Bluetooth Attacks Documentation

1. Bluejacking :

What is Bluejacking?

Bluejacking involves sending a contact (vCard) with a short message to nearby devices. The message is typically sent via Bluetooth's "send a business card" feature. Bluejacking doesn't gain control over a device but uses the Bluetooth discoverability feature.

Software used :

1. `bluez`: It's a package that contains Bluetooth utilities for Linux. It helps in scanning, pairing, and sending files to Bluetooth devices.

2. `obexftp`: This is used to send files over Bluetooth, specifically for protocols like OBEX (used for business cards).

Executing the attack :

Installation commands

```
sudo apt-get update
sudo apt-get install bluez obexftp
```

Start Bluetooth and scan devices

```
sudo systemctl start bluetooth
sudo systemctl enable bluetooth
hcitool scan
```

```
harish@harish-Inspiron-5570:~$ sudo systemctl start bluetooth
sudo systemctl enable bluetooth
[sudo] password for harish:
Synchronizing state of bluetooth.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable bluetooth
harish@harish-Inspiron-5570:~$ hcitool scan
Scanning ...
        FC:04:1C:5A:EF:E8       OPPO A15s
        E0:03:6B:55:55:24       [TV] Samsung AU7600 55 TV
        F8:71:0C:68:3B:C2       POCO F5
```

Create a vCard file

```
echo "BEGIN:VCARD
VERSION:3.0
FN:Bluejacking!
TEL:+1234567890
END:VCARD" > bluejack.vcf
#Full Name
#Placeholder - Not necessary
```

```
harish@harish-Inspiron-5570:~$ echo "BEGIN:VCARD
VERSION:3.0
FN:Bluejacking!    #Full Name
TEL:+1234567890    #Placeholder - Not necessary
END:VCARD" > bluejack.vcf
```

Send vCard to target device

```
obexftp --nopath --noconn --uuid none --bluetooth
<MAC_address> -<channel> -p bluejack.vcf
```

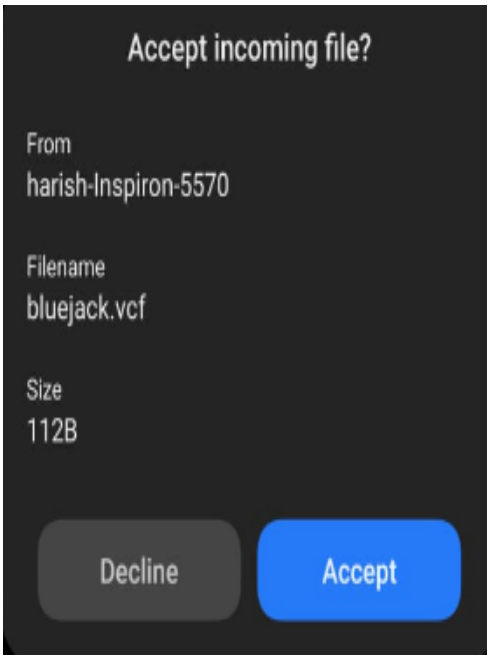
Find channel using

```
sudo sdptool browse <MAC_address>
```

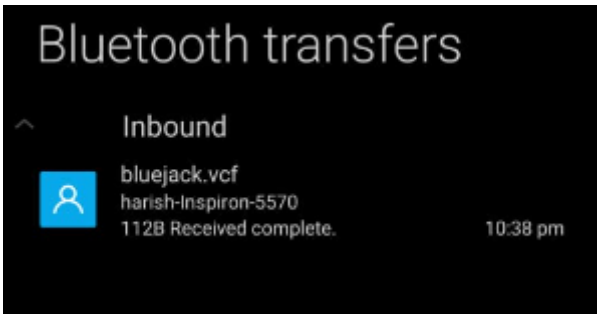
```
Service Name: OBEX Object Push
Service RecHandle: 0x1000b
Service Class ID List:
  "OBEX Object Push" (0x1105)
Protocol Descriptor List:
  "L2CAP" (0x0100)
  "RFCOMM" (0x0003)
    Channel: 12
  "OBEX" (0x0008)
Profile Descriptor List:
  "OBEX Object Push" (0x1105)
    Version: 0x0102
```

```
harish@harish-Inspiron-5570:~$ obexftp --nopath --noconn --uuid none --bluetooth F8:71:0C:68:3
B:C2 --channel 12 --put bluejack.vcf
Suppressing FBS.
Connecting..\done
Sending "bluejack.vcf".../done
Disconnecting..-done
```

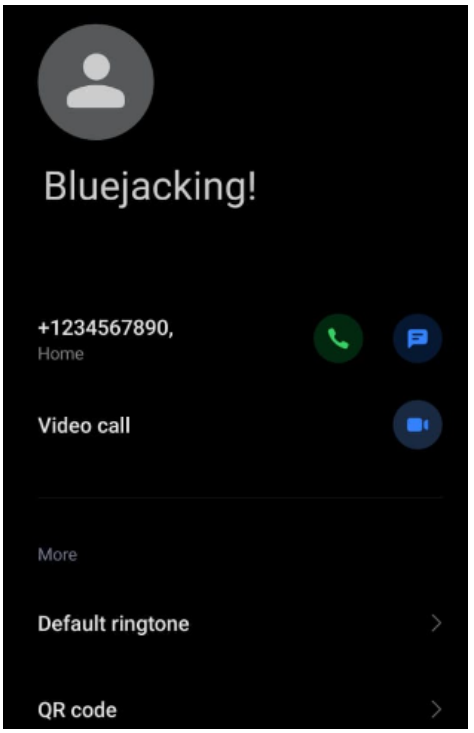
1.



2.



3.



2. Bluebugging

What is Bluebugging?

Bluebugging is a type of Bluetooth attack that allows an attacker to gain unauthorized access to a device. The attacker can exploit Bluetooth connections to control the victim's device, read messages, make calls, and more. Bluebugging attacks usually target devices with poorly configured Bluetooth security or outdated software.

Software used :

BlueZ: This is the official Linux Bluetooth protocol stack and is essential for interacting with Bluetooth devices on Ubuntu.

hciconfig: This tool is part of the BlueZ package and is used to configure Bluetooth devices. It helps manage the Bluetooth interface (hci0) for scanning and connecting to devices.

hcitool: Another part of the BlueZ suite, used to query devices, scan for Bluetooth devices, and establish connections.

rfcomm: A tool for setting up serial communication over Bluetooth RFCOMM channels. It can help in establishing a channel to a target device, a critical step in bluebugging.

Bluetooth Libraries and Utilities: Ensure that you have the libraries and utilities to facilitate communication and debugging. This includes libraries like `libbluetooth-dev`.

Bluebugger:
Bluebugger is a software tool used to exploit a vulnerability in older or improperly secured Bluetooth-enabled devices, allowing attackers to gain unauthorized access to the target device. This type of attack, known as bluebugging, can allow an attacker to:

- Access and control the victim's phone or device remotely.

- Make calls, send messages, or access contacts and messages without permission.
- Eavesdrop on phone conversations or retrieve personal data.

Installation:

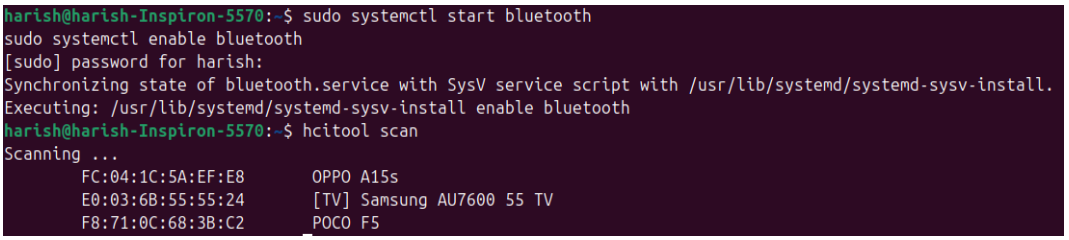
```
sudo apt install bluez bluetooth rfcomm
sudo apt install libbluetooth-dev
```

```
git clone https://github.com/webdragon63/Bluebugger.git
cd Bluebugger
make
```

Executing the attack

Start Bluetooth and scan devices

```
sudo systemctl start bluetooth
sudo systemctl enable bluetooth
hcitool scan
```



Accessing phonebook

3. Man in the middle attack(MITM)

A Bluetooth MITM attack involves intercepting and potentially altering communication between two Bluetooth devices.

Software used :

BlueZ: Official Linux Bluetooth protocol stack.

Wireshark: For capturing and analyzing network traffic.

hciconfig and hcitool: Tools for configuring Bluetooth devices in Linux.

Installation commands:

```
sudo apt update
sudo apt install bluez

sudo apt install wireshark
```

Configure Wireshark:

```
sudo usermod -aG wireshark $USER
```

Carrying out the attack:

Start bluetooth service

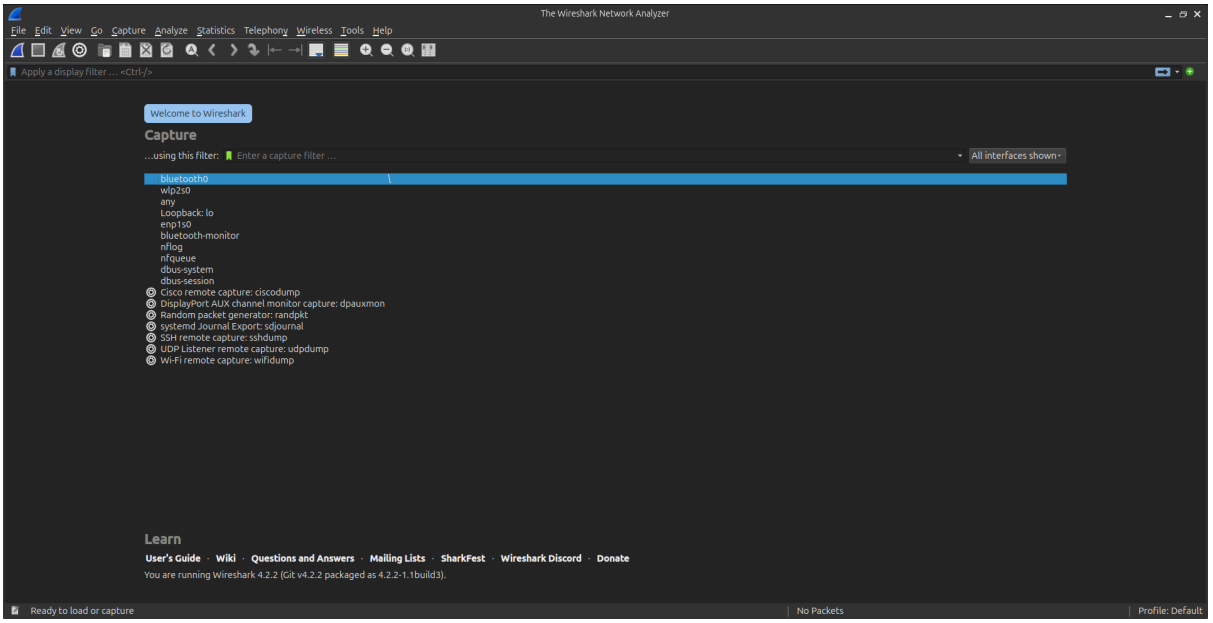
```
sudo systemctl start bluetooth
```

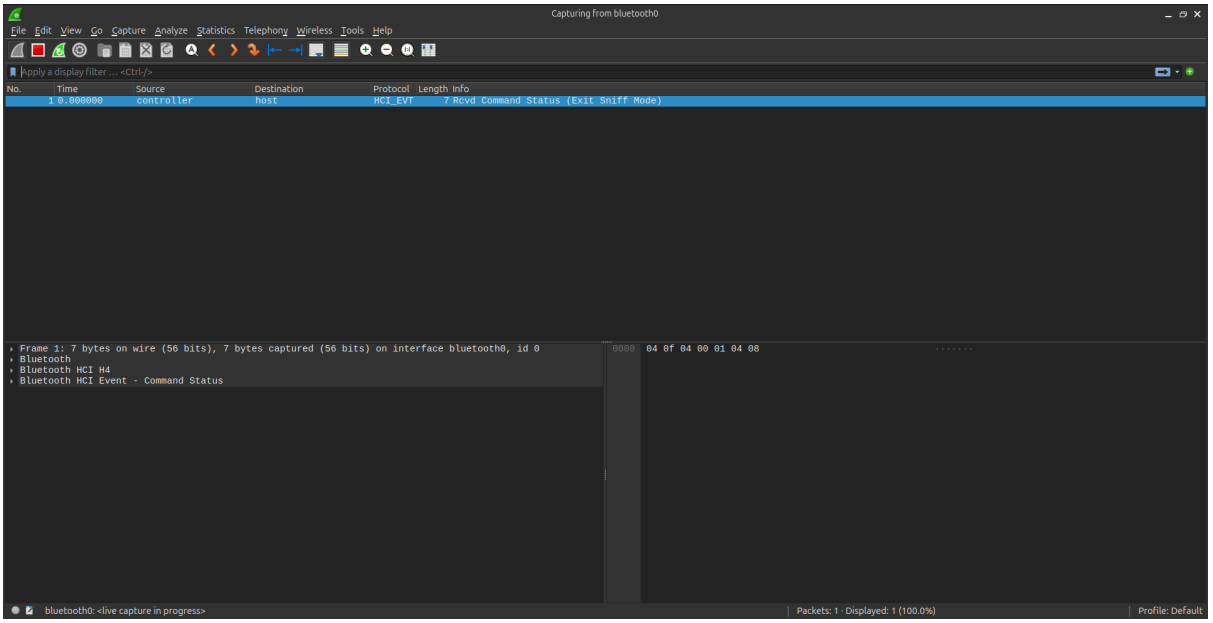
Scan for devices :

```
bluetoothctl
scan on

#after devices get listed

pair <target_mac_address>
```

Capturing transmitted information

```
exit
wireshark
```





Constant transmission of audio from target(phone)

```
sudo apt install pulseaudio pulseaudio-module-bluetooth
pavucontrol
```

```
harish@harish-Inspiron-5570:~$ sudo apt install pulseaudio pulseaudio-module-bluetooth pavucontrol
[sudo] password for harish:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
```