

## Bluetooth Increases Internet Security Risks



*Prepared for*  
**The IT Security Community and our Customers**

*Prepared by*

Lunarline, Inc.  
1875 I ST, NW, Suite 500  
Washington, DC 20006  
[www.lunarline.com](http://www.lunarline.com)

**15 December 2006**

**By Matt Metheny, PMP, CISSP, CAP, CISA**

## **Abstract**

This paper discusses the Bluetooth technology, and the threat posed by the security vulnerabilities that exists in modern day mobile devices such as cell phones, laptops, and smart phones. The current Bluetooth security issues and threats demonstrate the risk of improper implementations of the Bluetooth security model, and the various attacks that have taken advantage of the vulnerabilities. This paper also discusses the security features offered by the Bluetooth specification, and addresses specific countermeasures that should be considered before deploying Bluetooth technology within any organization.

## Table of Contents

Abstract.....	2
Introduction.....	4
Introduction to Bluetooth Technology.....	4
Bluetooth Security Issues and Mobile Threats .....	5
Bluetooth Security Features and Countermeasures .....	6
Conclusion .....	7
References.....	8

## Introduction

With the expansion of the wireless community, mobile devices are becoming more connected, and more susceptible to attacks every day. These devices are part of a wireless web that links together millions of devices making it easier to spread viruses, and launch attacks over the Internet. Bluetooth-enabled devices are setting the course for being the next generation Internet security threat because of the broad number of unprotected, mobile devices. This scenario is becoming more a reality each day, with the addition of each new unprotected Bluetooth-enabled device

### Introduction to Bluetooth Technology

Bluetooth technology is growing among mobile devices, from cell phones to keyboards. Bluetooth communicates over a common frequency (2.4GHz Industrial-Scientific-Medical radio band) that is free (unlicensed) low-cost, low-power, high-speed (723.2 kbps) and more flexible (allows 2 devices within 10-100 m to share data) than the other competing wireless technologies (<http://www.securityfocus.com/infocus/1830>, para. 1). Bluetooth technology has become an attractive alternative that offers a cable-free network for devices. This wireless connectivity is the best approach for devices that exist in close proximity, need to transfer data, and do not require line-of-sight alignment.

There are many different uses of Bluetooth technology, with the list growing every day. The viability of the technology to support different types of wireless devices makes it an extremely attractive choice for manufactures. It presents a common language that is understood across an array of industries. Bluetooth is supported and used in products of over 3000 companies such as Sony, Ericsson, Nokia, Toyota, BMW, and Microsoft. There is a wide range of products that are available in the market that have Bluetooth integrated into them including laptops, printers, keyboards, and DVD/DVRs (<http://www.securityfocus.com/infocus/1830>, para. 1).

Bluetooth also offers an easy way to extend existing networks or provide a mechanism for enabling devices that have limited interfaces to communicate. "Bluetooth wireless technology provides an easy way for a wide range of devices to communicate with each other and connect to the Internet" (<http://www.securityfocus.com/infocus/1830>, para. 1). Bluetooth Personal Area Networks (PANs) are being organized in lieu of expensive wireless networks (e.g., 802.11x) which require extensive knowledge of deploying and administrating (including security) various types of technology.

The extensibility offered by Bluetooth, also creates risks associated with abuse or being the target of exploitation. This is becoming more apparent in markets such as mobile phones where the popularity of smartphones and Bluetooth-enabled cell phones are increasing daily. Mobile phones drives 60% of the total Bluetooth market, with over 922 million devices expected by 2008 (<http://www.securityfocus.com/infocus/1830>, para. 1). The adoption of Bluetooth, like any new wireless technology must be controlled to

ensure access is limited and data is protected from eavesdropping. These basic concepts of security are widely overlooked because of the lack of awareness end-users have when it comes to the vulnerabilities in the mobile devices they use to store and transmit information (personal or business).

## **Bluetooth Security Issues and Mobile Threats**

The popularity of Bluetooth technology has prompted concerns with security. Like every new wireless technology, intruders will challenge the security architecture of the new technology and attempt to exploit its weaknesses. Bluetooth is a short-range, open standard protocol that can be freely used by anyone that wants to communicate, many times it's just as easy as being within range. Other implementations require additional hardware or software, and a keen understanding of the target that is being exploited. In either case, the Bluetooth implementation (or lack thereof) by the manufacturers provides intruders with an avenue to start their attack.

There are several known Bluetooth vulnerabilities that are commonly understood and used to exploit mobile devices. Many of these vulnerabilities are caused by the manufacturer's improper implementation of the Bluetooth security model, which enables attackers to use manual and automated tools to bypass these security features. Accompanying these vulnerabilities is the limitation of the user in understanding how to effectively protect themselves, or identify when these vulnerabilities exist. The responsibility should be shared by the manufacturer to ensure they adequately educate the limitation to the consumer and the risk associated with these vulnerabilities.

Some examples of most widely known Bluetooth threats that attempt to exploit the flaws in the implemented security features offered by Bluetooth technology in mobile devices are:

- “Bluesnarfing”
- “Bluebugging”
- Viruses and worms

Although not an exclusive list, these examples illustrate the variances that exist, and how they affect the security of the mobile community. To better understand the apparent risks with Bluetooth security, we will discuss each of these threats in detail.

### **“Bluesnarfing”**

“Bluesnarfing” is an attack that involves the downloading of data from a mobile device such as cell phones or laptops. This attack also leaves no trace, which means the user will have no knowledge they were even a victim, or exactly what information was stolen (<http://www.zdnet.co.uk/print/?TYPE=story&AT=39145881-39020348t-10000015c>, para. 7). There are many automated tools currently available across

hundreds of websites that can be used, by even novice hackers with a good tutorial, to exploit Bluetooth interfaces on mobile devices which contain this flaw. “Bluesnarfing occurs using the same service (OBEX Push Profile) for exchanging business cards because most implementations do not require authentication.

### “Bluebugging”

Beyond the threat imposed by the theft of personal data, attackers are becoming more creative with their exploits, even using the existing capabilities of mobile phones as listening devices, also known as “bluebugging”. This attack transforms the victim’s phone into a bugging device because the attacker will force the targeted phone to dial a number of their own (<http://www.pcworld.com/printable/article/id,118236/printable.html>, para. 4). This attack exploits the devices security flaw around the ASCII communication commands (AT commands) that are commonly issued to the devices such as modems. These commands do not require user intervention, and therefore could occur without the user’s knowledge. As more mobile phones become Internet accessible, this attack could even be used to remotely initiate attacks on other devices, or to send personal information back to an attacker.

### Viruses and Worms

So far we have seen two very different techniques for using Bluetooth technology to exploit mobile devices, however, another very new threat is emerging that may present a challenge for service providers, mobile device manufacturers, and security firms. The newest threat involves the spread of viruses and worms using mobile devices such as smartphones and laptops. For example, “according to F-Secure, Mabir is a worm that operates on Symbian Series 60 devices, and is capable of spreading both over Bluetooth and MMS messages” (<http://www.newswireless.com/index.cfm/article/2202>, para. 2). This is just one example of what can be expected as virus and worm authors learn how to use the capabilities of advancing technology, to either steal information, or affect service networks through mobile Denial-of-Service attacks.

## Bluetooth Security Features and Countermeasures

Bluetooth was designed with a security architecture that supports authentication, authorization, encryption, and data integrity. The goals of Bluetooth security were to provide a layered approach that included both device and service layer security. As part of the architecture, Bluetooth-enabled mobile devices can support three different modes of security. These three modes are:

- **“Security Mode 1 (non-secure):** No security procedures are performed” (Muller, 1999, p. 8).
- **“Security Mode 2 (service level security):** Security procedures initiated after channel establishment request has been received at L2CAP level. Whether security procedure is initiated or not depends on the service-level

type. Service (or application) level security implementation allows different access policies for different applications which may run in parallel” (Muller, 1999, p. 8).

- **“Security Mode 3 (link level security):** Security procedures are performed and authenticated at the LMP level before a channel is created for communication. A Bluetooth device in security mode 3 may reject a host connect based on host settings” (Muller, 1999, p. 8).

These modes were designed to provide various level of operational security, based on the needs of the application. For applications that want to ensure security is enforced across all applications, will use Mode 3 (Link-level security). The Bluetooth security architecture also addresses three levels of service security that are used by services running on the mobile device depending on the device-level security (trusted and untrusted):

- **Level 1** – “Services that require authorization and authentication. Automatic access is only granted to trusted devices. Other devices need a manual authorization” (Muller, 1999, p. 9).
- **Level 2** – “Services that require authentication only. Authorization is not necessary” (Muller, 1999, p. 9).
- **Level 3** – “Services open to all devices; authentication is not required, no access approval required before service access is granted” (Muller, 1999, p. 9).

The Bluetooth security model that should be adopted as part of the deployment of Bluetooth devices includes several security measures that can be used to prevent attacks and offer a more secure operating environment. The following security countermeasures should be implemented to protect devices against the attacks discussed in this paper.

- Set Bluetooth device to non-discoverable by other devices
- Implement pairing with PIN authentication
- Do not use short PINs
- Disable Bluetooth on mobile devices if not needed
- Educate users on the threats against Bluetooth technology

## Conclusion

The security of Bluetooth technology is continuously evolving as the Bluetooth Special Interest Group (SIG) improves on the Bluetooth specification. Industry is also working to reduce vulnerabilities through upgrades that exist in current software residing on mobile devices, and updating the design of new devices. As with any new technology, security can only be achieved through a consistent visibility of weakness and responsiveness to fixing the vulnerabilities through patches or upgrades.

## References

- Bialoglowy, M. (2005). Bluetooth Security Review, Part 1. Retrieved November 2, 2006 from <http://www.securityfocus.com/infocus/1830>.
- Brandt, A. (2004). Privacy Watch: Cell Phones Get Chatty With Hackers. Retrieved November 3, 2006 from <http://www.peworld.com/printable/article/id,118236/printable.html>.
- Kewney, G. (2005). Bluetooth worm “is a real threat” – patch available for Symbian phones. Retrieved November 5, 2006 from <http://www.newswireless.com/index.cfm/article/2202>.
- Kotadia, M. (2004). Bluetooth phones at risk from ‘snarfing’. Retrieved October 29, 2006 from <http://www.zdnet.co.uk/print/?TYPE=story&AT=39145881-39020348t-10000015c>.
- Muller, T. (1999). Bluetooth Security Architecture, Version 1.0. Bluetooth Special Interest Group (SIG).