International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 4 –NOVEMBER 2014.

# BLUE HACK- SECURITIZE YOUR BLUETOOTH

ANILAMBICA KATA[*1] and DR.B.RAMAIAH[#2]

*[1,2]Asst Prof, dept of Commerce KBN college, Vijayawada*

**Abstract— In the present world of Technology, man utterly depended on technology to make his life secure and comfort. There are lots of things around us that give us comfort but sometimes we misuse them. Ever since the first Bluetooth-enabled mobile phones started appearing a couple of years ago, numerous reports have suggested that the wireless technology is vulnerable to snooping. The purpose of this entire Bluetooth hacking is to hack your mobile phone and your privacy. Bluetooth hacking takes place because of security lacking in Bluetooth technology. This paper would be covering how a Bluetooth is being hacked and cause security issue. The theme of the topic is about Bluetooth Hacking, impact and its prevention. Further we will focus on how Bluetooth hacking is done, categories of Bluetooth hack, threat a business man and its prevention. While providing a great comfort but it is also a jeopardize.**

**KEY WORDS**
**Bluetooth, Blues narfing, Blue jacking, Blue bugging, Bluetooth firewall, Bluetooth file transfer**

## I. INTRODUCTION

Mobile, while providing great opportunity, security, it also provides risks. When we hear the term hacking, we usually think it’s only linked up with computer only. Now not only your computers are only hacked but also Bluetooth can be hacked too. This is one of the big drawbacks of Bluetooth. There are different types of hacking such as Blue jacking, Bluesnarfing, Bluebugging, Blueprinting etc. The purpose of this entire Bluetooth hacking is to hack your phone and your privacy. Bluetooth hacking takes place because of security lacking in Bluetooth technology. If someone hack your Bluetooth in that case hacker can steal your contacts, personal files, pictures, restore factory setting or they can use your phone for calling and using internet. Beside this they can access international mobile equipment identity number (IMEI), which they can use for cloning your cell phone. When your cell phone is cloned then your messages can be sent to other numbers. It will impact the business world. Mobile, while providing great opportunity, also provides security and risks. Companies need to protect their consumers in order to remain credible and reliable, for this, selection of the appropriate security policies for all Bluetooth capable devices will impact your business. This frequently includes handheld devices owned by employees. To avoid the fraudulent use of the corporate data, we need to follow some protocols: Keep BT in the disabled state and device in no discoverable mode. Use non regular patterns as PIN keys while pairing a device. Register your device at the Manufacturer site and insure that security updates are installed regularly to protect from previously known threat which had been rectified in new models. Proper security testing will provide customer satisfaction as well as increase company’s business.

## II. REVIEW OF LITERATURE

Bluetooth is a wireless technology for exchange of data over short distances (using short-wavelength UHFradio waves in the ISM band from 2.4 to 2.485 GHz) from fixed and mobile devices, and building personal area networks (PANs). Invented by telecom vendor Ericsson in 1994, it was originally conceived as a wireless alternative toRS-232 data cables. It can connect several devices, overcoming problems of synchronization.

Bluetooth itself was intended to unify a user’s devices to wireless personal area network (WPAN). A Bluetooth WPAN is called “PICONET” and may consist of mobile phones, PDAs, printers or personal computers.

## III. DIFFERENT TYPESOF BLUETOOTH RELATED THREATS AND ATTACKS BLUEJACKING

Blue jacking is a process of sending an anonymous message from a Bluetooth enabled phone to another, within a particular range without knowing the exact source of the received message to the recipient with in a range of 10m. Bluejacker will most likely comp out in crowded areas like shopping malls, airports- places with a potentially high percentage of people with Bluetooth enabled devices.

The best part of the blue jacking that it is very difficult out almost impossible for a victim to figure out the source of the received message.

BLUESNARFING: The term”snarf” means grabbing a large document or file and using it without the author’s permission. This Bluesnarfing is considered to be a serious issue in the category of blue hacking While Bluejacking is essentially harmless as it only transmits data to the target device, Bluesnarfing is the theft of information from the target device.

BLUEBUGGING: The third type of hacking mechanism is Bluebugging; Bluebugging goes well beyond Bluejacking and Bluesnarfing in which the hacker uses sophisticated attacks to gain control of victim’s mobile i.e. virtually complete takeover of a victims mobile They can even alter the call list, read the phone call list to see who their victims called or who called them.

## IV. PRECAUTIONS AND COUNTER MEASURES

As there are many aspects of security, the first ad the first and foremost precaution that has to be taken is the user awareness and vigilance is the best defense against the kinds of attacks of Bluetooth.

One of the effective countermeasures of Blue jacking is disable bluetooth on your mobile.

Configure your blue tooth settings and put your phone on Undiscourable /Hidden.

By regular Change of Bluetooth personal identification number (PIN) also makes a bit harder for attackers.

BLUETOOTH FIREWALL: protects our android device against all sort of Bluetooth attack from devices around us.

BLUETOOTH FILE TRANSFER: It provides custom security management for incoming BT connections, only authorized devices can connect, if you accept. If you refuse, no access is granted on your servers, personal data files and privacy are safe against hackers.

## V. CONCLUSION

The intent of this project was to determine how real the threat is of attacks to Bluetooth-enabled devices and how easy such attacks are to launch. The ideas that someone could listen to all conversations a victim is having without them even knowing, or have their text messages read, are key examples of the dangers of Bluetooth. Even worse, an attacker can initiate a call to someone or text someone without the victim ever knowing. The only way a user would be able to catch this activity is if they were to look through their call log or look at the sent messages on their phone. Even that might be insufficient, as the attacker can delete the records of their nefarious activity and the victim would never know until their bill comes out.

The victim would only know about unusual behavior if they carefully look at their bill, which is increasingly problematic since many people do not even look at their detailed call records. And even if someone complains that they "did not make a call on this date and time," the mobile service carrier has proof that the call was made from this device because, indeed, it was. Users need to be made aware of the vulnerabilities of these devices so that they can employ them more effectively, safely, and confidently.

## VI. REFERENCES

[1] An Ethical Guide to Hacking Mobile Phones By AnkitFadia
[2] Certified Ethical Hacker (CEH) Cert Guide By Michael Gregg
[3] Ceh Cert Ethical Hacker Exam Guide ByWalker
[4] http://gsyc.es/~anto/ubicuos2/bluetooth_security_and_hacks.pdf
[5] file:///C:/Documents%20and%20Settings/Administrator/Desktop/bluetooth_security_and_hacks.pdf