



ECKey

Bluetooth Security

Version 1.0
5th April 2006

TABLE OF CONTENTS

ECKEY..... I

1 INTRODUCTION..... 1

1.1 BACKGROUND..... 1

 1.1.1 Interference..... 1

 1.1.2 Range..... 1

 1.1.3 Power..... 1

 1.1.4 Name..... 1

 1.1.5 Stability..... 1

1.2 EVALUATION APPROACH 2

1.3 INTRODUCTION TO ECKEY..... 3

2 BLUETOOTH THREATS..... 4

2.1 CABIR WORM – RISK: NONE 4

2.2 CAR WHISPERER – RISK: NONE..... 4

2.3 BLOOVER – RISK: NONE..... 5

2.4 BLUESNARFING – RISK: NONE 6

2.5 BLUEBUGGING – RISK: NONE..... 6

2.6 BLUEJACKING – RISK: NONE..... 7

2.7 IMPERSONATION OF ECKEY – RISK: VERY LOW 7

2.8 BRUTE FORCE PAIRING – RISK: VERY LOW..... 7

2.9 INTERCEPTION OF PAIRING – RISK: VERY LOW..... 7

2.10 INTERCEPTION OF AUTHENTICATION – RISK: VERY LOW..... 8

2.11 PHONE THEFT/LOSS – RISK: MEDIUM 8

2.12 PIN DISCLOSURE – RISK: VERY LOW..... 8

2.13 DENIAL OF SERVICE – RISK: LOW 8

3 CONCLUSION 9

3.1 THREAT SUMMARY 9

3.2 BLUETOOTH SECURITY RECOMMENDATIONS..... 9

4 FREQUENCY ASKED QUESTIONS 11

5 REFERENCES..... 14

This document is copyright to ECKEY 2007 © and is not to be reproduced without permission

1 Introduction

In this document the security of Bluetooth as it relates to ECKey will be assessed. After a general introduction to Bluetooth and a description of the approach in this section, the threats are listed in section 2 and conclusions provided in section 3.

1.1 Background

Bluetooth wireless technology is the low-power, short-range radio technology that allows electronic devices such as mobile phones, headsets, PDA's and notebook PC's to speak to each other without wires. Bluetooth is the established short range wireless technology.

1.1.1 Interference

Bluetooth wireless technology's Adaptive Frequency Hopping (AFH) capability was explicitly designed to reduce interference between wireless technologies sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency. This is done by detecting other devices in the spectrum and avoiding the frequencies they are using. This 'adaptive hopping' allows for more efficient transmission within the spectrum, thereby providing the user with greater performance, even if using other technologies along with the *Bluetooth* wireless technology.

1.1.2 Range

- Class 3 radios - most commonly found in mobile devices - have a range of 10 meters or 30 feet.
- Class 1 radios - used primarily in industrial use cases - have a range of 100 meters or 300 feet

1.1.3 Power

The most commonly used radio (class 3) uses 1mW of power; *Bluetooth* wireless technology is designed to have very low power consumption; the specification reinforces this by allowing radios to be powered down when they are not active.

1.1.4 Name

"*Bluetooth*" refers to Harald Blatland, the 10th-century Danish king who unified the Danes and Norwegians.

1.1.5 Stability

Membership - There are over 3400 members in the Special Interest Group. Companies like IBM, Microsoft, Motorola, Nokia, DaimlerChrysler, Palm, ECKey, are all backers of the technology.

3M Products - Over three million *Bluetooth* products ship per week; that number increased rapidly (within 3 months from 2M and within 9 months from 1M).

Multiple Industries/Breadth of Products - *Bluetooth* wireless technology touches a number of industries like no other wireless technology. From computing and networking to consumer electronics, automotive, and even medical and industrial, there are innumerable uses for *Bluetooth* wireless technology. At this time, there are over 1700 different products with *Bluetooth* technology on the market - *Bluetooth* wireless technology is not only used in the everyday lives of consumers, but in hospital surgical units and delivery automation scenarios. There are even golf clubs with *Bluetooth* technology built in to transfer data about one's swing back to a laptop or PDA.

Qualification - The Special Interest Group oversees testing and qualification of all products bearing the *Bluetooth* trademark. This program is currently being enhanced to provide even higher interoperability standards for product manufacturers.

Security - *Bluetooth* wireless technology was built with security in mind. That said, there have been several issues brought to the forefront this year that have shown a light on security within *Bluetooth* products. The Special Interest Group works with members to eliminate issues and continues to update the specification and include security enhancements. The Special Interest Group also encourages consumers to use long alphanumeric PINs, pair in private and keep devices undiscoverable when not in use to reduce vulnerability. The roadmap announced Nov. 8, 2004, features security enhancements for the technology in 2005 and 2006. The Special Interest Group is also working with A.L. Digital to test the security of *Bluetooth* devices at UnPlugFests.

1.2 Evaluation Approach

In this document a wide range of potential threats associated with Bluetooth will be discussed together with an assessment of their level of risk associated with the ECKey solution. The level of risk of each threat has been measured against the following definitions.

Risk Level	Description
None	The threat does not apply to ECKey
Very Low	Investment of significant time (years), skill (experts) and money (thousands) required to have an impact on a single ECKey device.
Low	Ability for a skilled individual to have an impact on a single installation of ECKey.
Medium	Ability to low skilled individual to have impact on a ECKey in specific situations with the knowledge of the owner.
High	Ability for low skilled individual (that is reading the web) to have an impact on any

Risk Level	Description
	ECKey.

The list of threats is described in detail in section 2 with a risk summary provided in section 3.1. The independent sources of information used to prepare this whitepaper are referenced at the end of this document to enable the validation of the assessment provided.

1.3 Introduction to ECKey

ECKey is an authenticating proximity device for controlling secure access to various systems such as doors, gates, garages, alarms systems, and cars. The basic operation is as follows.

From within the secure location (such as inside the door) a button is pressed to initiate a search for a local discoverable Bluetooth devices such as a cellphone. Once discovered ECKey authorises the cellphone by requesting to pair or bond with the cellphone. This is achieved by entering a PIN on the cellphone that matches the PIN stored within ECKey. The PIN is not transferred themselves but converted into associated hash values which are transferred. The PIN is not stored on the cellphone but the resulting link key is stored. This is standard Bluetooth security that is described in more detail at www.bluetooth.org.

Once pairing is complete the cellphone is authorised. ECKey then scans for all the authorised devices within range. It does not scan for any device that is not authorised unlike the pairing process. When one of the authorised devices is found, it is authenticated using the link key created during pairing. If this is successful the unlocking process is activated. When the authenticated device moves out of range or disconnects, the locking mechanism is triggered.

In order to register additional devices or undertake administration of the system (such as changing a PIN), this must first be initiated from a button located in a secure location and the use of PIN. Further details can be found within the New Zealand patent application titled “Device and Method for Controlling a Switch”.

2 Bluetooth Threats

The Bluetooth Special Interest Group strives to keep Bluetooth technology secure. The Security Expert Group is in place to address new and existing vulnerabilities. Roadmap enhancements continue to address security concerns to keep Bluetooth wireless technology the most secure wireless technology.

2.1 Cabir Worm – Risk: None

The source code of the Cabir worm was released by an unknown programmer and F-Secure reported that 29ALabs has also publicly released the source code. A security threat at any level is a top priority to the Bluetooth Special Interest Group.

The Cabir worm is designed to affect Symbian series 60 mobile phones using the phones' Bluetooth functionality. There are currently 10 known versions of the worm, Cabir. A through .J. Most versions of the worm must be accepted and installed by the receiver. Thus far, the worm has not been directly destructive or malicious, it is capable of blocking customary Bluetooth connectivity and completely draining the battery power from the infected phone. The nature of the worm could change with the source code now public, so it is important to only accept content from trusted sources and use anti-virus software. Symantec, McAfee and F-Secure offer anti-virus software for mobile phones and handheld devices running a variety of operating systems.

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 behaviour, 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](#) .

As ECKey can not accept installation from other devices it can not be affected by the Cabir worm therefore the risk level is none.

2.2 Car Whisperer – Risk: None

Car Whisperer is a program that may allow a user to illicitly send or receive audio signals to and from *Bluetooth* hands-free (HFP) devices with specific implementations. The devices vulnerable to this program have the following implementation:

- They use a standard fixed PIN code such as 0000 or 1234. The code is often printed in the user manual and is publicly known.
- They stay continuously in visible pairing mode when not connected to an authorized cell phone and don't require any user interaction to accept a pairing.

To reduce the threat of programs like Car Whisperer, the SIG advises its members to:

- Recommend to their end users to always pair *Bluetooth* devices in a safe, private environment.
- Use longer, unique alphanumeric PIN codes.
- Require user interaction to accept pairing between devices

At a recent European wireless security meeting, a computer consultant demonstrated a Linux program called "Car Whisperer" that allegedly allowed him to illicitly send or receive audio signals to and from Bluetooth hands-free (HFP) or headset (HSP) devices with a specific implementation. This presentation has been covered by the media, including a recent PC World article <http://www.pcworld.com/news/article/0,aid,122077,00.asp>. More information and a download of the tool can also be found at http://trifinite.org/trifinite_stuff_carwhisperer.html.

Using a portable computer with a Bluetooth radio and a directional antenna, the consultant used the "Car Whisperer" program to remotely connect to and communicate with the car, sending audio to the speakers and receiving audio from the microphone in the remote device. The consultant stated that he was able to accomplish this because some Bluetooth device manufacturers have not implemented the SIG's recommendations for security practices. The devices vulnerable to this attack are easily connected to because of their implementation:

It is also likely that the same attack could work on headsets under the same conditions. While most manufacturers are delivering HSP and HFP implementations that are secure from this type of attack, some are not and this can create challenges for all of us. The public is rarely able to distinguish between specification and implementation vulnerabilities. Often the blame for implementation vulnerabilities is laid on the technology itself.

As ECKEY does not use standard or fixed PIN codes and does not transmit sensitive information it is not affected by this threat and therefore the risk level is none.

2.3 Bloover – Risk: None

The Bloover program was released by Adam Laurie of A.L.Digital and Martin Herfurt of the Trifinite Group. The Bloover program, a proof-of-concept auditing tool for identifying vulnerability to bluesnarf and bluebug attacks in phones, was recently released to the public. The program is a Java version of a tool that helps to identify these security flaws in some manufacturers' mobile phones. The tool is currently limited as to not allow hackers to cause financial damage. However, if a user's mobile phone is not updated, there is a potential someone could use Bloover to enter the phone and copy contact information. For those phones that require a patch, it is recommended to do so.

The Bloover program, a proof-of-concept auditing tool for identifying vulnerability to bluesnarf and bluebug attacks in phones, was recently released to the public. The program is a Java version of a tool that helps to identify these security flaws in some manufacturers' mobile phones. The tool is currently limited as to not allow hackers to cause financial damage. However, if a user's mobile phone is not updated, there is a potential someone could use Bloover to enter the phone and copy contact information. For those phones that require a patch, it is recommended to do so.

As ECKey uses the latest implementations of Bluetooth it is not affected by this threat and therefore the risk level is none.

2.4 Bluesnarfing – Risk: None

Recently, there have been reports of “bluesnarfing,” defined by security experts as breaching the security of a mobile phone and obtaining information from phone books and calendars located on the phone through its Bluetooth wireless connection. This issue is a result of how Bluetooth wireless technology is implemented in a limited number of products and is not inherent to Bluetooth wireless technology itself.

Bluetooth wireless technology has advanced security features built into the technology and can be considered one of the most secure wireless technologies available on the market today.

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.

As ECKey does not have a Bluetooth phone book or calendar it is not affected by this threat and therefore the risk level is none. It also will not connect to a new device unless initiated from a secure location.

2.5 Bluebugging – Risk: None

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 read SMS, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.

This is a separate vulnerability from bluesnarfing and does not affect all of the same phones as bluesnarfing. The majority of phones on the market with Bluetooth technology are not vulnerable to this attack. Additionally, manufacturers are currently testing future phone models for this vulnerability meaning this will not be an issue going forward.

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 read SMS, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet. As with all the attacks, 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.

As ECKey does not use the phone interfaces and therefore is not affected by this threat and therefore the risk level is none.

2.6 Bluejacking – Risk: None

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.

As ECKey only accepts encrypted business cards during administration from authenticated sources it is not affected by this threat.

2.7 Impersonation of ECKey – Risk: Very low

An impostor could try to impersonate ECKey with a stronger transmission power and request the PIN from a user. As the user would not have initiated the pairing process on ECKey it should ring alarm bells for them if a device labelled as ECKey tries to get access. Even if the user entered the PIN without thinking it is not transmitted to the impostor device. Only the link key is transferred and it would still take the impostor several years to decode the keys to get the PIN. With the PIN the impostor would have to initiate the pairing process to obtain entry. In order to initiate entry they would need to get access to the secure location (inside the door) to press a button to start the process. If they are inside the secure location why do they need to break the electronic lock? If an impostor succeeded this would be obvious as another user would be registered and visible from the administration interface.

2.8 Brute force pairing – Risk: Very low

An impostor could try different PIN numbers to pair however they would need access to a secure location (inside the door) in order to initiate the pairing process. If they are inside the door why do they need to attack the lock? With an 8 digit PIN this would take 6 years to try all the possible combinations. If an impostor succeeded this would become obvious as another user would be registered and visible from the user interface.

2.9 Interception of pairing – Risk: Very low

Theoretically a hacker can monitor and record activities in the frequency spectrum during a pairing process and then use a computer to regenerate the PIN codes being exchanged. This requires specially built hardware and thorough knowledge of *Bluetooth* systems.

In ECKey the pairing occurs once and is only repeated if the initiated by the user from a secure location, for example inside the door. This makes the likelihood of interception very low.

By using a PIN code with 8 or more alphanumeric digits it would take the hacker years to discover the PIN with advanced software. By using a 4 digit numeric PIN code, the hacker could discover the PIN in a matter of a few hours, therefore 4 digit PINs should be avoided.

If the impostor has the PIN they still need access to the secure location to initiate the pairing process, negating any benefit that may be obtained by getting the PIN in the first place.

2.10 Interception of authentication – Risk: Very low

Theoretically a hacker can monitor and record activities in the frequency spectrum during the authentication that is repeating. As the information is encrypted and the private keys have already been established this would take millions of years to break through brute force attempts to decode the keys.

If the impostor has the PIN they still need access to the secure location to initiate the pairing process, negating any benefit that may be obtained by getting the PIN in the first place.

2.11 Phone theft/loss – Risk: Medium

The theft of your cellphone would enable someone to open the door and this is no different with a key or security card. If a phone is lost, it can be deleted from ECKey. This is similar to rekeying a lock. As the PIN is not stored on the lost device there is no need to change the PIN.

2.12 PIN disclosure – Risk: Very low

ECKey stores a user changeable PIN in memory and is set up to avoid any issues with the PIN being disclosed. Every time two Bluetooth devices pair a different link key is created. By only allowing pairing when initiated from a secure location (for example inside the door) a second device can not impersonate the first without entering the secure location (inside the door) to initiating the pairing. Once inside the door there is no value in trying to unlock the door.

2.13 Denial of Service – Risk: Low

Denial of service is the act of disrupting the service or function of another system. For example hitting a website to overload it and stop it from servicing valid requests. This is theoretically possible with Bluetooth however the denial of service 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.

3 Conclusion

Most of the threats discussed in the previous section have either been resolved or do not apply to ECKey. Those that do apply either have a very low risk or the same level of risk as a traditional key or proximity card or remote control system.

ECKey is a secure implementation of Bluetooth suitable for the replacement of keys, proximity cards and security remote controls.

3.1 Threat Summary

The following is a summary of the threats and the level of risk discussed in this whitepaper. The greatest risk arises from the loss or theft of a phone and its use before the owner deactivates that phone. This is similar to the risk of someone stealing your keys and using them before you have a chance to change the locks. One difference here is that the owner can disable the phone without professional assistance.

Threat	ECKey Security Risk
Cabir Worm	None
Car Whisperer	None
Blover	None
Bluesnarfing	None
Bluebugging	None
Bluejacking	None
Impersonation of ECKey	Very low
Brute force pairing	Very low
Interception of pairing	Very low
Interception of authentication	Very low
Phone theft/loss	Medium
PIN disclosure	Very low
Denial of Service	Low

3.2 Bluetooth Security Recommendations

Just as locking your door is an important part of physical security there are number of similar actions required for the security of Bluetooth systems. There are inherent security features built into the specification and additional security features in the

roadmap looking forward. Security consultants acknowledge that *Bluetooth* technology, when implemented according to Special Interest Group security recommendations, is safe.

The Bluetooth Special Interest Group advises that:

- Always pair *Bluetooth* devices in a safe, private environment.
- Use 8 digit, unique PIN codes.
- After pairing make your device non discoverable
- Do not reveal your PIN
- Do not accept connection or pairing requests from untrusted or unexpected sources

ECKey support these recommendations and has incorporated some additional security features to ECKey.

- ECKey is only available to pair or accept connections for a limited time after being initiated from manually pressing a button from a secure location (such as inside the door).
- ECKey uses the minimum transmission power during pairing to reduce signal leakage.
- Once paired ECKey does not respond to any unregistered device.
- No private or sensitive information is ever transmitted once in use.
- The highest Bluetooth security mode (link level) is used in ECKey.

4 Frequency Asked Questions

The following frequency asked questions is taken from the Bluetooth Special Interest Group discussion on 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 3000 member manufacturers, has a *Bluetooth* Security Experts Group made up of engineers from its member companies, which 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

These security modes are determined by the manufacturer of each product. Devices and services also have different security levels. For devices, there are 2 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.

To learn more about security, the *Bluetooth* SIG recommends that members participate in the *Bluetooth* SIG Security Experts Group (SEG). For more information on joining the SEG, please visit https://www.bluetooth.org/bluetooth/landing/sig_groups.php.

Why are fixed PINs a potential security risk?

The *Bluetooth* PIN (Personal Identification Number) code is the passkey that is required to enable pairing between two devices. If the device PIN is fixed and publicly known, it is much easier for unauthorized users to attempt to connect to that device. The SIG advises its members to use unique PINs for their devices. The SIG also recommends the use of unique, 8 character alphanumeric PIN codes to further improve security.

Why should Bluetooth devices require user interaction to accept pairing between devices?

Required interaction can raise the level of security because a user can refuse to accept pairing from an unauthorized or unknown device by simply not taking any action such as pushing an “accept” button. Even if the device PIN code is known and transmitted, the pairing request will be denied without interaction.

What are phone manufacturers doing on security?

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](#).

Is Bluetooth wireless technology susceptible to hackers in other ways?

Currently, "bluesnarfing and bluebugging" 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 the 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.

How does a PIN affect security?

The Personal Identification Number (PIN) is a 4 or more digit alphanumeric code that is temporarily associated with ones products for the purposes of a one time secure pairing. It is recommended that users use an 8 digit 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.

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.

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. 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* 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.

The *Bluetooth* SIG also recommends that members participate in the *Bluetooth* SIG Security Experts Group (SEG). For more information on joining the SEG, please visit https://www.bluetooth.org/bluetooth/landing/sig_groups.php. For more resources see,

5 References

The following sources were used in the preparation of this white paper.

Author	Location
Bluetooth SIG	http://www.bluetooth.org
Yaniv Shaked and Avishai Wool	http://www.eng.tau.ac.il/~yash/shaked-wool-mobisys05/index.html
Keijo Haataja	http://www.cs.karelia.ru/fdpw/2004/haataja.pdf
Marek Bialoglowy	http://www.securityfocus.com/infocus/1830
Laura Taylor	http://www.pdastreet.com/articles/2005/10/2005-10-4-Security-Plug-Those.html