Report Submission

CON101- Introduction to Computer Science and Engineering

Indian Institute of Technology Delhi

Name: Deepanshu Entry Number: 2019CS50427 Group: 04

1 Introduction

Bluetooth is one of the most important aspect of wireless communication. It provides very cost effective solution for small range communication, though not very fast.
Not only mobile phones, it is also present in cars, headsets, security cameras, laptops and in many more devices.

2 Previously found attacks on bluetooth

2.1 Bluebugging

Bluebugging is one of the most dangerous and strong attack on any device. Bluebug allows an attacker to make phone calls, send and read messages, read and write contacts, change call settings and much more.
It is considered dangerous because of the immense "write access" it has. More advanced versions of bluebugging, if injecting in let say, self driving cars can take over the software system and control the movement of the vehicle which is never desirable and can prove to be fatal.
Confidentiality: High Integrity: High Availability: Moderate

2.2 Bluejacking

It sends unwanted messages to nearby open bluetooth device. Not to forget that mass spamming from a device can lead to abrubtly large phone bills, slowing down of the machine and much more.
It has very less writing access
Confidentiality: Low Integrity: High Availability: Moderate

2.3 Bluesnarf/Bluesnarf++

This works when the device is in discoverable mode. Bluesnarf allows attacker to access user information.

With bluesnarf++, attacker has full read and write access. What makes it even more dangerous is the fact that the attacker can remove/modify pivotal system files from the device.
Here also confidentiality is at high risk. Thus, it becomes as powerful as Bluebugging as far as modifying the data is concerned (because attacker gets write access apart from usual read access).
Confidentiality: High Integrity: High Availability: Low

3 Security measures enshrined in Bluetooth to prevent such attacks

Given that bluetooth surrounds most of the modern technology/devices, it is becomes even more important to look for various security measures to prevent these attacks.

1. **Authentication**
   The bluetooth device is verified before establishing any kind of wireless connection. This ensured all further verification/exchange of data is safe and secure.

2. **Confidentiality**
   It prevents the data ensures that only authorised device can read and write the data. It is one of the most important process as it helps in preventing Bluebugging and Bluesnarf++.

3. **Authorisation**
   For confidentiality to work fine, proper authorisation of devices is carried. It is done using cryptographic techniques and is often accompanied by encrypted key-lock matching technique.

Many advanced security models use different layers of verification. This can be achieved in various ways. For example authentication is encrypted and information is first encrypted, then sent to the device. There, it is decrypted and thus the information is received.

4 References

1. https://commons.erau.edu/cgi/viewcontent.cgi?article=1025&context=db-security-studies
2. https://blogs.getcertifiedgetahead.com/common-bluetooth-attacks/
3. https://www.researchgate.net/publication/326511381_Security_Vulnerabilities_in_Bluetooth_Technology_as_Used_in_IoT
4. https://www.researchgate.net/publication/225279567_Security_Threats_Analysis_in_Bluetooth-Enabled_Mobile_Devices
5. https://www.electronics-notes.com/articles/connectivity/bluetooth/security.php
6. https://www.mdpi.com/2224-2708/7/3/28/pdf