

Explaining Bluetooth Hacking



Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | Twitter: [@dalemeredith](https://twitter.com/dalemeredith) | LinkedIn: [dalemeredith](https://www.linkedin.com/in/dalemeredith)



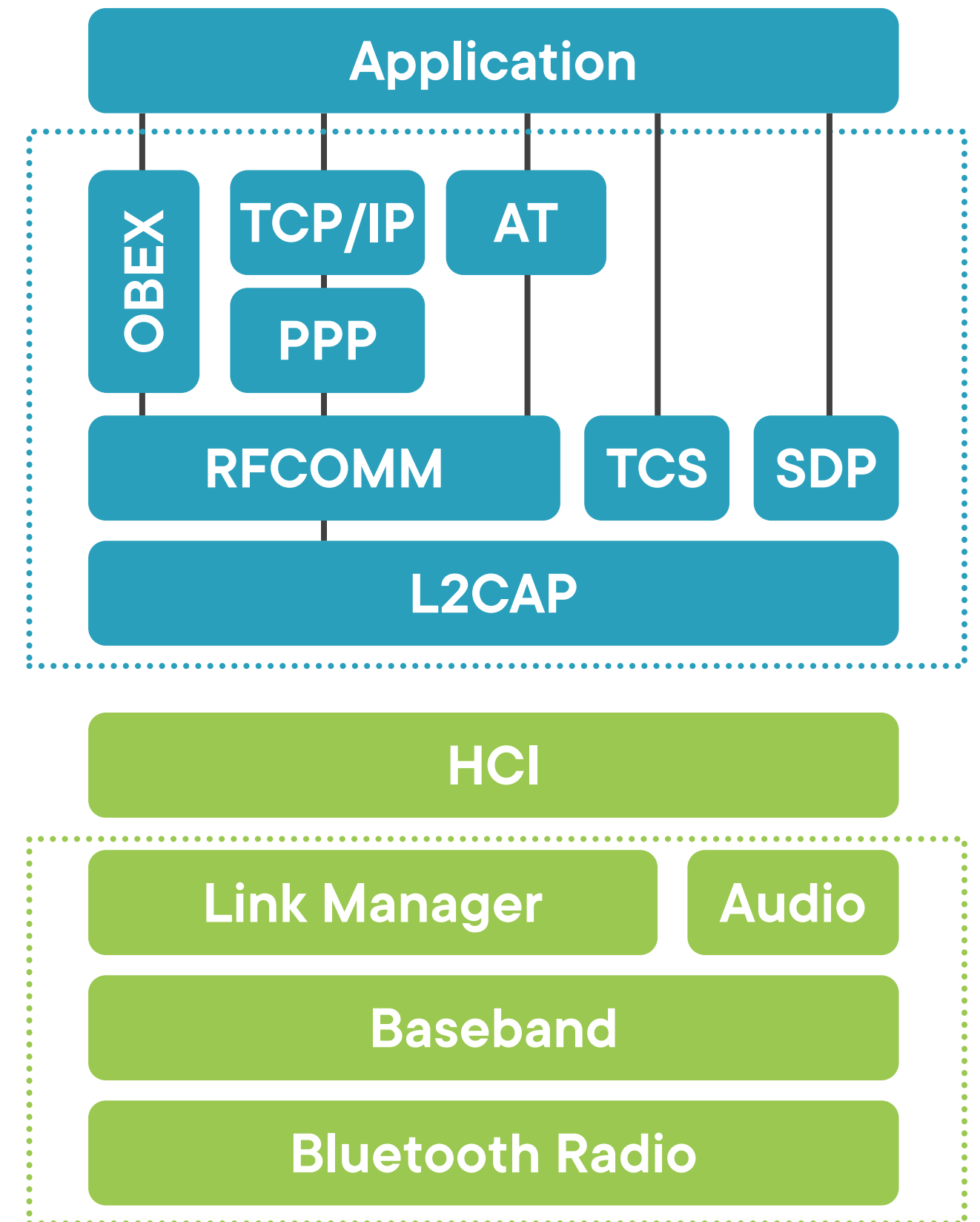
Bluetooth Stack

A Bluetooth stack refers to an implementation of the protocol stack.

It allows an inheritance application to work over Bluetooth.

Middleware
Protocol
Group

Transport
Protocol



Acronyms and Terms



Bluetooth Modes

Discoverable Modes

Discoverable

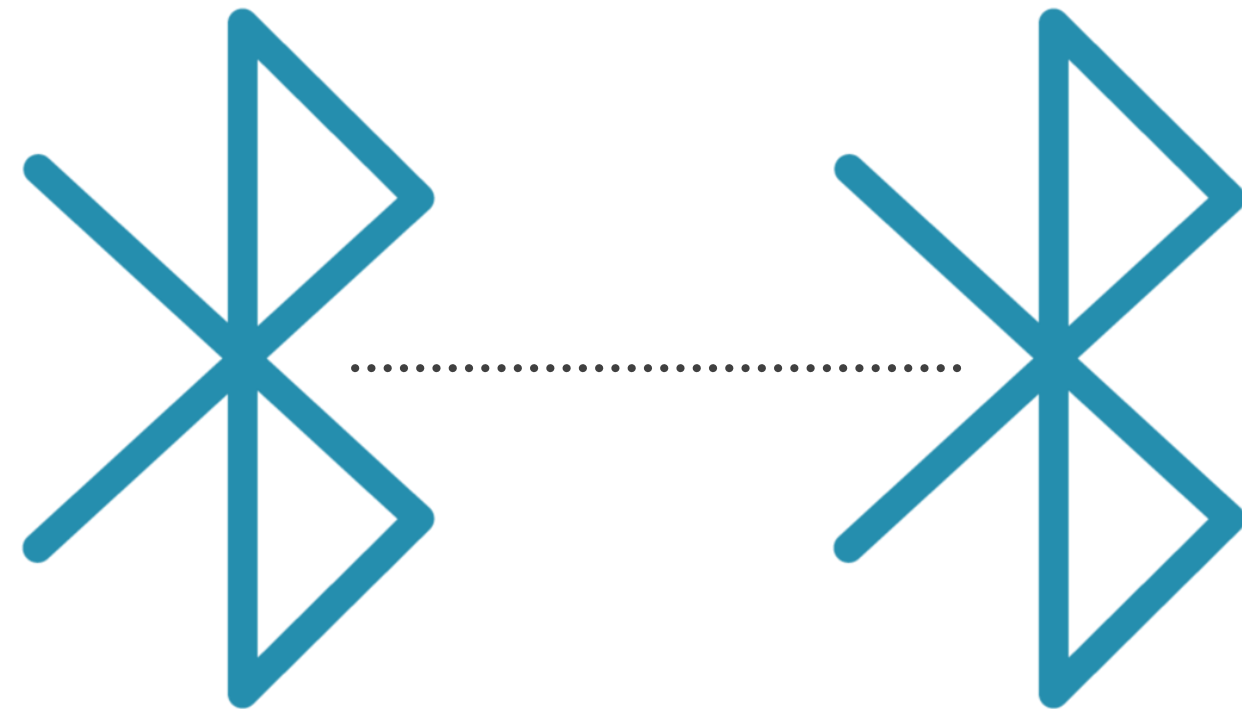
**Limited
discoverable**

Non-discoverable

Pairing Modes



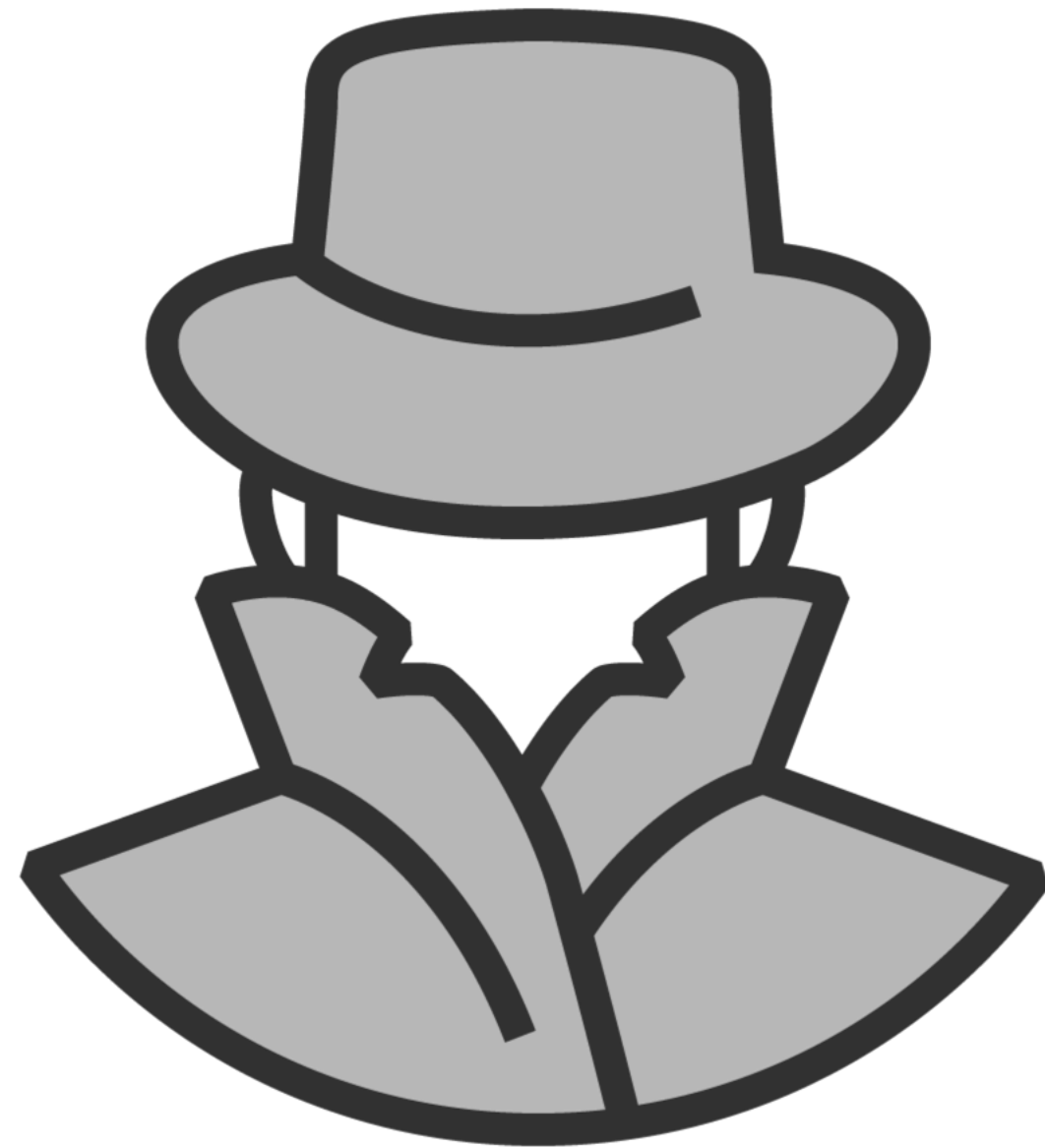
Non-pairing mode



Pairing mode

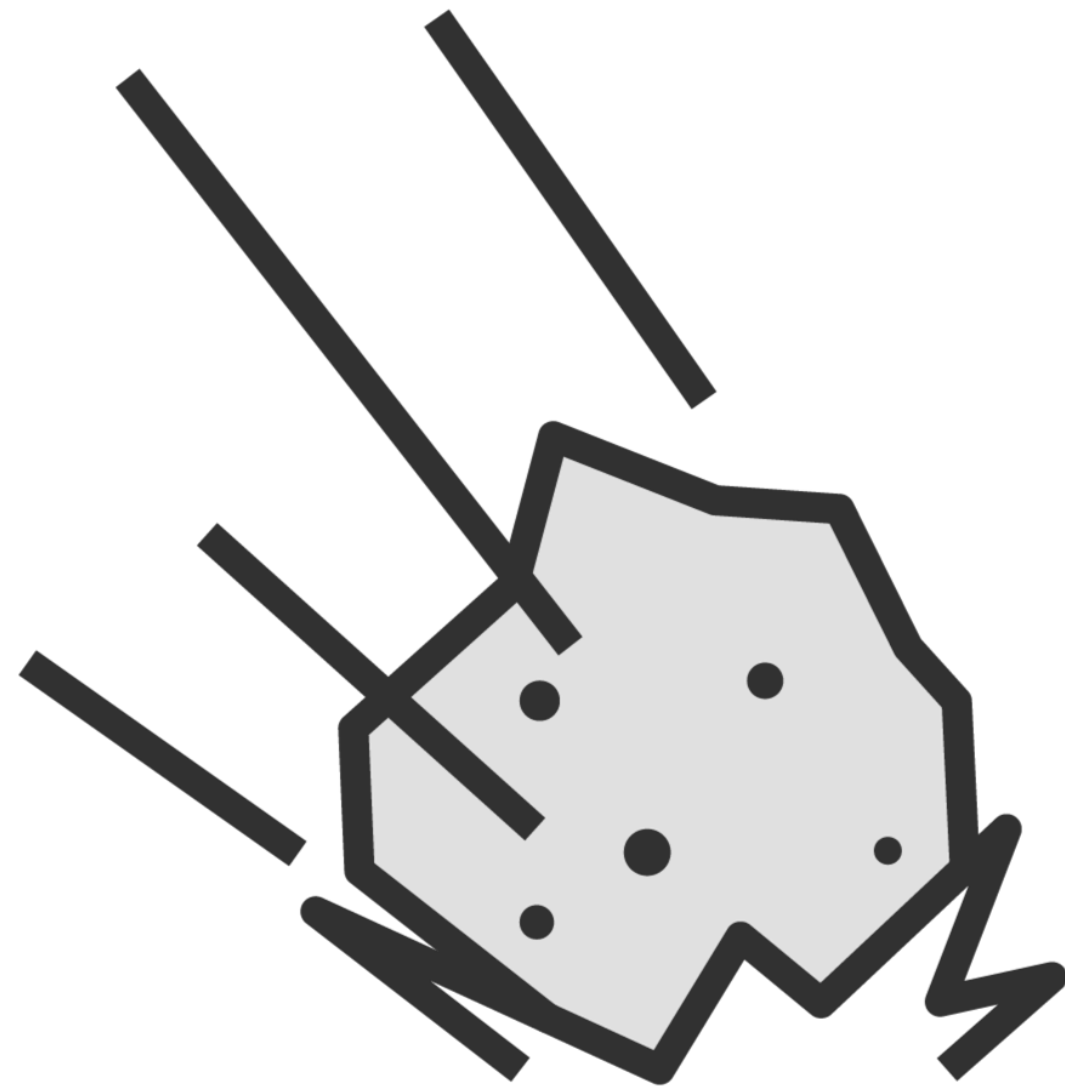
Methods of Attack

Bluetooth Hacking



Bluejacking

Bluetooth Hacking



Bluejacking

Bluesmacking

Bluetooth Hacking

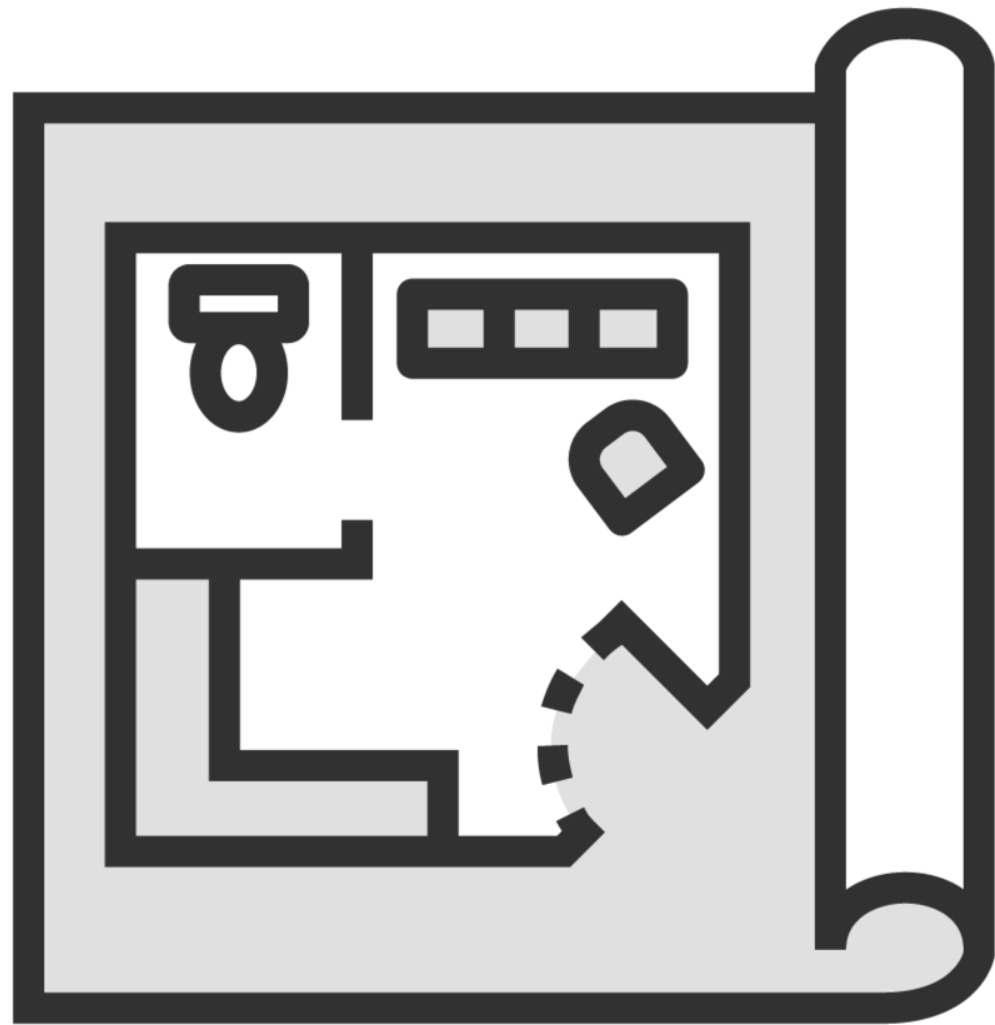


Bluejacking

Bluesmacking

Bluesnarfing

Bluetooth Hacking



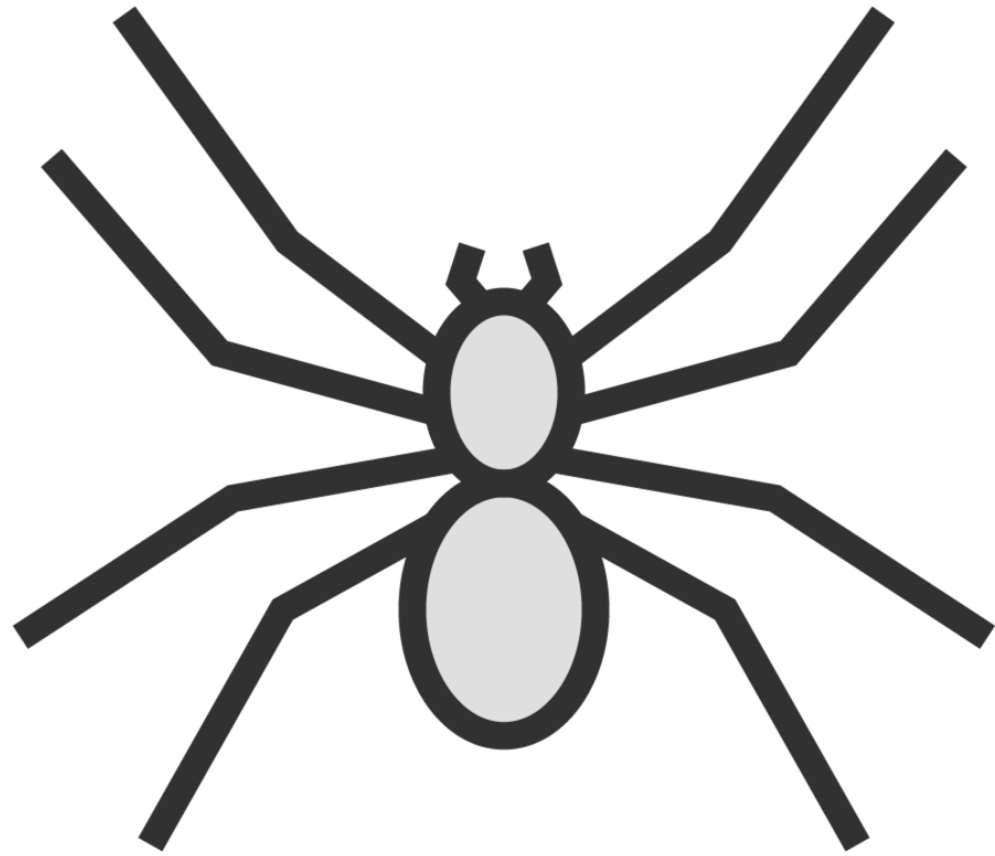
Bluejacking

Bluesmacking

Bluesnarfing

Blueprinting

Bluetooth Hacking



Bluejacking

Bluesmacking

Bluesnarfing

Blueprinting

Bluebugging

Bluetooth Hacking



Bluejacking

Bluesmacking

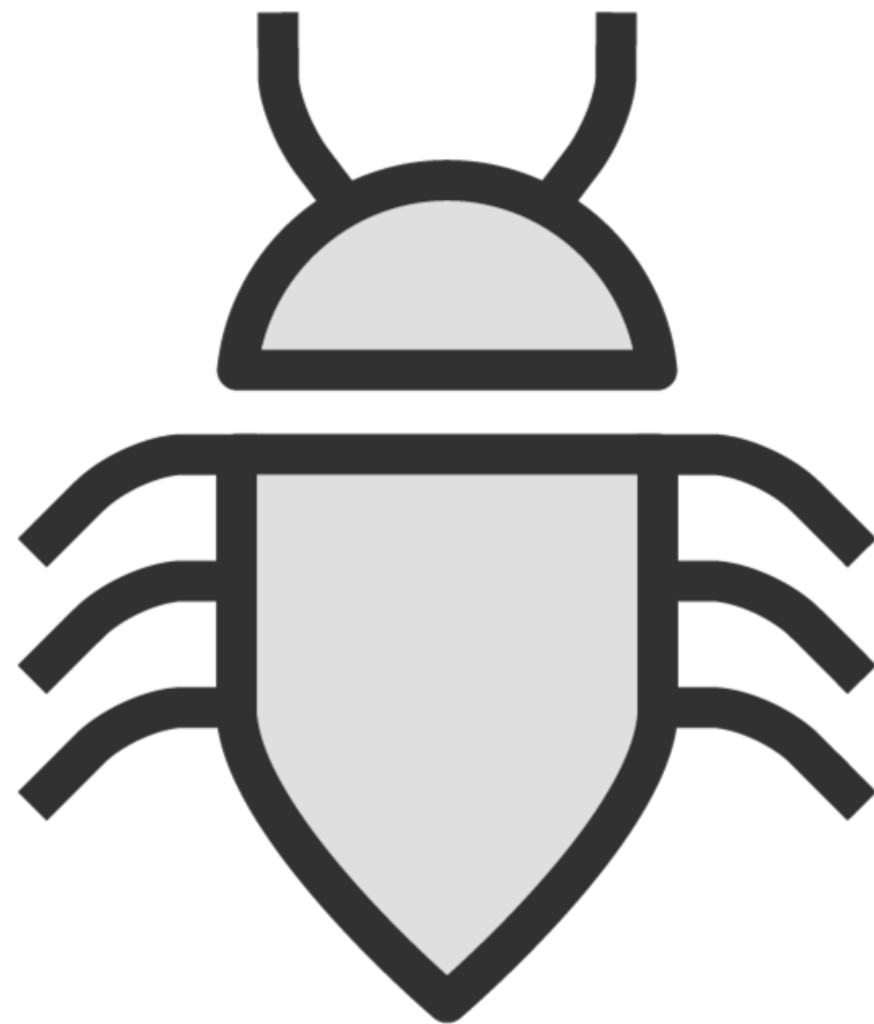
Bluesnarfing

Blueprinting

Bluebugging

BlueSniff

Bluetooth Hacking



Bluejacking

Bluesmacking

Bluesnarfing

Blueprinting

Bluebugging

BlueSniff

Btlejacking

Bluetooth Hacking



Bluejacking

Bluesmacking

Bluesnarfing

Blueprinting

Bluebugging

BlueSniff

Btlejacking

KNOB attack

Bluetooth Hacking



Bluejacking

Bluesmacking

Bluesnarfing

Blueprinting

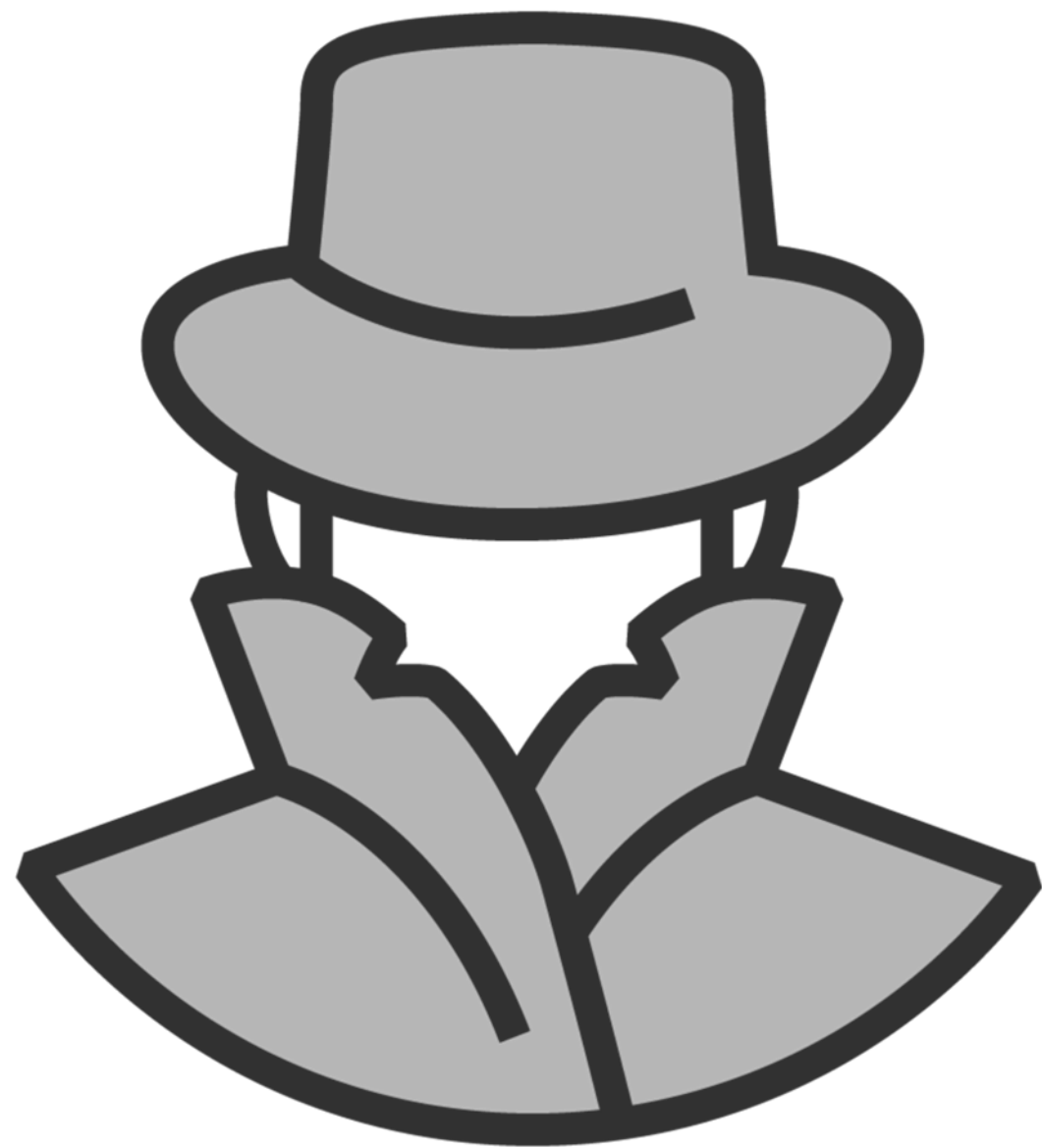
Bluebugging

BlueSniff

Btlejacking

KNOB attack

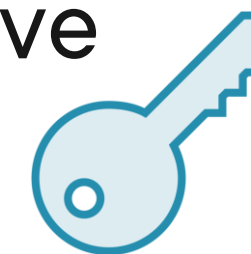
Person-In-The-Middle



Master



Slave



Bluetooth Threats

Bluetooth Threats



**Leakage of calendars
and address books**



Remote control



Bugging devices



Social engineering



Sending SMS messages



Malicious code



Causing financial losses



Protocol vulnerabilities

Demo



BluetoothView

Learning Check

Learning Check



Limited mode



Bluesmacking



Bluejacking



Bluesnarfing



KNOB



Up Next:

Distinguishing Wireless Countermeasures
