Bluetooth Security

By Colleen Rhodes

Graduate Student, East Carolina University

Abstract

Bluetooth provides a short range wireless communication between devices making it convenient for users and thus eliminating the need for messy cables. According to Bluetooth Special Interest Group (2006), "Bluetooth wireless technology is the most widely supported, versatile, and secure wireless standard on the market today." Bluetooth operates in the open 2.4 GHz ISM band and is "now found in a vast array of products such as input devices, printers, medical devices, VoIP phones, whiteboards, and surveillance cameras. [However], the proliferation of these devices in the workplace exposes organizations to security risks." (Detecting Bluetooth Security Vulnerabilities, 2005) This paper will explain what Bluetooth is, how it works, and some of the vulnerabilities and risks associated with it.

What is Bluetooth?

In the past, the only way to connect computers together for the purpose of sharing information and/or resources was to connect them via cables. This can be not only cumbersome to set up, but it can get messy real quick. Bluetooth provides a solution to this problem by providing a cable-free environment. According to the official Bluetooth website, www.bluetooth.com,

> Bluetooth wireless technology is a short-range communications technology intended to replace the cables connecting portable and/ore fixed devices while maintaining high levels of security. The key features of Bluetooth technology are robustness, low power, and low cost. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

"The idea behind Bluetooth technology was born in 1994, when a team of researchers at Ericsson Mobile Communications…initiated a feasibility study of universal short-range, low-power wireless connectivity as a way of eliminating cables between mobile phones and computers, headsets and other devices." (2005, Bialoglowy) In 1998, this group evolved to the Bluetooth Special Interest Group (SIG). Along with Ericsson, other founding members included Nokia, Intel, IBM and Toshiba. Today, "the SIG is comprised of over 4,000 members who are leaders in the telecommunications, computing, automotive, music, apparel, industrial automation, and network industries,

and a small group of dedicated staff in Hong Kong, Sweden, and the USA." (Bluetooth SIG, 2006)

Many people wonder where the name "Bluetooth" came from. According to Bluetooth SIG (Bluetooth SIG, 2006),

> The name "Bluetooth" is taken from the 10th century Danish King Harald Blatand - or Harold Bluetooth in English. During the formative stage of the trade association a code name was needed to name the effort. King Blatand was instrumental in uniting warring factions in parts of what is now Norway, Sweden, and Denmark - just as *Bluetooth* technology is designed to allow collaboration between differing industries such as the computing, mobile phone, and automotive markets. The code name stuck.

How Bluetooth Works

Bluetooth can be used to connect almost any device to another device. "Bluetooth can be used to form ad hoc networks of several (up to eight) devices, called piconets. (Vainio, 2000). When Bluetooth devices first connect, there is a piconet master that initiates the connection, and the others are slave devices. "One piconet can have a maximum of seven active slave devices and one master device. All communication within a piconet goes through the piconet master. Two or more piconets together form a scatternet, which can be used to eliminate Bluetooth range restrictions." (Haataja, 2006) It is not possible to be a master of two different piconets because a piconet is a group of devices all synchronized on a hopping sequence set by the master. For that reason, any devices that share a master must be on the same piconet. "Scatternet environment requires that

different piconets must have a common device (so-called scatternet member) to relay data between the piconets." (Haataja, 2006)

As stated in the Bluetooth SIG website, "Bluetooth technology operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries." Bluetooth devices within a 10 to 100 meters (or 30 to 300 feet) range can share data with a throughput of 1 Mbps for Version 1.2 and up to 3 Mbps for Version 2.0 + Enhanced Data Rate (EDR).

Data is transmitted between Bluetooth devices in packets across the physical channel that is subdivided into time units known as slots. As described in an article of JDJ, the world's leading java resource,

> The radio layer is the physical wireless connection. To avoid interference with other devices that communicate in the ISM band, the modulation is based on fast frequency hopping. Bluetooth divides the 2.4 GHz frequency band into 79 channels, 1 MHz apart (from 2.402 to 2.480 GHz), and uses this spread spectrum to hop from one channel to another, up to 1,600 times per second. (Mikhalenko, 2006)

Bluetooth SIG further explains that

> Within a physical channel, a physical link is formed between any two devices that transmit packets in either direction between them. In a piconet physical channel there are restrictions on which devices may form a physical link. There is a

> physical link between each slave and the master. Physical links are not formed directly between the slaves in a piconet. (Bluetooth SIG, 2006)

Profiles are used with Bluetooth so that devices can communicate with each other and that there is interoperability between vendors. These profiles define behaviors of the Bluetooth devices and "the roles and capabilities for specific types of applications. (Mikhalenko, 2005). Each profile specification contains information on the following topics:

- Dependencies on other profiles
- Suggested user interface formats
- Specific parts of the Bluetooth protocol stack used by the profile. To perform each task, each profile uses particular options and parameters at each layer of the stack. (Bluetooth SIG, 2006)

Bluetooth Security

Security has played a major role in the invention of Bluetooth. The Bluetooth SIG has put much effort into making Bluetooth a secure technology and has security experts who provide critical security information. In general, Bluetooth security is divided into three modes: (1) non-secure; (2) service level enforced security; and (3) link level enforced security. In non-secure, a Bluetooth device does not initiate any security measures. In service-level enforced security mode, "two Bluetooth devices can establish a nonsecure Asynchronous Connection-Less (ACL) link. Security procedures, namely authentication, authorization and optional encryption, are initiated when a L2CAP (Logical Link Control and Adaptation Protocol) Connection-Oriented or Connection-Less channel request is

made." (Haataja, 2006). The difference between service level enforced security and link level enforced security is that in the latter, the Bluetooth device initiates security procedures before the channel is established.

As mentioned above, Bluetooth's security procedures include authorization, authentication and optional encryption. Authentication involves proving the identity of a computer or computer user, or in Bluetooth's case, proving the identity of one piconet member to another. Authorization is the process of granting or denying access to a network resource. Encryption is the translation of data into secret code. It is used between Bluetooth devices so that eavesdroppers can not read its contents. However, even with all of these defense mechanisms in place, Bluetooth has shown to have some security risks. The next section of this paper will describe some of these vulnerabilities associated with Bluetooth technology.

Bluetooth Vulnerabilities and Security Risks

- Bluejacking is the process of sending unsolicited messages, or business cards, to Bluetooth-enabled devices. This does not involve altering any data from the device, but nonetheless, it is unsolicited. Devices that are set in non-discoverable mode are not susceptible to bluejacking. In order for bluejacking to work, the sending and receiving devices must be within 10 meters of one another. While this method has been widely used for promotional purposes, Bluetooth device-owners should be careful never to add the contact to their address book. While bluejacking is usually not done with malicious intent, repetitive bogus messages

can be annoying to the user, and in some cases, can render the product inoperable. This can also open the door to a variety of social engineering attacks.

- Bluesnarfing is a method of hacking into a Bluetooth-enabled mobile phone and copying its entire contact book, calendar or anything else stored in the phone's memory. By setting the device in non-discoverable, it becomes significantly more difficult to find and attack the device. However, "the software tools required to steal information from Bluetooth-enabled mobile phones are widely available on the Web, and knowledge of how to use them is growing." (Kotadia, 2004) Companies such as Nokia and Sony Ericsson are making sure new phones coming to market will not be susceptible to bluesnarfing.
- "The backdoor attack involves establishing a trust relationship through the "pairing" mechanism, but ensuring that it no longer appears in the target's register of paired devices. In this way, unless the owner is actually observing their devices at the precise moment a connection is established, they are unlikely to notice anything untoward, and the attacker may be free to continue to use any resource that a trusted relationship with that device grants access to…This means that not only can data be retrieved from the phone, but other services, such as modems, or Internet, WAP and GPRS gateways may be accessed without the owner's knowledge or consent." (The Bunker, 2003)
- The cabir worm is malicious software that uses Bluetooth technology to seek out available Bluetooth devices and send itself to them. According to Bluetooth SIG (2006), "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." Although this may be the case, this shows that it is achievable to write mobile viruses that spread via Bluetooth and may cause other hackers to explore the possibilities of writing Bluetooth viruses. The Mabir worm is essentially a variant of the Cabir worm where it uses Bluetooth and Multimedia Messaging Service messages (MMS) to replicate.

Conclusion

Bluetooth wireless is constantly growing in popularity because of the convenience of exchanging information between mobile devices. As Bluetooth usage rises, so do the security risks associated with the technology. Advantages to Bluetooth include "the ability to simultaneously handle both data and voice transmissions [which] enables users to enjoy [a] variety of innovation solutions such as a hands-free headset for voice calls, printing and fax capabilities, and synchronizing PDA, laptop, and mobile phone applications." (Bluetooth SIG, 2006) Bluetooth users should familiarize themselves with Bluetooth security issues before using Bluetooth devices, and especially before they bring these devices into the work place.

References

*Bialoglowy, Marek. 2005. *Bluetooth Security Review, Part 1*. Security Focus. Retrieved from http://www.securityfocus.com/print/infocus/1830 on July 1, 2006.

*Bialoglowy, Marek. 2005. *Bluetooth Security Review, Part 2*. Security Focus. Retrieved on July 1, 2006 from http://www.securityfocus.com/print/infocus/1836.

Bluetooth SIG, 2006, http://www.bluetooth.com

*Haataja, Keijo M.J. 2006. *Security in Bluetooth, WLAN and IrDA: a comparison.* Retrieved on July 1, 2006 from http://www.cs.uku.fi/research/publications/reports/A-2006-1.pdf.

Korzeniowski, Paul. 2005. *Bluetooth Security Threats Starting to Spread*. TechNewsWorld. Retrieved July 1, 2006 from http://www.technewsworld.com/story/40124.html

Kotadia, Munir. 2004. Bluesnarfing tools 'spreading quickly'. ZDNet UK. Retrieved July 11, 2006 from http://news.zdnet.co.uk/internet/security/0,39020375,39146427,00.htm

Mikhalenko, Peter V. 2005. *Developing Wireless Bluetooth Applications in J2ME*. JDJ Volume 10, Issue 1. Retrieved on July 1, 2006 from http://java.sys-con.com/read/47688.htm

*Sarbanes-Oxley Compliance Journal. 2005. Detecting Bluetooth Security Vulnerabilities. Retrieved July 1, 2006 from http://www.s-ox.com/News/detail.cfm?articleID=1217

*The Bunker. 2003. Security Briefs. *Serious flaws in Bluetooth security lead to disclosure of personal data*. Retrieved on July 1, 2006 from http://www.thebunker.net/security/bluetooth.htm

*Vainio, Juha T. 2000. *Bluetooth Security*. Retrieved on July 7, 2006 from http://www.niksula.hut.fi/~jiitv/bluesec.html.

*Denotes a reference from a technical journal or proceeding, or any paper that has at least 5 references.