

13.2.2 Bluetooth Hacking Facts

As an ethical hacker, you should understand the common ways of exploiting Bluetooth flaws; be able to identify and use tools that can perform Bluetooth hacking; and use security tools that can help you defend your network from Bluetooth hacking.

This lesson covers the following topics:

- Bluetooth threats
- Bluetooth hacking
- Bluetooth hacking tools
- Linux Bluetooth configuration and discovery tools
- Countermeasures

Bluetooth Threats

Following are examples of threats to the privacy of users' personal information from hackers who have exploited Bluetooth vulnerabilities.

- Calendars and address books have been leaked through the Bluetooth protocol.
- Generally available software has activated Bluetooth cameras and microphones, making it easy to create bugging and eavesdropping devices.
- Compromised smart phones are used to visit internet sites and make phone calls to numbers that charge fees.
- Victims have been fooled into disabling Bluetooth security, allowing attackers to pair with a device and steal its information.
- Smartphone worms have been created that replicate and spread by exploiting Bluetooth connections.

Bluetooth Hacking

The following table lists some common forms of Bluetooth hacking:

Bluetooth Hacking	Description
Bluesmacking	A BlueSmack attack is a denial-of-service attack. The L2CAP layer of the Bluetooth Protocol stack is used to transfer an oversized packet. This causes the L2CAP layer to crash, denying Bluetooth services to the user.
Bluejacking	Bluejacking is the act of sending unwanted data to Bluetooth devices that are enabled and discoverable. Bluejacking hackers don't gain control of the device and can't steal data from the device. The messages they send are usually more annoying than malicious.
Bluesnarfing	Bluesnarfing exploits the Object Exchange (OBEX) protocol to gain access to a device. If that device is a smartphone, the attacker can access the address book, call data, text data, and other sensitive information.
Bluesniffing	Bluesniff is a Bluetooth wardriving utility that finds discoverable and hidden Bluetooth devices. Hackers use it to locate vulnerable devices.
Bluebugging	A Bluebugging attack exploits a Bluetooth device to install a backdoor that bypasses normal authentication, giving full access to the device. Bluebugging has been used to initiate and forward phone calls from a smart phone, send text messages, steal sensitive data, track the victim, and even change network provider settings.
Blueprinting	<p>Blueprinting is the act of gathering details about a Bluetooth device that might indicate its manufacturer and model. Using this information, the attacker can research whether the device has any security vulnerabilities. One readily available item that the attacker uses is the device address.</p> <p>Details that an attacker uses to determine the manufacturer and model are:</p> <ul style="list-style-type: none"> ▪ The first part of the Bluetooth address. ▪ Responses using the Service Discovery Protocol, which give information on how to access the device's services.
Bluetooth MAC spoofing	<p>Bluetooth MAC spoofing occurs when an attacker changes the Bluetooth address of his own device to match the address of a target device. In this attack, the data meant for the victim's device reaches the attacker's device first.</p> <ul style="list-style-type: none"> ▪ Bluetooth MAC spoofing can be part of an impersonation attack where the attacker's device appears to be the victim's device. ▪ If the attacker forwards the data to the victim device after intercepting it, it can be classified as a man-in-the-middle attack.

Bluetooth Hacking Tools

The following table lists some common Bluetooth hacking tools. Each tool is designed to run on either the Windows or Linux platform.

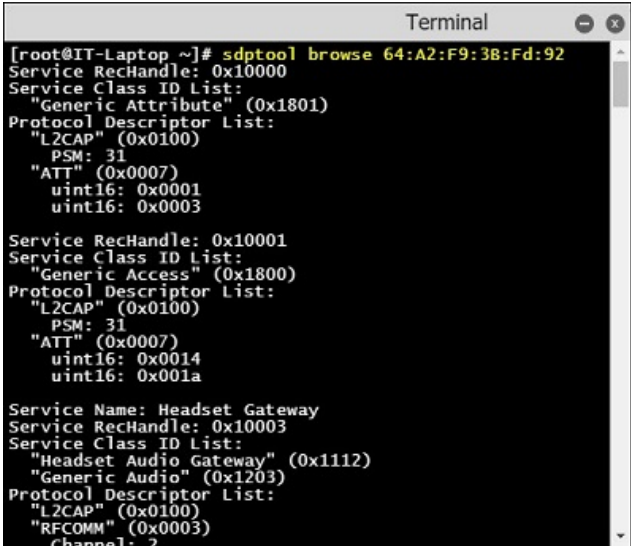
Bluetooth Hacking Tool	Platform	Description
BluetoothView	Windows	BluetoothView is a small utility that lists discoverable Bluetooth devices with information such as the device name, Bluetooth address, major device type, and minor device type. It runs in the background and monitors the activity of Bluetooth devices. It can also send a notification when a new Bluetooth device is detected.
BTScanner	Linux	BTScanner is Linux-based Bluetooth sniffing tool that provides the same functions as BluetoothView.
Btlejuice	Linux	Btlejuice is a complete framework to perform man-in-the-middle attacks on Bluetooth smart devices. It is composed of an interception core, an interception proxy, and a dedicated web interface. The core and proxy components are run on two independent computers, each with a Bluetooth adapter. Using the two adapters, Btlejuice can send and receive Bluetooth communications to perform a man-in-the-middle attack.
Bluediving	Linux	Bluediving is a Bluetooth penetration suite that runs on Linux. It can implement several attacks, including Bluebug, Bluesnarf, and Bluesmack. It also performs Bluetooth address spoofing.
Super Bluetooth Hack	Android	Super Bluetooth Hack is an Android phone application to view the files on another Bluetooth-connected Android phone.

Linux Bluetooth Configuration and Discovery Tools

Many distributions of Linux include a Bluetooth stack called BlueZ. BlueZ includes basic tools that discover and set up Bluetooth devices. Using it, you can collect helpful information about the devices and people around you.

To help configure and manage Bluetooth on these distributions, use the following commands:

Name	Description	Example
hciconfig	<p>This tool can view and manage Linux Bluetooth devices. When run without any options, hciconfig displays the name and basic information of all the Bluetooth devices installed in the system. hciX (where <i>x</i> is a number) is the name of a Bluetooth device installed in the system. HCI is an acronym for Host Controller Interface.</p> <p>Common commands for this tool are:</p> <ul style="list-style-type: none"> ▪ hciX up, which opens and initializes the Bluetooth device. ▪ hciX down, which closes the Bluetooth device. 	<p>hciconfig displays the name and basic information about all the Bluetooth devices installed in the system. In the sample output, you can see that the name of this device is hci0 and that the device is currently down. To use this device, it must be up or initialized.</p> <p>Sample output: hci0 Type: Primary BUS: UART BD Address: 23:82:FD:2B:6B:BF ACL MTU: 1021:5 SCO MTU: 96.5 DOWN</p> <p>hciconfig hci0 up opens and initializes the hci0 Bluetooth device.</p>
hcidtool	<p>This tool configures Bluetooth connections and sends special commands to the Bluetooth devices. If no command is given, or if the option -h is used, hcidtool prints some usage information and exits.</p> <p>Common commands for gathering information about Bluetooth devices using this tool are:</p> <ul style="list-style-type: none"> ▪ scan inquires (searches) for remote devices. For each discovered device, the device MAC address and name are displayed. ▪ ing searches for remote devices. For each discovered device, the clock offset and class are shown. 	<p>hcidtool scan sample output: 64:A2:F9:3B:FD:92 Mac Laptop</p> <p>hcidtool ing output: 64:A2:F9:3B:FD:92 clock offset: 0x614e class: 0x5a020c</p>
sdptool	<p>This tool provides the interface for performing Service Discovery Protocol (SDP) queries on Bluetooth devices. sdptool checks which services are made available by a specific device and can work when the device is not discoverable, but is still nearby.</p> <p>A common command is browse mac_address. This browses all available services on the device as specified by the Bluetooth MAC address parameter.</p>	<p>sdptool browse 64:A2:F9:3B:FD:92 sample output:</p>

		
l2ping	<p>L2ping sends an L2CAP echo request to the Bluetooth MAC address given in dotted hex notation. L2ping can be run only by the root user and can check to see if the Bluetooth device is up.</p> <p>Pressing Ctrl + c stops the ping process.</p>	<p>l2ping 64:A2:F9:3B:FD:92 sample output:</p> <pre>44 bytes from 64:A2:F9:3B:FD:92 id 0 time 16.37ms 44 bytes from 64:A2:F9:3B:FD:92 id 1 time 10.59ms 44 bytes from 64:A2:F9:3B:FD:92 id 2 time 19.46ms 44 bytes from 64:A2:F9:3B:FD:92 id 3 time 24.45ms 4 Sent, 4 received, 0% loss</pre>

Countermeasures

Many Bluetooth attacks can easily be defeated by common sense security countermeasures:

- Ensure each Bluetooth device is operating in a higher security mode.
 - The Bluetooth specification details four security modes.
 - Mode 1 is insecure, but has been phased out in later versions.
 - Each successive security mode is more secure.
 - Mode 4 requires encryption and the use of Diffie-Hellman techniques for key exchange and key generation.
 - Later versions of Bluetooth require mode 4.
- Use non-regular patterns when pairing. Setting PIN keys using regular patterns, such as sequential numbers, makes them easier to guess.
- Disable Bluetooth on a device immediately after the intended task is completed.
- While Bluetooth is enabled, use hidden mode. Hidden mode prevents other devices from finding your device.
- Use a Bluetooth firewall on Android devices.
- Lower the power setting on Bluetooth devices. This decreases Bluetooth range, but reduces the possibility of an outsider attack.