Attacks on Bluetooth devices and measures taken

October 2020

1 Introduction

Bluetooth is a wireless technology standard introduced on 7th May 1989 for exchanging data between compatible devices over short range. The range varies depending on the version and requirements (max range possible is 400m by Bluetooth 5(LE)). It uses UHF radio waves (2.402-2.480 GHz). Nowadays, the use of Bluetooth has increased tremendously. Almost every electronic device has Bluetooth now. Also the max range achieved by using antenna and signal amplifiers is 1.78km. So, the attacks on Bluetooth devices has also increased very much.

2 Attacks on Bluetooth

2.1 Bluesnarfing

It is the unauthorized access of data by use of Bluetooth. It can be done without the knowledge of user. Contact lists, emails, messages, calendars and in some phones pictures and videos can also be accessed. With this the confidentiality is totally lost.

2.2 Cabir worm

It is a malicious software which self-replicates. It tries to pair with another Bluetooth device. When pairing happens it gets transferred and installed in the target device. It drains the battery of the device. It can be detected by noticing that Bluetooth getting turned on automatically. Viruses that can be transferred by Bluetooth automatically first appeared in 2004 in mobile phones of Symbian OS, described by Kaspersky Lab. But it needed the permission of user for installation. In January 2005 a self-replicating worm known as Lasco began targeting Symbian OS. It infected .SIS files which made it possible to spread through hard drive also.

2.3 Bluetooth impersonation attacks (BIAS)

It is an attack discovered in 2020. It is the first type of attack that is able to bypass authentication procedures. It exploits the facts that, LSC authentication is not used mutually, devices can switch authentication role(master/slave). During pairing of devices, a long term key used is to connect the devices. In subsequent connections it uses a different session key extrapolated from long term key and other public factors. Using this flaw, the attackers can impersonate the devices.

3 Security measures taken to prevent attacks

SSP pairing method was introduced. It uses Elliptic Curve Diffie HeIlman techniques. In SSP a link key is shared between 2 devices. It authenticates two devices and creates a temporary encryption code which is used to encrypt and decrypt the data shared.

In addition to authentication and encryption, authorisation was introduced in Bluetooth 2.1. Authorisation is checking whether the device is authorised to access a particular service. By doing so it is possible to provide access to only a few services.

From version 3+ alternative MACs was used for transporting Bluetooth profile data and large data. When large data must be sent other MAC PHY transports the data.

Length of keys were extended with limited discovery time so that time available for hacking is very much reduced.

4 References

Wikipedia, Bluetooth
Amer Owaida, Bluetooth flaw exposes countless devices to BIAS attacks
Stephanie Ho, Brian Ng, Justin Kwong and Frank Wu, Security Analysis of Bluetooth Enabled Mobile Devices