Bluetooth SIG Shop | Bluetooth.org

search site enter keywords here search

Learn
Bluetooth Basics
Benefits of *Bluetooth* Technology
How *Bluetooth* Works
Bluetooth Technology
Security
Device Protection
Glossary
Connect
Apply
About the Bluetooth SIG
Press & Analysts

Bluetooth Assembler

Wireless Security

Security

Today's wireless world means that data is being sent, among us, invisibly from device to device, country to country, person to person. This data, in the form of e-mails, photos, contacts and addresses are precious and private to each of us. This private information, no longer making its way along wires in plain sight, needs to be sent securely to its intended recipient without interception. Wireless standards the world over are evolving and have various formats for dealing with the security issues of its users. *Bluetooth* wireless technology is no exception.

Bluetooth wireless technology has, from its inception, put great emphasis on wireless security so that users of this global standard can feel secure while making their connections. The Bluetooth Special Interest Group (SIG), made up of over 4000 member manufacturers, has a *Bluetooth* security experts group made up of engineers from its member companies who provide critical security information and feedback that is taken into account as the *Bluetooth* wireless specification evolves.

Product developers that use *Bluetooth* wireless technology in their products have several options for implementing security. There are three modes of security for *Bluetooth* access between two devices.

> Security Mode 1: non-secure
> Security Mode 2: service level enforced security
> Security Mode 3: link level enforced security

The manufacturer of each product determines these security modes. Devices and services also have different security levels. For devices, there are two levels: "trusted device" and "untrusted device." A trusted device, having been paired with one's other device, has unrestricted access to all services.With regard to services, three security levels are defined: services that require authorization and authentication, services that require authentication only and services that are open to all devices.

Lately, confusion and misinformation surrounding security and *Bluetooth* wireless technology has increased. The current security issues typically involve mobile phones. How these issues apply to other classes of devices is important and is often not addressed. The encryption algorithm in the *Bluetooth* specifications is secure. This includes devices such as mice and keyboards connecting to a PC, a mobile phone synchronizing with a PC, and a PDA using a mobile phone as a modem to name just a few of the many use cases.

Cases where data has been compromised on mobile phones are the result of implementation issues on that platform. The Bluetooth SIG diligently works with our members to investigate any issues that are reported to understand the root cause of the issue. If it is a specification issue, we work with the membership to get patches out and ensure future devices don't suffer from the same vulnerability. This is an on-going process. The recently reported issues of advanced "hackers" gaining access to information stored on select mobile phones using *Bluetooth* functionality are due to incorrect implementation. The names bluesnarfing and bluebugging have been given to these methods of illegal and improper access to information. The questions and answers below provide users with more information about these current issues and will address their concerns for dealing with these security risks.

What is bluejacking?
Bluejacking allows phone users to send business cards anonymously using *Bluetooth* wireless technology. Bluejacking does NOT involve the removal or alteration of any data from the device. These business cards often have a clever or flirtatious message rather than the typical name and phone number. Bluejackers often look for the receiving phone to ping or the user to react. They then send another, more personal message to that device. Once again, in order to carry out a bluejacking, the sending and receiving devices must be within 10 meters of one another. Phone owners who receive bluejack messages should refuse to add the contacts to their address book. Devices that are set in non-discoverable mode are not susceptible to bluejacking.

What is bluebugging?
Bluebugging allows skilled individuals to access the mobile phone commands using *Bluetooth* wireless technology without notifying or alerting the phone's user. This vulnerability allows the hacker to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet. As with all the attacks, without specialized equipment, the hacker must be within a 10 meter range of the phone. This is a separate vulnerability from bluesnarfing and does not affect all of the same phones as bluesnarfing.

What is bluesnarfing?
Bluesnarfing allows hackers to gain access to data stored on a *Bluetooth* enabled phone using *Bluetooth* wireless technology without alerting the phone's user of the connection made to the device. The information that can be accessed in this manner includes the phonebook and associated images, calendar, and IMEI (international mobile equipment identity). By setting the device in non-discoverable, it becomes significantly more difficult to find and attack the device. Without specialized equipment the hacker must be within a 10 meter range of the device while running a device with specialized software. Only specific older *Bluetooth* enabled phones are susceptible to bluesnarfing.

What are phone manufacturers doing to address the situation?
Both Nokia and Sony Ericsson have developed software upgrades for phones vulnerable to bluesnarfing and bluebugging. Both companies have also worked hard to make sure new phones coming to market will not be susceptible to these attacks. For more information on how users can obtain applicable software upgrades for their phones, visit the websites of Sony Ericsson and Nokia.

What is Car Whisperer?
The car whisperer is a software tool developed by security researchers to connect to and send or receive audio to and from *Bluetooth* car-kits with a specific implementation. An individual using the tool could potentially remotely connect to and communicate with a car from an unauthorized remote device, sending audio to the speakers and receiving audio from the microphone in the remote device. Without specialized equipment, someone using the tool must be within a 10 meter range of the targeted car while running a laptop with the car whisperer tool. The security researchers' goal was to highlight an implementation weakness in a select number of *Bluetooth* enabled car-kits and pressure manufacturers to better secure *Bluetooth* enabled devices.

How can I tell if my car kit or car is vulnerable to the car whisperer?
To be accessed by the car whisperer tool, the car-kit needs to be continuously in pairing mode, have a standard fixed four digit PIN code and not be connected to a phone. If a user consistently has a phone paired with the car kit, an unauthorized device cannot connect to the car kit. Concerned individuals, whose car kits are continuously in pairing mode and have a standard fixed four digit PIN code (i.e. 0000 or 1234), should contact the manufacturer directly for more information on the vulnerability of their devices and to obtain applicable software upgrades for their car-kits.

Is *Bluetooth* wireless technology susceptible to hackers in other ways?
Currently, the attacks listed on this page are the only known possibilities for hacking into a limited amount of products on the market, if appropriate measures are taken such as having security turned on and using reasonably long PIN codes or pairing devices in private. The Bluetooth SIG continues to study security risks associated with the technology and determine their viability as the technology spreads and develops.

What can consumers do to protect their data?
Consumers can do a number of things to protect their data. If users have a phone that is vulnerable to bluesnarfing or bluebugging, they should contact the phone's manufacturer or take the phone to a manufacturer authorized service point. The manufacturers of the vulnerable devices have developed software patches to fix the

vulnerability. In addition, if users are still concerned about a device being targeted, they can turn the device to non-discoverable mode when not using *Bluetooth* wireless technology and in unknown areas. Users can also ensure their data is secure by not "pairing" with unknown devices. If a user were to receive an invitation to pair with another device, and asked to put in a PIN code, but was unsure of what device was inviting to pair, the user should not pair. Only pair with known devices.

What is the cabir worm? Which devices does the cabir worm affect?
The cabir worm is malicious software, also known as malware. When installed on a phone, it uses *Bluetooth* technology to send itself to other similarly vulnerable devices. Due to this self-replicating behavior, it is classified as a worm. The cabir worm currently only affects mobile phones that use the Symbian series 60 user interface platform and feature *Bluetooth* wireless technology. Furthermore, the user has to manually accept the worm and install the malware in order to infect the phone. More information on the cabir worm is available from the software licensing company Symbian and on the websites of F-Secure, McAfee and Symantec.

How does a PIN affect security?
The personal identification number (PIN) is a four or more digit alphanumeric code that is temporarily associated with one's products for the purposes of a one time secure pairing. It is recommended that users employ at minimum an eight character or more alphanumeric PIN when possible. Product owners must share that PIN number only with trusted individuals and trusted products for pairing. Without this PIN number, pairing cannot occur. It is always advisable to pair products in areas with relative privacy. Avoid pairing your *Bluetooth* enabled devices in public. If, for some reason, your devices become unpaired, wait until you are in a secure, private location before repairing your devices.

Do I need to remember my PIN?
No. It is not necessary to remember your PIN except in the seldom situation when the PIN is a fixed PIN - in which case simply retaining the user manual, with given PIN, for future reference is advisable.

Why does pairing in a public location potentially introduce a security risk?
Theoretically a hacker can monitor and record activities in the frequency spectrum and then use a computer to regenerate the PIN codes being exchanged. This requires specially built hardware and thorough knowledge of *Bluetooth* systems. By using a PIN code with eight or more alphanumeric characters it would take the hacker years to discover the PIN. By using a four digit numeric PIN code, the hacker could discover the PIN in a matter of a few hours. Still advanced software is required.

Is this a real risk to *Bluetooth* enabled devices?
Bluetooth devices generate a secure connection by means of the initial pairing process. During this process one or both devices need a PIN code to be entered, which is used by internal algorithms to generate a secure key, which is then used to authenticate the devices whenever they connect in the future.

A new academic paper puts forward a theoretical process that could potentially "guess" the security settings on a pair of *Bluetooth* devices. To do this the attacking device would need to listen in to the initial one-time pairing process. From this point it can use an algorithm to guess the security key and masquerade as the other *Bluetooth* device. What is new in this paper is an approach that forces a new pairing sequence to be conducted between the two devices and an improved method of performing the guessing process, which brings the time down significantly from previous attacks.

To perform this hack, it is necessary for the attacker to overhear the initial pairing process, which normally only happens once in a private environment and takes a fraction of a second. The authors have put forward some possible methods to try and force a deletion of the security key in one of the two *Bluetooth* devices, and hence initiate a new pairing process, which they could then listen in to. To do this, they need to masquerade as the second device during a connection. The equipment needed for this process is very expensive and usually used by developers only. If this process succeeds the user will see a message on their device that asks them to re-enter a PIN code. If they do this while the attacker is present, and the PIN code they enter is sufficiently short, then the attack could theoretically succeed.

If the PIN key that has been used consists of only four numeric characters, a fast PC can calculate the security key in less than one tenth of a second. As the PIN key gets longer, the time to crack the security code gets longer and longer. At eight alphanumeric characters it would take over one hundred years to calculate the PIN making this crack nearly impossible.

This is an academic analysis of *Bluetooth* security. What this analysis outlines is possible, but it is highly unlikely for a normal user to ever encounter such an attack. The attack also relies on a degree of user gullibility, so understanding the *Bluetooth* pairing process is an important defense.

Can the SIG guarantee me that all of my future *Bluetooth* products will be secure?
Absolute security can never be totally guaranteed - in technology or otherwise. Security is an ongoing and important effort for any technology. The *Bluetooth* SIG has made security a high priority from day one with security algorithms that to date have proven adequate. In the roadmap for the advancement of *Bluetooth* wireless technology, the *Bluetooth* SIG published security and privacy enhancements. These enhancements to the specification further strengthen the pairing process and ensure privacy after a connection is established. We are continuing with our work in this area, trying to always stay a step ahead of people trying to hack into devices.

What is denial of service (DoS)?
The well known denial of service (DoS) attack, which has been most popular for attacking internet web sites and networks, is now an option for hackers of *Bluetooth* wireless technology enabled devices. This nuisance is neither original nor ingenious and is, very simply, a constant request for response from a hacker's *Bluetooth* enabled computer (with specific software) to another *Bluetooth* enabled device such that it causes some temporary battery degradation in the receiving device. While occupying the *Bluetooth* link with invalid communication requests, the hacker can temporarily disable the product's *Bluetooth* services.

Can a hacker get access to my devices data or content with DoS?
The DoS attack only offers the hacker the satisfaction of temporary annoyance, but does not allow for access to the device's data or services – no information residing on the receiving device can be used or stolen by the attacker.

What devices are vulnerable to attacks, and what is the Bluetooth SIG doing about it?
DoS attacks can be performed on any discoverable *Bluetooth* enabled device but in some cases, advanced hackers can determine the address of a non-discoverable *Bluetooth* device. The *Bluetooth* SIG takes all security issues seriously, and we constantly work to make the specification more secure. Therefore, future *Bluetooth* core specifications are planned to include features that will make it impossible to penetrate non-discoverable devices. There are also ways for manufacturers to reduce the risk of DoS attacks at the implementation level of *Bluetooth* wireless technology.

What is the risk of being on the receiving end of a DoS attack?
To date, DoS attacks on *Bluetooth* devices have only been conducted in laboratory tests. The risk of an attempted DoS attack should be considered minimal given the requirements and the normally short range of *Bluetooth* wireless technology.

Imagine

we have tools that will open your mind to new possibilities in connection, communication, and innovation

sitemap | legal | privacy policy