BlueJacking

Pimal Khanpara¹, Param Khanpara²
Dept. of Computer Science and Engineering, Nirma University, Ahmedabad, Gujarat, India - 382 481.

Abstract— Bluetooth technology is designed and optimized for use in mobile devices such as mobile computers, cellular handsets, network access points, printers, PDAs, desktops, keyboards, joysticks and virtually any other device. The Bluetooth protocol uses a combination of circuit and packet switching to send/receive data. The Bluetooth Protocol Architecture includes radio, baseband, link manager, logical link control and adaptation (L2CAP), Host Controller Interface (HCI), TCP, SDP, RFCOMM and application layers. Bluetooth technology has grown through the years, but because of the increase, security has become an issue. There are different vulnerabilities in the design already, which have been maliciously exploited. One of these exploits is Bluejacking. Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phone, 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. Various software tools are available for Bluejacking. Bluejacking can be used for sending business cards, as a marketing channel, as a medium for performing community activities and providing location based services. There are some codes of ethics which need to be followed by an ethical bluejacker. This paper studies all the concepts and issues related to Bluejacking.

Index Terms— Bluetooth, Bluejacking

INTRODUCTION
In the world of modern communication, devices like laptops, mobile phones and PDAs are equipped with the facility of sending messages through transceivers using the Bluetooth protocol. The Bluetooth protocol enables the wireless devices to send messages over short distances. Using Bluetooth people can exchange their electronic business cards in the vCards format.

Bluejacking is a technique that works on Bluetooth enabled devices. In this technique, unsolicited messages are sent from one device to another providing that both devices are Bluetooth enabled. People mostly send such unsolicited messages in form of vCards.

Bluejacking is completely based on the Bluetooth technology. Bluetooth protocol can work within a very limited range usually around 10 meters for mobile devices and up to 100 meters for laptop computers. As Bluejacking is based on Bluetooth technology, to carry out Bluejacking, the sending and receiving devices need to be within 10 meters of one another if Bluejacking is done using mobile phones. If laptops are used for this purpose then the distance between such devices must be 100 meters or less.

Bluejacking is usually a harmless phenomenon but it is often associated with hijacking or hacking because bluejacked people generally don’t know what has happened to their phones. In fact, a bluejacker only sends a text message. In any case, the bluejacker cannot control or hack the recipients’ device. Bluejacking is just meant to be a harmless prank with the intention of evoking a response of bewilderment on the face of the person whose device is bluejacked. Applications of bluejacking are mainly found in the marketing field.

Bluejacking was reportedly started by a Malaysian IT consultant who used his phone to advertise Sony Ericsson [6]. He also gave the name “Bluejacking” to this technique, as it is based on Bluetooth technology and Jacking—the act of taking over something, a shortening of hijack.
BLUETOOTH

Bluetooth [4] is based on the wireless LAN technology in which short range radio links are used for data communication between two wireless devices. A Bluetooth LAN network is an ad hoc network that works on IEEE 802.15 standard. In such a network, the devices which are in each other’s range form a network called Piconet. It operates in short range distances of 10 to 100 meters and uses frequency hop spread spectrum. Because of the attracting features of Bluetooth, like low cost and low power, Bluetooth technology has become very popular. Bluetooth technology can work at either physical level or at protocol level. At physical level, it uses radio frequency standard. While at the protocol level, there must be some agreement on number of bits to be sent, time at which bits are to be sent and message integrity.

Bluetooth can form two types of networks: Scatternet and Piconet.

i) Piconet [8]:
A Bluetooth network is called piconet or small net. A piconet can be formed by maximum 8 stations out of which one station acts as a primary or master station and others act as secondary or slave stations. A piconet can have only a single primary station. The primary station decides the frequency hopping sequence and time slots for the device. It initiates the communication which can be continued either in one to one or in one to many manners between the primary and secondary devices. All the slave devices have to synchronize their clocks and hopping sequence with the master device. In a piconet, each Bluetooth device has a unique 48 bit hard wired device address for identity which allows for 248 devices. The master searches for Bluetooth devices or accepts the invitations to join the piconet addressed to specific devices. Then the primary device assigns a member address to each secondary device. The piconet can have an additional 8th slave device if it is in the parked state. A slave device in the parked state is synchronized with the master device but it can take part in the communication only when it moves from parked state to active state. At a time only 8 devices can be in active state so to activate a device from the parked state, an active device have to go to the parked state.

ii) Scatternet [9]:
Piconets can be combined to form a scatternet. A secondary device in one piconet can be the primary in another piconet. This station can receive messages from the primary of the first piconet and acting as a primary can deliver messages to the secondary devices in the second piconet.

BLUETOOTH LAYERS

Each layer of Bluetooth implements a different protocol to establish a communication link for data transfer between devices that support Bluetooth stack. The following figure shows the Bluetooth layered architecture [4]:

The protocols implemented by this architecture are divided into three groups:
i) Transport Protocol Group
ii) Middleware Protocol Group
iii) Application Protocol Group

1. Transport Protocol Group [5]:
Using transport protocol group Bluetooth devices can locate each other. The protocols defined in this group are different from the protocols defined in the Transport layer of OSI reference model. The transport protocol group defines the protocols which correspond to Physical and Data link layers of OSI model. The transport protocol group includes the Radio, Baseband, Link Manager, Logical Link Control and Adaption layers and the Host Controller Interface. Both synchronous and asynchronous transmissions are supported by these protocols.

a) Radio Layer:
The radio layer specifies the design of the Bluetooth transceivers. It has the coincidence with the physical layer of OSI model. Bluetooth devices use a 2.4 GHz ISM band. To avoid interference from other devices or other networks, Bluetooth uses frequency hopping spread spectrum in the radio layer. Bluetooth uses Gaussian Bandwidth Filtering Frequency Shift Keying method to transform the bits to signal.

b) Baseband Layer:
This layer defines how Bluetooth devices search for and connects to other devices and assigns the roles of primary and secondary devices. The devices use a time division duplexing (TDD), packet-based polling scheme to share the air-interface. The master and slave each communicate only in their pre-assigned time slots. Types of packets, error detection and correction methods, encryption techniques, packet processing methods and packet transmission and retransmission procedures are also defined in this layer. The Baseband layer supports two types of links: Synchronous Connection-Oriented (SCO) and Asynchronous Connection-Less (ACL).
SCO links are mainly used for fast transmissions which require minimum latency and are characterized by periodic packet assignment. A physical connection is created between the master and slave device by reserving specific slots at regular time intervals. No retransmission occurs if packet is damaged.
ACK links are used for providing data latency. Retransmission can occur in this type of link if payload field of the packet gets corrupted.

c) Link Manager Layer:
Link Manager Protocol is implemented by this layer. Properties of the air interface link and links between Bluetooth enabled devices are controlled by this protocol. This protocol also manages bandwidth reservation and allocation, power control, authentication and trust relationship between devices. Power control is implemented by determining the transmission power levels and low power activity modes. This layer also deals with link generation, baseband packet sizes, link exchange and control, authentication and encryption techniques.

d) Host Controller Interface Layer:
To access the lower layer applications, upper layer applications of the stack require an interface. The Host Controller Interface Layer (HCI) provides this interface. By using the command interface provided by this layer, control registers and other hardware can be accessed. There is a uniform method for accessing the bluetooth baseband capabilities. This layer removes transport dependencies and provides a common device driver interface to various interfaces like RS 232, UART and USB.

e) Logical Link Control and Adaptation Protocol Layer:
Connection oriented and connectionless services between higher layer protocols and lower layer transport protocols are provided by this layer. It allows various protocols and applications to share the air interface by supporting multiplexing of several higher layer protocols like RFCOMM and
This layer also deals with segmentation of data packets that exceed the maximum transmission unit size before they are transmitted. This segmentation is done in such a way that the opposite of it, that is re-assembly can be done at the receiving end in order to retrieve the original data packet back. This layer also allows the information exchange regarding the QoS for the pair of Bluetooth enabled devices. By using this protocol, groups can be formed and mapped on to a piconet. The main advantage of this layer is compatibility and simplicity.

2. Middleware Protocol Group [5]:
The Middleware Protocol Group includes third party and industry standard protocols. The protocols defined in this group allow existing and new applications to operate over Bluetooth links.

a) Industry Standard Protocols:
Industry Standard Protocols include the following protocols adopted from Infrared Data Association (IrDA):

i) Point-to-Point Protocol (PPP): An internet standard protocol
iii) Wireless Application Protocol (WAP): Bluetooth can be used to transfer data between a WAP client and a WAP server. This protocol operates on the top of Bluetooth stack using TCP/IP protocol suite and PPP.
iv) Object Exchange (OBEX) Protocol: This session protocol is defined by IrDA. Bluetooth uses this protocol for enabling the application to use either IrDA or radio technologies.

b) Bluetooth SIG-developed Protocols:
These protocols include a serial port emulator (RFCOMM) to operate seamlessly over Bluetooth transport protocols which is mainly used for cable replacement. Using this simple transport protocol, circuits like RS-232 can be emulated over the Bluetooth protocol stack. It supports a variety of applications that use serial communication. It provides flow control, reliable data stream, serial cable line settings and multiple concurrent connections.

For managing telephony operations, a packet based telephony control signalling protocol (TCS) is used. The TCS protocol defines the call control signalling to establish voice and data calls between Bluetooth enabled devices. This bit oriented protocol also supports group management.

A service discovery protocol (SDP) allows devices to discover the services of available Bluetooth devices by obtaining information about each device’s available services. This is the basic requirement for all Bluetooth models. Using the information obtained by SDP, a connection between two or more Bluetooth enabled devices can be established.

3. Application Protocol Group [5]:
This protocol group includes Bluetooth aware applications and actual applications that use Bluetooth links.

**BLUETOOTH PAIRING**
The various stages included in the process of Bluetooth pairing are [1,11]:

i) Passive Mode: During this mode, a device is listening to the network.

ii) Inquiry: During this phase the primary device sends an inquiry request to all devices found in its vicinity. All devices that receive the query, reply with their addresses. So with this phase, establishment of connection begins.

iii) Paging: Paging is a technique through which the primary device selects an address and synchronizes with a device (also called an access point) within its range. Here the primary device synchronizes its frequency and clock with the device to be connected.
iv) Access point service discovery: The primary device starts the access point discovery phase using a protocol called Service Discovery Protocol (SDP). After this, a link with the access point gets established.

v) Creating a channel with access point: At the end of Service discovery phase, the primary device becomes ready to create a link between the access point and it.

vi) Pairing with security: The access point may use a security mechanism called Pairing, which restricts access to authorized users only. This technique is normally used to protect piconet from unauthorized access. Pairing is done with an encryption key called PIN (Personal Information Number).

vii) Using the network: Once the pairing is done, the primary device can use the communication link which is established between the access point and it.

EXPLOITING THE BLUETOOTH PAIRING PROTOCOL
The pairing protocol is designed to exchange the information between Bluetooth enabled devices as well as to update and synchronize the data. Bluejacking is a technique that involves exploiting the Bluetooth pairing protocol. Using this protocol, bluetooth devices can authenticate each other. This authentication is mainly used to pass a message during the initial handshake phase. The name of the initiating Bluetooth device displays on the target device as a part of the handshake exchange. This protocol also allows a name field to be passed as a message. This is actually a potential security problem that can cause exploitation of the protocol. The Bluejacking technique uses the first part of the pairing process in which information exchange takes place. During this initial phase of handshaking, the Bluejacker can successfully pair with target device.

IMPLEMENTATION OF BLUEJACKING
There are some basic requirements to implement Bluejacking. These requirements are as follows:

a) A Bluetooth enabled device: Any Bluetooth enabled device which can make use of its Bluetooth facility can be used to initiate Bluejacking. The technique used to implement Bluejacking in each Bluetooth enabled device is inherently the same except for certain minor differences. All of these take advantage of the loopholes in the Bluetooth pairing protocol to implement Bluejacking.

b) Software for Bluejacking: Bluejacking can also be implemented using certain softwares. These can be installed on a Bluetooth device and run to initiate Bluejacking. By using this technique, manual procedure of performing Bluejacking attack can be bypassed.

c) A crowded place: This is required since a Bluejacker is likely to find a recipient for his Bluejacking attack only in a crowded place. At such places, there is a higher probability of finding people with their Bluetooth on in their devices. A Bluejacker can make such a device a target of his attack.

A. Bluejacking using cell phones
This is similar to the creation of a contact on a Bluetooth enabled cell phone. The steps involved in this procedure are:

i. Select the “Create Contact” option in the phonebook/contact list.

ii. In the name field, enter the message that is to be sent as a part of Bluejacking message.

iii. Do not specify any number for the contact.

iv. Save this newly created contact.

v. Select this newly created contact from phonebook/contact list.

vi. Select the option of send Vcard or business card for that particular contact.

vii. Select the sub option “send via Bluetooth” for sending the Vcard/business card.
viii. A list of all the Bluetooth enabled devices with their Bluetooth in the discoverable mode will be displayed.

ix. Select any one device from this list to make an attack on.

x. Send the Vcard.

xi. The target will receive the Bluejacking message.

B. Bluejacking using Bluetooth enabled laptops

The steps involved in this procedure are:

i. Go to the contact in Email address book. (Any address book program such as Outlook).

ii. Create a new contact.

iii. Enter the message to be sent to an unsuspecting Bluetooth enabled user into the name field.

iv. Save the new contact.

v. Go to address book.

vi. Double click on the contact just created.

vii. Go to the action tab.

viii. Go to send to Bluetooth.

ix. Click on other.

x. Select a device from the list of Bluetooth enabled devices and double clicks on it.

The device will receive the Bluejacking message.

C. Bluejacking using Software tools

There is a variety of tools that are available for Bluejacking. Such tools can bypass the entire manual procedure for implementing Bluejacking. These softwares can be downloaded, installed and run on a Bluetooth configured device to send any anonymous, unsolicited message to another Bluetooth enabled device. Some examples of such tools are eJack, Meeting Point, Bluespam, Proximity mail, Freejack etc.

1) Bluespam:

This software searches for all discoverable Bluetooth devices and sends a file to them. A small text is sent to spam the other Bluetooth enabled device. To customize the message to be sent, the file or the message to be sent need to be put into a directory specific to the device and the software. This message or file will then be sent when Bluejacking is done. Bluespam also supports backfire, if the corresponding device is in discoverable and connectable mode.

2) Meeting Point:

It is software which is used to search for Bluetooth devices. A meeting point can be set to a specific channel to meet up with people who have not met before. This can be combined with any Bluejacking softwares. These softwares are compatible with almost all operating systems.

3) Freejack:

This is another tool for Bluejacking. It is compatible with java based cell phones.

APPLICATIONS OF BLUEJACKING

Bluejacking was originally started off for playing a prank on other strangers and to amuse oneself at the cost of the bewilderment of the recipients of the Bluejacking messages. But now, Bluejacking is no longer used just to play a prank. It is now being used as a new way of communication for marketing industry. The marketing industry has taken the benefit of such communication channels to communicate with their potential customers even though Bluejacking was never meant to be a marketing platform. Bluejacking offers three main opportunities to marketers:

a) Viral Communication [2]:

This deals with sharing the content like text, images and internet references for exploiting the communication between customers. This content is shared in the form of Bluejacking messages to a large audience for marketing the services or products. Because of mobile phones, such type of
communication has a very good influence on people for buying products as mobile phones are now become part of the personal space of any human being.

b) **Community activities [2]:**

Bluetooth can be used to send messages over distances of up to approximately 10 meters (33 feet) making event-based activities possible. This provides a platform for community based activities. Dating or gaming events could be facilitated using Bluetooth as a channel to communicate between participants. The anonymous nature of bluejacking makes it a superb physiological tool for communication between individuals in a localized environment such as a cafe or pub. Games publishers such as Cellsoft and Lavastorm Engineering have ported multiplayer games to Bluetooth-enabled devices.

c) **Location based services [2]:**

These location based services enable Bluejacking 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. They can be sent electronic coupons or promotional messages as they pass a high street shop or supermarket to lure them into getting inside and buying stuff. Such messages can be sent to all the users in the area with a Bluetooth enabled mobile handset or PDA.

**CODE OF ETHICS**

There are certain code of ethics that need to be followed by anyone who performs the act of Bluejacking. These are:

- Bluejackers should only send messages/pictures. They should never try to 'hack' device for the purpose of copying or modifying any les on any device or upload any executable.
- Any such messages or pictures sent should not be of an insulting, libelous or pornographic nature and will be copyright free or copyrighted by the sender.
- Any copyright protected images/sound les should only be sent with the written consent of the copyright holder.
- If no interest is shown by the recipient after 2 messages the bluejacker should desist and move on.
- The bluejacker should 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.
- If Bluejackers sense that they are causing distress rather than mirth to the recipient they should immediately decease all activity towards them.
- If bluejackers are caught 'in the act' of Bluejacking, they should be as co-operative as possible and not hide any details of their activity (honesty is the best policy).
- Bluejackers should follow all social practices of bluejacking.

**CONCLUSION**

Bluejacking technique can be used to 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. 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. So this technology can become the key for advertising and to interact with world and to get the location messages on the phone when a person is somewhere out. There are few security issue which can be minimized by taking some simple precautions.
REFERENCES