Bluetooth Attacks
(CSB20-15)

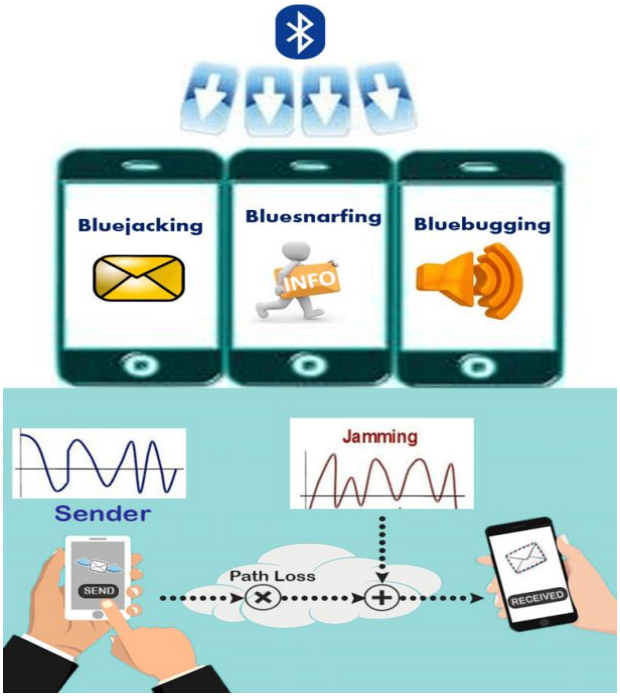
SUMMARY

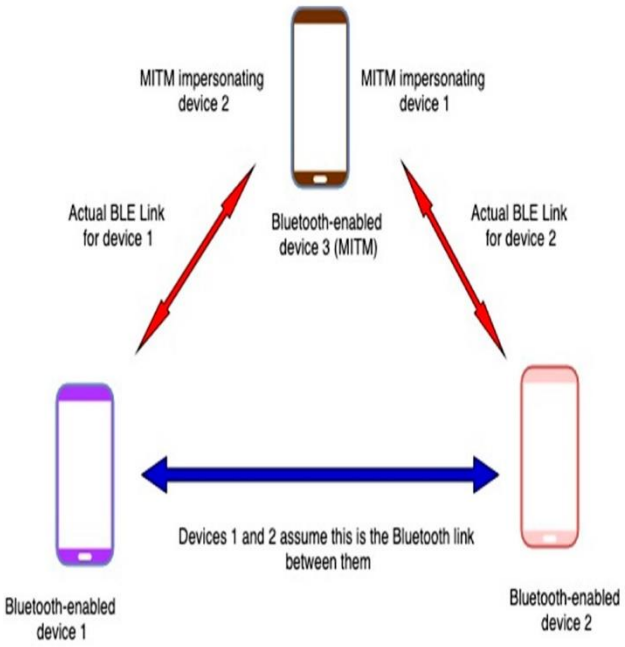
Bluetooth technology and associated devices like laptops, tablets, headsets and smartphones are susceptible to general wireless networking threats. Bluetooth attacks are made possible by the flaws in the Bluetooth Classics specification, any standard-compliant Bluetooth device can be expected to be vulnerable.

There are common Bluetooth attacks such as Bluejacking, Bluesnarfing and Bluebugging. Bluejacking is the sending of spontaneous messages over Bluetooth to Bluetooth-enabled devices. Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection. Bluebugging is a technique that allows skilled hackers to access mobile commands on Bluetooth-enabled devices that are in discoverable mode.

The attacker must establish a secure Bluetooth connection with two users attempting to connect, while pretending to be the other user, intercepting the data shared between them. They conduct BIAS attacks to bypass Bluetooth's authentication procedures that take place during the establishment of a connection. The flaws that are exploited in the attack include lack of integrity protection, encryption, and mutual authentication.

HOW IT WORKS





SECURITY RISK

Steal a great deal of data, spread worm virus or execute arbitrary code on the devices.

RECOMMENDATION

- Change the default PIN code and use a secured password;
- Turn off Discoverable/Visible Mode;
- Switch off Bluetooth when not in use; and
- Ensure that devices are updated to latest versions.

MITIGATIONS

- Minimize the range of devices to the shortest reasonable distance;
- Configure devices so that the user has to approve any connection request; and
- Install anti-virus and personal firewall software on Bluetooth devices.

REFERENCE

- https://www.webroot.com/us/en/
- https://www.techrepublic.com/article/secure-your-bluetooth-wireless-networks-and-protect-your-data/