



A Guide For
Bluetooth

The United States Internet Crime Task Force, Inc.
A Non-Profit / Government-Assist / Victim Advocate Agency

Securing Your Bluetooth Device

Bluetooth Security

- 1.) Introduction
- 2.) Bluetooth Attacks
- 3.) Safeguarding Your Device

Securing Your Bluetooth Device

Introduction

Since its inception more than a decade ago, Bluetooth technology has become a prevalent feature in a wide array of consumer electronics. As technology grows in power and reduces in size, people all over the world are becoming free to work (or even play) without the need for cables, wires, or any other sort of tether between the devices they carry. This freedom provides an essential means for users to multitask on the go, but the very leisure we depend on everyday may also serve as a window of opportunity for tech savvy predators that lurk in public places.

Bluetooth enabled devices often contain a wealth of knowledge about the user. Some devices have stored pictures, contact information, calendars, and other personal data that the user of the device intends to keep private. More often than not, the information is stored on a cellular phone, which is almost always a Class 2 Bluetooth device with an operating range of approximately 30 meters. While this approximate range is a seemingly small radius of danger, most users go unaware of vulnerabilities that expose their personal information to the public at large.

Remember that a cellular phone might have a Bluetooth range of about 30 meters, which isn't much, but pales in comparison to the power of a Class 1 Bluetooth antenna which may be installed in a laptop. The range of a Class 1 Bluetooth device can be up to 100 meters, which is quite a large area of operations for a malicious user.

To set the scene, imagine that you are on a business trip and that you are waiting at the airport for your plane to begin boarding. You sit in the terminal and begin making calls on your Bluetooth enabled cellular phone. You pair your phone and your headset and begin your conversation. Without your knowledge, someone with a laptop sits nearby with a mind to make mischief with your phone. This malicious user has a plethora of harmful options for your device. He or she, can redirect your calls to international numbers, steal your address book, view your pictures, copy your calendar, and even listen in on the calls you are making. All of this can be done without you even knowing it took place, and this is not the complete extent wrongdoing that can be performed against you and your device.

The following pages will provide a detailed description of the various attacks that can be performed on a typical Bluetooth enable device, with recommendations for protecting yourself and your device against these specific vulnerabilities. For more information about this and other security related issues, visit the United States Internet Crime Task Force, Inc. website at www.usict.org.

Attacks Against Your Bluetooth Enable Device

This section will provide you with information about the types of attacks that can be carried out on your Bluetooth enabled device. Keep in mind that not every Bluetooth device is susceptible for every attack, and that certain attacks can have serious repercussions for the affected users (especially in respect to identity theft).

Backdoor Attack: Every Bluetooth user knows about “pairing”, which is the action of linking two Bluetooth capable devices for the purpose of transferring data. This attack is carried out through this specific pairing mechanism by establishing a trust relationship between the user’s device and the attacker’s laptop or PDA. The pairing process in this attack does not appear on the target handheld, so the attack goes on without notice unless the user happens to be looking at the device during the establishment of the connection. Once the connection is made, the attacker is free to access any resource the target device can provide via Bluetooth. This can be a variety of different resources such as data transfer, cellular calls, GPS services, and Internet access that are all now exposed to the attacker and are readily available for his or her use.

Bluebug Attack: This type of vulnerability can allow an attacker to create a serial connection to the target device. Once the connection is established, the attacker would have access to the various communication functions of the target device. The attacker could then initiate calls (sometimes to international or pay per minute numbers), forward calls, send and receive SMS messages, connect to the Internet, and even monitor calls on a GSM phone. Attacks of this nature can often provide the attacker with the tools he or she will need to steal your identity, and possibly cause damage to the user, financially.

Bluejacking: This is not always an attack; so much as it is a barrage of marketing material sent to your Bluetooth device. When you pair Bluetooth devices a message will normally appear on your handset. The message can be up to 248 characters in length, and is often abused by others as a method of sending messages to your device. Your device will display the message and then ask you for permission to pair your device with the attacker. This can be a precursor to other attacks, especially if the message tells you that you have won something, and goes on to say that you need to input a specific four digit code to collect your prize. If you were to type in this four digit code (the pairing passcode) your device would then be open for any of the other attacks.

Bluesnarfing: The term “snarf” means (in the relative context), to take a large document or file for the purpose of using it with or without the author's expressed permission. This definition is befitting of this type of attack, as that is generally what takes place. On many Bluetooth devices, it is possible to complete the pairing process without informing the user of the “target” handheld. Once the connection is established, the attacker can gain access to restricted information. This information can be anything from pictures, files, contacts, device settings, calendar information, as well as serial and SIM numbers that uniquely identify your phone.

Denial Of Service (DOS): These types of attacks serve only to be annoyance to the target user’s device. The attacker can use his or her Bluetooth device to send a flurry of pairing requests to the user’s Bluetooth handset. Since no information is exchanged and the range of Bluetooth technology is limited, the attack will never do much damage. It can however temporarily paralyze a phone or PDA and cause a notable drain on the battery as well.

Preventing Bluetooth Attacks

There are several different ways to prevent your device from being the target of any of the attacks launch via Bluetooth. Listed below are some good practices that will keep your device and the information you have stored on it safe.

Know your environment: Examine the area you are in, and use common sense. If you are in a public area where there are a great number of people with laptops or PDAs (like an airport terminal) you may want to take immediate precautions to secure your device from unauthorized access.

Be ‘invisible’: By turning off the discovery option in your Bluetooth settings, you will not appear visible to many different methods of detection. While there are ways to find Bluetooth devices that do not allow discovery, this practice will drastically reduce the possibility of your device becoming a target.

Abstinence is best: If you feel that the environment you are in poses a great enough risk, the best thing you can do is turn off the Bluetooth radio on your device. You will only need to do this for the duration of your time in the unsafe area, or until you feel that you are out of the range of any possible attack.

More information can be found at the following sites:

Official Bluetooth Website: www.bluetooth.com

United States Internet Crime Task Force, Inc. Website: www.usict.org

