

# ***Bluetooth Security Notes***

Paul Day, paul (at) bur.st, 04/08/04

## **REVISION CONTROL**

- Paul Day, 04/08/04, Initial draft
- Paul Day, 25/08/04, Final revision
- Paul Day, 26/08/04, included generic intro to BT and more Windows examples

## **1- INTENDED AUDIENCE**

- Any user of Bluetooth

## **2- INTRODUCTION**

This document is intended to:

- Introduce Bluetooth and its capabilities
- Highlight security drawbacks and vulnerabilities in devices and computers with Bluetooth enabled
- Outline measures that can be taken to minimize your vulnerability from the use of Bluetooth

## **3- INTRODUCTION TO BLUETOOTH AND ITS USE**

Bluetooth is a radio (2.4Ghz) data technology that allows a user to wirelessly connect numerous personal devices to allow communication between them all. Bluetooth achieves what is sometimes referred to as a Personal Area Network (PAN) allowing you to, for example, have your mobile phone, hands-free kit and laptop computer all communicating wirelessly.

Bluetooth is an industry specification defined by the Bluetooth Special Interest Group (SIG), which is a group of approximately 2000 members who design and manufacture Bluetooth-enabled products.

Products containing Bluetooth technology include computers, headsets, keyboards and mice, printers, handheld computers, mobile phones, digital cameras and GPS units.

Common uses of Bluetooth include:

- Use a wireless mouse and keyboard with your PC.
- Use a wireless mobile phone headset while leaving your phone in your pocket.
- Synchronise personal data between your palm computer, your laptop and your mobile phone.
- Copy pictures off your digital camera to your desktop computer.

Bluetooth has a number of built-in security mechanisms:

- Shared key between devices
- Encryption of data
- Ability to remain hidden while searching

These security mechanisms, and a number of issues they currently possess, are discussed below.

## **4- SECURITY VULNERABILITIES WITH BLUETOOTH**

### ***4.1-- Automatic file sharing of sensitive data by some vendors***

A number of computer operating systems share a folder or drive out via Bluetooth by default, for read-only access or read/write access. eg, MacOSX automatically shares out the “Shared” folder for reading and allows people to write files to the “Drop Box” folder by default.

Some users are unwittingly using the shared folders for storage of personal or sensitive data, allowing an attacker to easily gain access to the files.

### ***4.2- Lack of authentication in Object Exchange (OBEX)***

Many mobile phone manufacturers have decided that Bluetooth authentication is not necessary in OBEX to aid easy exchange of business cards from phone to phone. Unfortunately, this also allows an attacker to easily gain access to other files and personal information stored on the phone, such as:

- entire phonebook
- calendar
- real-time clock
- business card
- properties<sup>1</sup>

An attacker may also then:

- Initiate a phone call
- Write a phone book entry
- Send an SMS (Short Message Service)/text message

via other methods.

---

<sup>1</sup> “Serious flaws in Bluetooth security lead to disclosure of personal data “, Adam Laurie of A.L. Digital Ltd. , <http://www.thebunker.net/release-bluestumbler.htm>

Exploiting this vulnerability is commonly referred to as snarfing, bluesnarfing or bluejacking. Some manufacturers have since released updated firmwares for their phones to address it.

While most devices are only vulnerable to this attack while in “visible” mode, there are techniques to allow an attacker to find a device that is in invisible/hidden mode.

#### ***4.3- Deleted paired device still having full access***

Some devices leave all credentials after deleting a pairing which allows the deleted paired device to still connect as normal. To the user, the device does not appear as “trusted” in a list of devices, however the attacker may still have full access via Bluetooth.

An attacker may quickly take the device from the owner, pair the attacking device, delete the pairing so it is no longer visible to the owner, return the device and still have full ability to connect to the owner’s device without their knowledge.

This is commonly referred to as the backdoor attack. The attacker is then free to continue using your device as if s/he has full access to it. Data can be retrieved from your computer or a mobile phone can be used as a WAP or GPRS data gateway without your knowledge.

#### ***4.4- The bluebug attack***

The above two attack methods can also be used to establish a serial profile with your device, known as the bluebug attack. This gives the attacker full access to resources shared by the device over serial. eg, a mobile phone can be used to make phone calls using the AT command set or a laptop computer could have your PDA’s data stolen onto an empty PDA owned by the attacker.

#### ***4.5- Discovery of undiscoverable devices***

There are also tools available, such as @stake’s RedFang, which allow brute-force discovery of hidden or undiscoverable devices. “Hidden” or “undiscoverable” mode may stop your device from broadcasting its presence, however it will still respond to a number of requests, allowing brute-force discovery of it.

Some manufacturers claim this would take an unreasonable amount of time (eg, 11 hours). However, a multi-threaded version of RedFang could simultaneously utilize up to 8 USB Bluetooth devices which would reduce the 11hrs to approximately 90 minutes (based on one vendor’s range)<sup>2</sup>.

---

<sup>2</sup> “War Nibbling: Bluetooth Insecurity”, Ollie Whitehouse, @stake

## **5- SUGGESTED ACTIONS TO SECURE BLUETOOTH**

While the examples given are only for an Ericsson T610 mobile phone and computers running Apple MacOSX 10.3 or Microsoft Windows XP, the actions and ideas themselves apply to all Bluetooth-enabled devices.

### **5.1- Turn it off!**

If you're not actively using the Bluetooth connection on your device or computer, you should disable the Bluetooth adapter. Not only is this more secure, it will considerably reduce battery consumption on devices such as a phone.

*On an Ericsson T610 mobile phone:* Menu -> Connectivity -> Bluetooth -> Turn Off

*On a MacOSX 10.3 computer:* Apple menu -> System Preferences -> Bluetooth -> Settings -> "Turn Bluetooth Off"

*On a WinXP computer:* Start menu -> Control Panel -> Bluetooth Configuration -> Accessibility -> untick "Let other Bluetooth devices to discover this computer" -> Allow menu, choose "No devices to connect"

If you're actively using the Bluetooth connection in your device, take the following precautions to minimize your risk:

### **5.2- Ensure you have the latest Bluetooth firmware and device drivers on all devices**

Nokia and Sony Ericsson have both released newer firmwares for their phones in the first half of 2004 to address the issue of bluesnarfing. Contact your manufacturer's telephone support to organise a software upgrade on your phone.

Owners of computers, notebooks and palm computers with Bluetooth hardware should check the website of the manufacturer of their computer or Bluetooth adapter for the latest software drivers and latest Bluetooth firmware.

### **5.3- Put the device in hidden/invisible mode**

Your devices only need to be in "visible" or "discoverable" mode when pairing them with your other Bluetooth devices. Once you have paired your devices (headset to phone, mouse to computer, Palm computer to laptop) you should disable the visibility of your device.

Once paired, devices are still able to communicate even when not in discoverable mode.

*On an Ericsson T610 mobile phone:* Menu -> Connectivity -> Bluetooth -> Options -> Visibility -> Hide phone

*On a MacOSX 10.3 computer:* Apple menu -> System Preferences -> Bluetooth -> Settings -> untick "Discoverable"

*On a WinXP computer:* Start menu -> Control Panel -> Bluetooth Configuration -> Accessibility -> untick "Let other Bluetooth devices to discover this computer"

#### **5.4- Turn on authentication**

Once Bluetooth authentication is on, devices generally (there are vulnerabilities in some vendor's implementations of Bluetooth) need to then use a common password to pair with another device.

*On a MacOSX 10.3 computer:* Apple menu -> System Preferences -> Bluetooth -> Settings -> tick "Require Authentication"

*On a WinXP computer:* Start menu -> Control Panel -> Bluetooth Configuration -> General -> security -> choose "High" from drop-down menu

#### **5.5- Turn on encryption**

Turning on Bluetooth encryption means that the majority of data transmitted between the two Bluetooth devices is encrypted with a common key. This makes it difficult for a third party to sniff the data or use recorded data in "replay attacks".

*On a MacOSX 10.3 computer:* Apple menu -> System Preferences -> Bluetooth -> Settings -> tick "Require Authentication" -> tick "Use Encryption"

*On a WinXP computer:* Start menu -> Control Panel -> Bluetooth Configuration -> General -> security -> choose "High" from drop-down menu

#### **5.6- Do not allow auto-acceptance of files**

It is best to always be asked by your device when accepting a file so that you don't unwittingly allow a dangerous file or Trojan to be automatically uploaded.

*On a MacOSX 10.3 computer:* Apple menu -> System Preferences -> Bluetooth -> File Exchange -> "When receiving items:" -> Choose "Prompt for each file" -> "When PIM items are accepted" and "When other items are accepted:" -> Choose "Ask"

#### **5.7- Disable file shares**

If you do not actively share files from the Bluetooth device to your other devices, disable all sharing (read-only and read/write) of files.

*On a MacOSX 10.3 computer:* Apple menu -> System Preferences -> Bluetooth -> File Exchange -> untick "Allow other devices to browse files on this computer"

*On a WinXP computer:* Start menu -> Control Panel -> Bluetooth Configuration -> Information Exchange -> remove the "Shared Directory"

#### **5.8- Permanently remove pairings**

To ensure there are no "hidden" pairings in your device, it is best to do a factory reset of it. Unfortunately, this may not be convenient.

Computer users may wish to delve into the registry or settings files of their operating system to ensure that there are no extra device pairings present.

### **5.9- Do not pair with unknown devices or give up physical access to your device**

To alleviate the chances of an attacker pairing with your device (and then potentially hiding the pairing by “deleting” it), do not pair with an unknown device or allow physical access to your device to any un-trusted party.

### **5.10- Do not ever assume you’re “out-of-range”**

While commodity devices come with low-power transmitters and very poor antennas, resulting in usage areas of only a few meters, there are number of other items on the market which allow an attacker to extend the range of Bluetooth:

- High-gain directional antennas for the 2.4Ghz band can be easily made or purchased.
- Higher-powered Bluetooth adapters can be easily purchased.

## **6- CONCLUSIONS**

While Bluetooth does introduce a number of vulnerabilities to a user’s devices and data, there are number of methods that will dramatically reduce your risk.

After going through the suggestions above, the user must then weigh up the convenience of using Bluetooth vs the relatively small remaining risk.

It is hoped that manufacturers will address remaining vendor-specific issues in their Bluetooth implementations in future releases of software and or firmware. A number of vulnerabilities (eg, short time to brute-force discovery of hidden devices) have also been addressed in the upcoming release of Bluetooth version 1.2 by the Bluetooth SIG.

## **7- BIBLIOGRAPHY**

“BlueBug”, Martin Herfurt of Herfurt Salzburg Research Forschungsgesellschaft mbH, Austria , [http://agentsmith.salzburgresearch.at/agentsmith\\_projects\\_bluebug.html](http://agentsmith.salzburgresearch.at/agentsmith_projects_bluebug.html)

“Bluesnarfing @ CeBIT 2004 - Detecting and Attacking enabled-enabled Cellphones at the Hannover Fairground”, Martin Herfurt of Salzburg Research Forschungsgesellschaft mbH, Austria, [http://agentsmith.salzburgresearch.at/Downloads/BlueSnarf\\_CeBIT2004.pdf](http://agentsmith.salzburgresearch.at/Downloads/BlueSnarf_CeBIT2004.pdf)

“Bluetooth - The Official Bluetooth Membership Site”, Bluetooth Special Interest Group, <https://www.bluetooth.org/>

“Serious flaws in Bluetooth security lead to disclosure of personal data “, Adam Laurie of A.L. Digital Ltd. , <http://www.thebunker.net/release-bluestumbler.htm>

“War Nibbling: Bluetooth Insecurity”, Ollie Whitehouse of @stake, October 2003, [http://www.atstake.com/research/reports/acrobat/atstake\\_war\\_nibbling.pdf](http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf)