

Exposing the Potential to Invade Privacy with Bluetooth Enabled Devices

William M. Fitzgerald, *Telecommunications Software & Systems Group (TSSG), Waterford Institute Of Technology Ireland*

Abstract—With the over whelming and unpredictable growth of the Internet concerns have risen about a citizen's privacy. Privacy has become a major concern and the Internet has created numerous new privacy issues that society has not seen before. Spamming violates a citizen's privacy, and steals resources by invading the user in a "junk" form manner. Bluejacking a method to SPAM Bluetooth devices anonymously is the focus of this paper.

Index Terms—Bluetooth, Privacy, Security, BlueJacking

I. INTRODUCTION

THE term SPAMMING can be described as a spammer's ability to control the type, rate, and sequence of information a user may be viewing. This paper discusses what it is to SPAM Bluetooth devices and demonstrates how it can be achieved in an easy and non technical manner.

II. BACKGROUND

Definition: BlueJacking is defined as “the practice of sending messages between mobile users using a Bluetooth wireless connection” [1]. It is a legitimate activity that can be exploited to SPAM and invade the privacy of other Bluetooth enabled devices within range of the Bluejacker. Hence anonymous messages can be sent to a target device and or all devices in range [2].

Definition: BlueSnarfing is defined as “the theft of information from a wireless device through a Bluetooth connection” [1]. Bluesnarfing copies data from a target device provided device pairing succeeds. [2]

Definition: BlueStumbling is a method of monitoring and logging all visible Bluetooth devices (name, MAC, signal strength, capabilities), and identify manufacturer from MAC address lookup.

Definition: BlueBrowsing can be defined as the methodology of displaying the available services on a selected device (FAX, Voice, OBEX file transfer etc).

This paper is primarily focused on discussing Bluejacking as a means of invading privacy anonymously and as a means of SPAM.

III. BLUEJACKING SPAM HOW-TO

THIS section will describe two particular methods of how to Bluejack from a Bluetooth enabled Windows PC and from a Motorola V525 mobile phone [3]. There are many other methods depending on the mobile device but the principles should remain the same.

Bear in mind a Bluetooth enabled PC normally has a range of 100 meters whereas a Bluetooth phone has a range of 10 meters.

A. Bluetooth Enabled PC

- Go to contacts in your Email Address Book
- Create a new contact
- Enter the message you want to send to an unsuspecting Bluetooth enabled user into the name field
- Save the new contact
- Go to the address book
- Double click on the contact just created
- Go to action tab
- Go to Send to Bluetooth
- Click on other
- Select a device from the list and double click on it
- Voila!

B. Bluetooth Enabled Motorola V525

- Select New Entry from Contacts
- Select Phone Number
- Insert the message you want to send in Name field
- Enter 0 into No. field
- Save contact
- Select the just created contact from Contacts
- Press the Info button (middle button on bottom menu bar)
- Scroll to Send and select Send
- Choose Bluetooth
- Select Look For Devices
- Then select the device you want to Bluejack
- Voila!

Manuscript written 22 February, 2005. “*Exposing the Potential Implications for Privacy with Bluetooth Enabled Phones*”

William M. Fitzgerald is with the Telecommunications Software & Systems Group, at Waterford Institute of Technology, Ireland (phone: 00353 51 302937; fax: 00353 51 302901; e-mail: wfitzgerald@tssg.org).

C. Generic BlueJacking Method

- Create a new contact
- Enter the message to deliver in the Name field and any digit in the Number field if required
- Save contact
- Select that contact and search through send options until you see something like send via Bluetooth.
- Select the send via Bluetooth option
- Voila!

IV. CONCLUSION

THIS paper has described the methods by which Bluetooth devices are susceptible and it focuses its main concern to Bluetooth SPAMING (BlueJacking). It demonstrated how easy it is to perform such attacks on an individual or a group of individual's privacy.

REFERENCES

- [1] Whatis IT Related Definitions: <http://whatis.techtarget.com>
- [2] Leydan John, "Bluejacking Ain't Hijacking", theregister.co.uk, November 2003.
- [3] Motorola V525 user guide



William M. Fitzgerald (MSc, BSc) obtained a Master of Science Degree in Computer Science from National University of Ireland Maynooth (N.U.I.M) in Maynooth in 2002 and an Honors Bachelor of Science degree (majoring in Computer Science & Mathematics) also from N.U.I.M in 2000.

He is currently employed as an applied researcher for the Telecommunications Software & Systems Group (TSSG) at the Waterford Institute of Technology in Waterford, Ireland. William is focused on the security arena within European projects such as SecurIST, Daidalos and the PASR initiative. His current research interests are security (wired & wireless) Malware (Virology, RAT's, Worms, Phyogenetic's). Prior to his current employment he was employed as an applied security researcher with Ericsson's Systems Expertise Group, Dublin, Ireland. There he researched security of Ad-Hoc networks, reputation based metrics and novel game theoretic approaches to network node cooperation.

Some of William's publications: (1) *An Approach for Network Forwarding Systems Quality*, Information Technology and Telecommunications (IT& T), Athlone, Ireland, pp 103 -111, ISSN 1649 - 1246, 2001, (2) *Performance Analysis of Host Based Routing*, Masters of Science, N.U.I. Maynooth Library, 2002, (3) *Ericsson OSS Security Architecture: Current State and Challenges Ahead*, Ericsson R&D Ireland, 2003, (4) *Reputation and Cooperation in Ad Hoc Networks*, Ericsson R&D Ireland, Ericsson R&D Ireland, 2003, (5) *Constructing a Wireless Intrusion Detection System with Snort, MySQL, Apache, PHP, ACID & BASE on a Linux Platform*. Visit www.williamfitzgerald.org