Group Members
Salman Saeed: 6479018

Anishka Shetty: 6676431

Muneeb Ahmed: 7346091

Riely Benson: 6360507

Topic: Wireless Attack: Bluesnarfing and Blue jacking
Vulnerability, attack, and defence descriptions

Introduction:

In this report, we will showcase a well known wireless attack called "Bluesnarfing". This attack aims to steal data from any electronic device such as personal computers, cell phones and laptops that are enabled with Bluetooth.This is done through software that requests information from a device via Bluetooth (this device can be either in discoverable or non-discover-able mode). Once the phone is paired to the hackers device, the attacker will have access to personal data. This information can include one's contact list, calendar, e-mails and text messages. The report will also examine the deficiencies in security that can make devices prone to this attack, and highlight steps that can be taken to prevent a general theft of information attack.

Potential Tools

- Wireless device with bluetooth connection
- Blue Scanner - software to discover devices with Bluetooth connection and obtain information on the device

Expected Results

- Theft of text messages and emails
- Theft of contact list, along with personal information and data
- Sending unsolicited images, videos, messages, or data to other bluetooth enabled devices
- Ways to avoid a bluesnarfing attack would be to leave your bluetooth disabled when not in use, not accepting pairing requests from unknown contacts, and requiring approval for all contacts to pair