

Analysis of Bluetooth based attacks using inbuilt tools

Shruti Avhad(20074030)

Liza Pradhan(20074019)

Mohammad Zaid(20075056)

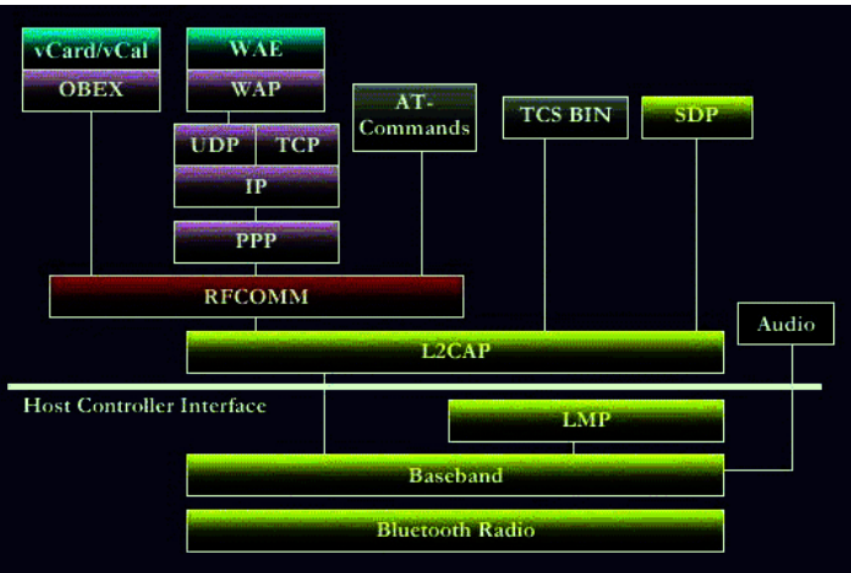
¹ **PROJECT SUPERVISOR:-**

² Dr. Mayank Swarnkar Assistant Professor,
Department of Computer Science and Engineering,
Indian Institute of Technology (BHU) Varanasi

May 1, 2022



- 1 Introduction
- 2 Motivation
- 3 Work Done/ Proposed Method-I
- 4 Work Done/ Proposed Method-II
- 5 Experimental Setup
- 6 Experimental Results
- 7 Conclusion
- 8 References
- 9 Thank You



The primary use of Bluetooth involves connecting multiple devices without using either cables or wires.

This wireless technology allows us to make safe calls when behind the wheel, listen to music on our walks, talk to loved ones through a microphone, and share files.

When two Bluetooth devices connect, this is referred to as pairing. Nearly any two Bluetooth devices can connect to each other. Any discoverable

Bluetooth device transmits the following information:

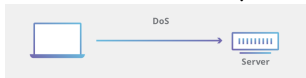
- * Name
- * Class
- * List of services

Hackers can exploit this exchange of sensitive data between the devices. Hence it is very necessary to understand and study the Bluetooth vulnerabilities.

Launch Various Bluetooth Attacks using in-built tools

We performed following attacks on various host devices.

Denial Of Service/Bluesmack Attack:



When the victim's device is overwhelmed by huge packets it is known as Bluesmacking.

Blueborne Attack:

Hackers leverage Bluetooth connections to penetrate and take complete control over targeted devices.

Bluesnarfer Attack:

```
bluesnarfer

rootkali:~# bluesnarfer --help
bluesnarfer: invalid option -- '-'
bluesnarfer, version 0.1
usage: bluesnarfer [options] [ATCMD] -b bc_addr

ATCMD      : valid AT+CMD (GSM EXTENSION)

TYPE       : valid phonebook type -.
example    : "DC" (dialed call list)
            "SM" (SIM phonebook)
            "RC" (received call list)
            "EX" such more

-b bc_addr  : bluetooth device address
-c chan     : bluetooth rfcomm channel

-C ATCMD    : custom action
-r N-M      : read phonebook entry N to M
-d N-M      : delete phonebook entry N to M
-f name     : search "name" in phonebook address
-s TYPE     : select phonebook memory storage
-l          : list available phonebook memory storage
-i          : device info
```

Hackers leverage over the bluetooth connections and procure information such as phonebook entry etc.

Bluejacking Attack:

Sending messages to host devices through bluetooth.

- 1 Attacker Device
- 2 Softwares and Packages:
 - i Kali, Parrot, Ubuntu OS
 - ii Wireshark
 - iii Bluez Module
 - iv Bluesnarfer Module
- 3 Bluetooth Dongle
- 4 Victim Device

Bluetooth
attacksShruti, Liza,
Zaid

Introduction

Motivation

Work Done/
Proposed
Method-IWork Done/
Proposed
Method-IIExperimental
SetupExperimental
Results

Conclusion

References

Thank You

Attack	Devices	Successful, what is the end result?	Reason
Denial Of Service/Bluesmacking attack	Motorola XS	No, it runs for some time then shows the host is down.	This attack mainly works on IOT devices that are weak in Bluetooth security.
	Samsung galaxy S4	No	
	Macbook	No	
	Google Home Nest	Yes, the speaker stops playing music.	It is an IOT device, it performs the task of playing music gets loaded by
	JBL wireless speakers	No	
	Boat rockerz headphones	No	
	Philips Speaker	Yes, the speaker dysfunctions and no one can connect to it afterwards	
Bluesnarfer Attack	Samsung galaxy S4	Yes, its recent call logs were visible.	Relatively older device with weak security protocols.
	Motorola XS	No, shows an error code.	Immediately stops unidentified data transfer.
	Macbook	No	Immediately stops

Bluetooth attacks

Shruti, Liza, Zaid

Introduction

Motivation

Work Done/
Proposed
Method-IWork Done/
Proposed
Method-IIExperimental
SetupExperimental
Results

Conclusion





References

Thank You

	Samsung galaxy J7	yes	
	Oneplus X	Yes, shows recent call logs	Relatively older device with weak bluetooth security
	Nokia	Yes, shows recent call logs	Relatively older device with weak bluetooth security
	Poco M3	No, shows errors	No transfer of data
<u>Blueborne Attack</u>	mi	Not vulnerable	
	Motorola X4	Not vulnerable	
	Iphone 12	Not vulnerable	
	Oneplus X	Yes, vulnerable and it will extract data from the unpatched bluetooth device	
Blueranger	Motorola X4	Shows proximity of devices based on its connection strength.	Generally works on all devices

- There are various other bluetooth attacks that can be launched provided if we have proper kits and tools.
- These Vulnerabilities cause a serious threat for the privacy of the people.
- These exploit can happen only and only when the bluetooth of a device is on, so we must ensure that the bluetooth is turned off if not in use.

-  K. Haataja and P. Toivanen, "Two practical man-in-the-middle attacks on bluetooth secure simple pairing and countermeasures," *IEEE Transactions on Wireless Communications*, vol. 9, no. 1, pp. 384–392, 2010.
-  N. Patel, H. Wimmer, and C. M. Rebman, "Investigating bluetooth vulnerabilities to defend from attacks," in *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)*, pp. 549–554, 2021.
-  T. A. D. Fatani, *Bluetooth Vulnerabilities on Smart Phones Running in Ios and Android Operating System*.
PhD thesis, Universiti Teknologi Malaysia, 2013.
-  S. N. Premnath and S. K. Kasera, "Battery-draining-denial-of-service attack on bluetooth devices," *Thanks to*, p. 3, 2008.

-  J. T. Vainio *et al.*, “Bluetooth security,” in *Proceedings of Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking, Spring*, vol. 5, 2000.
-  A. C. Santos, Á. Í. Silva, V. Nigam, I. E. Fonseca, *et al.*, “Ble injection-free attack: a novel attack on bluetooth low energy devices,” *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–11, 2019.
-  P. Gullberg, “Denial of service attack on bluetooth low energy,” 2016.
-  D. Singelée and B. Preneel, “Improved pairing protocol for bluetooth,” in *International Conference on Ad-Hoc Networks and Wireless*, pp. 252–265, Springer, 2006.
- [1]. [2]. [3] [4] [5] [6] [7] [8]

Bluetooth attacks

Shruti, Liza,
Zaid

Introduction

Motivation

Work Done/
Proposed
Method-I

Work Done/
Proposed
Method-II

Experimental Setup

Experimental Results

Conclusion

References

Thank You