairing only when absolutely required. [6][7]

Many users take privacy for granted. Unfortunately, the Bluetooth system wasn't intended for confidential purposes. Although improvement in the domain of Bluetooth security

has been made, one should never assume that information being sent using a Bluetooth connection is private. Attachments, if sensitive, should be encrypted before they are sent across.

Bluejacking first showed up in popular use in 2003 or so when Bluetooth devices gained popularity. It has hitherto been used for advertising purposes by vendors. It is the modus operandi by which we can network with new people and has the ability to revolutionize market by propelling advertisements about the products, services, enterprises, etc. on the Bluetooth-configured devices.

Bluejacking is more of a prank than an attack, and unquestionably an annoying one at that, but at the same moment its future prospects in the field of advertising and marketing are vividly dazzling.

REFERENCES

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