L&T Technology Services

BLUETOOTH HACKING AND ITS PREVENTION

Trapti Pandey | Pratha Khare

Table of Contents

ABSTRACT

There are lot of things around us to give comfort but we sometime misuse them. In this topic we would be covering how a Bluetooth is being hacked and cause security issue. The main objective of this presentation is about Bluetooth hacking, the impact and prevention. Further we will focus on how Bluetooth hacking is done, different categories of Bluetooth hack, threat a business can face and its prevention.

When we hear term hacking, we usually think it's attached with computer only. Now your computers are not only hacked but your Bluetooth can be hacked too. This is one of the big drawbacks of Bluetooth. There are different types of hacking such as Bluejacking, Bluesnarfing, Bluebugging, Bluetoothing, 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 non-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.

INTRODUCTION

Bluetooth is a wireless communication standard that was developed in 1998 to revolutionize the small, personal and portable electronic device market. It provides a protocol for low power peripherals (cell phones, PDA's, mobile computers) to communicate with each other over a small range.

In any wireless networking setup, security is a concern .Unfortunately, Bluetooth still contains a large number of security vulnerabilities despite the claims made by the Bluetooth special interest group.

Bluetooth hacking is a technique used to get information from another Bluetooth enabled device without any permissions from the host. This event takes place due to security flaws in Bluetooth technology. Bluetooth hacking is not limited to cell phones, but is also used to hack PDAs, Laptops and desktop computers.

TECHNOLOGY

Figure 1 shows a diagram of the Bluetooth protocol stack in order to show the various attack vectors.

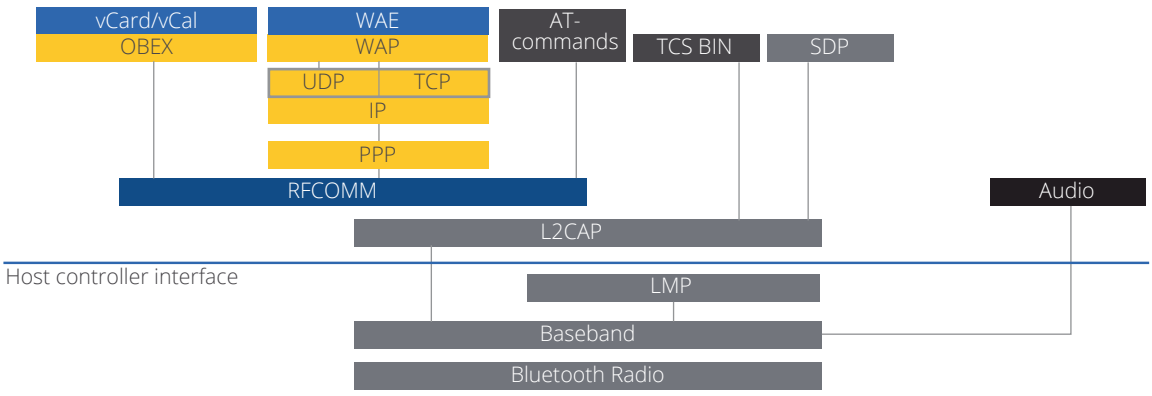

FIGURE 1 : BLUETOOTH PROTOCOL STACK

The protocol layers of particular interest in this paper are:

- Logical Link Control and Adaptation Protocol (L2CAP): Provides the data interface between higher layer data protocols and applications, and the lower layers of the device; multiplexes multiple data streams and adapts between different packet sizes.
- Radio Frequency Communications Protocol (RFCOMM): Emulates the functions of a serial communications interface (e.g., EIA-RS-232) on a computer. As Figure 1 shows, RFCOMM can be accessed by a variety of higher layer schemes, including AT commands, the Wireless Application Protocol (WAP) over the Transmission Control Protocol/Internet Protocol (TCP/IP) stack or the Object Exchange (OBEX) protocol.
- Object Exchange protocol: A vendor-independent protocol allowing devices to exchange standard file objects, such as data files, business cards (e.g., vCard files) and calendar information (e.g., vCal files). OBEX is a higher layer application and runs over different operating systems and different communications protocols

Most of the tools that are being used to hack Bluetooth phones use the Java programming language. In order for the software to work, the phone that is used to initiate the attack needs to support JSR-82, which is the official Java Bluetooth Application Programming Interface (API). If the attacker's phone does not support JSR-82, that phone cannot be used to attack other phones. This is an important note because although Bluetooth is widely available on cell phones, Java and JSR-82 support may not be.

The capabilities of JSR-82 include the ability to:

- Register services
- Discover devices and services
- Establish L2CAP, RFCOMM, and OBEX connections between devices, using those connections to send and receive data (voice communication is not supported)
- Manage and control the communication connections

BLUETOOTH SECURITY

Bluetooth defines three security modes:

1. Security Mode 1: non-secure
2. Security Mode 2: service level enforced security
3. Security Mode 3: link level enforced security

All Bluetooth services have a default set level of security. Within the service level security, there are also three levels of security. Some services that require authorization and authentication in order to be used, some require authentication only, and some are open to all devices .Bluetooth devices themselves have two levels of security when describing other devices, namely trusted devices and untrusted devices.

DIFFERENT TYPES OF BLUETOOTH-RELATED THREATS AND ATTACKS

BLUEJACKING: Blue jacking is the 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. 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.

BLUESNARFING: The term "snarf" means grabbing a large document or file and using it without the author's permission. Bluesnarfing is considered a serious compromise in the category of Bluetooth hacking especially if the information vulnerable, is quite critical, as such attacks can allow the hacker access to victims; contact list, text messages, emails and even private photos and videos.

Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their knowledge. While Bluejacking is essentially harmless as it only transmits data to the target device, Bluesnarfing is the theft of information from the target device.

Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) may be susceptible to Bluejacking, and possibly to Bluesnarfing if there is vulnerability in the vendor's software. By turning off this feature, the potential victim can be safer from the possibility of being Bluesnarfed; although a device that is set to "hidden" may be Bluesnarfable by guessing the device's MAC address via a brute force attack. As with all brute force attacks, the main obstacle to this approach is the sheer number of possible MAC addresses. Bluetooth uses a 48-bit unique MAC Address, of which the first 24 bits are common to a manufacturer. The remaining 24 bits have approximately 16.8 million possible combinations, requiring an average of 8.4 million attempts to guess by brute force.

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. In this hacker can manipulate the users phone the way he desires by executing commands on the victims phone. The hacker could forward mobile calls from the victim's mobile to his own device and can even manipulate the mobile to follow a Bluetooth headset instructions like; receive call, send messages etc. They can even alter the call list, read the phone call list to see who their victims called or who called them.

There are many more types of attacks like bluetoothing, blueprinting etc.

TOOLS FOR ATTACK:

1 Super Bluetooth Hack

2. Blue Sniff

3. Blue Scanner

4. BlueBugger

5. BT Browser

6. BT Crawler

PRECAUTIONS

As with so many aspects of security, user awareness and vigilance is the best defence against the kinds of attacks described here. The best way to protect a device, obviously, is to simply turn Bluetooth off. A device cannot be hacked via a Bluetooth attack vector if other Bluetooth devices cannot see it. Some devices come with Bluetooth turned on by default so users need to check this setting.

If Bluetooth must be enabled, the user can set the device to be hidden .Setting a device to be invisible will still allow Bluetooth communications to function but will only allow connections to trusted devices that have been previously configured. This protection is not perfect, however; if an attacker finds out that a particular device is trusted, they can use their own Bluetooth device as the trusted device and will then be able to connect to the target phone.

If a user must use Bluetooth, they should also only turn it on as needed. In addition, users should change their Bluetooth personal identification number (PIN) every month or so. Changing the PIN requires that any Bluetooth devices that the user regularly employs will need to be re-paired, but it also makes it a bit harder for attackers. Attacks succeed because many users will balk at constantly turning their Bluetooth port on and off, or changing the PIN, but at the very least users should change the default PIN when they first get their Bluetooth enabled device.

User must use updated software and drivers to take advantage of product improvements and security fixes .It's also recommended to stop using a non-supported or not secure Bluetooth-enabled devices or module, e.g. Bluetooth 1.0 and 1.2

For Android devices there are many Application available in Play store, for protecting device from Bluetooth hacking, some are mentioned below:-

1. BLUETOOTH FIREWALL: Mobile Bluetooth Firewall protects our android device against all sort of Bluetooth attack from devices around us. It displays alerts when Bluetooth activities take place. You can also scan your device and detect apps with Bluetooth capabilities. So if you have installed a malicious app unknowingly this is the time to detect and uninstall it.

2. 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.

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 behaviour 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.

ACKNOWLEDGMENT

We would like to give our sincere gratitude to Mr Pradip Bonde, Mr Ashish Motwani, Mr Vikram Rathod, Mr Santosh Mahadik, Mr Chaitanya Telang and Mrs Vity Patle to provide with their Valuable feedback and suggestion valuable feedback and suggestion for this paper. Last but not the least; we would like to thank our colleagues for supporting us.

REFERENCES

1. http://www.onlytechtalks.com/techtalks/2009/05/tips-for-preventing-bluetooth-hack/
2. http://www.codenomicon.com/defensics/bluetooth/
3. http://en.wikipedia.org/wiki/Bluesnarfing
4. http://en.wikipedia.org/wiki/Bluejacking
5. http://en.wikipedia.org/wiki/Bluebugging

References

i. National Highway Traffic Safety Administration, http://www.nhtsa.dot.gov/

ii. Robert Laganiere "OpenCV 2 Computer vision Application programming cook book", Aug 2013.

iii. Bruno Keymolen "Theory of Hough Transformation" May 2013.

iv. Probabilistic and non-probabilistic Hough transforms: overview and comparisons, by Heikki, Petri, Lei Xu.

ABOUT L&T TECHNOLOGY SERVICES

L&T Technology Services is a subsidiary of Larsen & Toubro with a focus in the engineering services space, partnering with a large number of Fortune 500 companies globally. We offer design and development solutions through the entire product development chain, across various industries such as Industrial Products, Medical Devices, Transportation, Telecom and Hi-tech and the Process Industry. We also offer solutions in the areas of Mechanical Engineering Services, Embedded Systems & Applications, Engineering Process Services, Product Lifecycle Management, Engineering Analytics, Power Electronics and Machine-to-Machine and the Internet-of-Things (IoT).


L&T Technology Services