BLUETOOTH SECURITY: PROTECTING WIRELESS NETWORKS AND DEVICES

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Wireless devices and networks provide practical, cost effective access to online information and to voice communications for many people. Bluetooth technology, which was originally developed in the 1990s, is the foundation for wireless personal area networks (WPAN), also referred to as ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of business and consumer devices, such as cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets.

With their wireless devices, users are able to form ad hoc networks that support voice and data communications. They can share applications between devices, and send information to their printers and other peripheral devices without the need for cable connections. Using PDAs and cell phones, users can update and synchronize their personal databases in address books and calendars that are on different devices, and they can gain access to network services such as wireless e-mail and Web browsing. All of these capabilities offer innovative approaches and cost savings for government, retail, manufacturing, public safety and many other applications.

The National Institute of Standards and Technology (NIST) recently issued a new guide to Bluetooth technology and to the security issues that are related to the use of Bluetooth devices. The new publication updates an earlier publication that dealt with security for Bluetooth and IEEE 802.11 standard wireless technologies. See the More Information section at the end of this bulletin for other NIST publications dealing with wireless network security issues.

NIST Special Publication (SP) 800-121, Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology

NIST SP 800-121, Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology, was issued in October 2008. Written by Karen Scarfone of NIST, and by John Padgette of Booz Allen Hamilton, the publication helps organizations protect their Bluetooth devices from security threats and vulnerabilities.

SP 800-121 overviews Bluetooth technology, and discusses the primary characteristics of networks and devices. Topics addressed include the frequency-hopping scheme and the radio link power control properties that enable Bluetooth devices to find and establish communication with each other. The architecture of Bluetooth networks is explained, and diagrams of basic network topologies are provided.

One section of SP 800-121 is devoted to a discussion of the security features that are defined in the Bluetooth specifications and that support four modes of security. Also discussed are three modes of encryption that facilitate the cryptographic protection of the confidentiality of information.

Another major section of the guide covers the common vulnerabilities and threats involving Bluetooth technologies and recommends countermeasures to improve Bluetooth security. To help organizations manage their reviews of the security of their Bluetooth devices and information, NIST has included in the publication detailed security checklists. The checklists itemize recommendations or guidelines, and areas of concern for the security of Bluetooth devices. The security threats and vulnerabilities associated with each of these areas, and the risk mitigation practices for securing the devices from these threats, are delineated. The column format of the checklists enables staff members to review and check off the items that are relevant to their organizations.

The appendices provide a glossary of terms, lists of acronyms and abbreviations used in the document, references to Bluetooth specifications and papers, and Bluetooth online resources.

NIST SP 800-121 is available on the NIST Web site:

http://csrc.nist.gov/publications/PubsSPs.html

Bluetooth Technology

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology was originally conceived by Ericsson in 1994. Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Interest Group (SIG), a not-for-profit trade association organized to promote the development of Bluetooth products and serving as the governing body for Bluetooth specifications. Bluetooth standards are developed by the IEEE 802.15 Working Group for Wireless Personal Area Networks that formed in early 1999 as IEEE 802.15.1-2002.

Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks. Bluetooth is a low-cost, low-power technology that provides a mechanism for creating small wireless networks on an ad hoc basis, known as *piconets*. A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence. An example of a piconet is a Bluetooth-based connection between a cellular phone and a Bluetooth-enabled ear bud.

Bluetooth piconets are established on a temporary and changing basis. This property offers communication flexibility and scalability between mobile devices, and it enables easy file sharing and synchronization of information between Bluetooth devices. A Bluetooth-enabled device can form a piconet to support file sharing capabilities with other Bluetooth devices, such as laptops. For example, a laptop can use a Bluetooth

connection to have a mobile phone establish a dial-up connection, so that the laptop can access the Internet through the phone.

Bluetooth operates in the unlicensed 2.4 gigahertz (GHz) to 2.4835 GHz Industrial, Scientific, and Medical (ISM) frequency band. Other technologies also operate in this band, including the IEEE 802.11b/g WLAN standard, making the band somewhat crowded because of the volume of wireless transmissions. Bluetooth employs frequency hopping spread spectrum (FHSS) technology for all transmissions. FHSS reduces interference and transmission errors and provides a limited level of transmission security.

With FHSS technology, communications between Bluetooth devices use 79 different radio channels by hopping, or changing, frequencies about 1,600 times per second for data/voice links and about 3,200 times per second during page and inquiry scanning. A channel is used for a very short period (usually 625 microseconds for data/voice links), followed by a hop designated by a pre-determined pseudo-random sequence to another channel; this process is repeated continuously in the frequency-hopping sequence.

Bluetooth also provides for radio link power control, which permits devices to negotiate and adjust their radio power according to signal strength measurements. Each device in a Bluetooth network can determine its received signal strength indication (RSSI) and make a request of the other network device to adjust its relative radio power level by incrementally increasing or decreasing the transmission power. This operation can be performed to conserve power and also to keep the received signal characteristics within a preferred range.

Several versions of Bluetooth have been developed; the most recent are version 2.0 + Enhanced Data Rate (EDR) (November 2004) and version 2.1 + EDR (July 2007). Version 2.0 + EDR provides transmission speeds of up to 3Mbits/second, faster than previous versions, and version 2.1 + EDR provides a significant security improvement for link key generation and management in the form of Secure Simple Pairing (SSP). SP 800-121 addresses the security of both of these versions of Bluetooth, as well as the earlier versions 1.1 and 1.2.

Security Features of Bluetooth Technology

The Bluetooth standard provides three basic security services:

- **Authentication** to verify the identity of communicating devices. User authentication is not provided.
- **Confidentiality** to prevent the compromise of information and ensure that only authorized devices can access and view data.
- **Authorization** to allow the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

Four security modes are specified in the various versions of Bluetooth specifications:

- **Security Mode 1** is not secure. There are no capabilities for security authentication and encryption. This mode is supported only by version 2.0 + EDR and earlier devices.

- **Security Mode 2** has a security manager, as specified in the Bluetooth architecture, that controls access to specific services and devices. The centralized security manager maintains policies for access control and interfaces with other protocols and device users. Varying security policies and trust levels to restrict access may be defined for applications with different security requirements operating in parallel. It is possible to grant access to some services without providing access to other services. This mode allows for authorization, the process of deciding if a specific device is allowed to have access to a specific service. All Bluetooth devices can support Security Mode 2; however, version 2.1 + EDR devices can only support it for backward compatibility with version 2.0 + EDR (or earlier) devices.

- **Security Mode 3** requires a Bluetooth device to initiate security procedures before the physical network link is fully established. Bluetooth devices operating in Security Mode 3 mandate authentication and encryption for all connections to and from the device. This mode facilitates encryption and unidirectional or mutual authentication. The authentication and encryption features are based on a separate secret link key that is shared by paired devices, once the pairing has been established. Security Mode 3 is only supported in version 2.0 + EDR (or earlier) devices.

- **Security Mode 4** was introduced in Bluetooth version 2.1 + EDR. This mode is a service level enforced security mode in which security procedures are initiated after link setup. Secure Simple Pairing uses Elliptic Curve Diffie Hellman (ECDH) techniques for key exchange and link key generation. Device authentication and encryption algorithms are identical to the algorithms in Bluetooth version 2.0 + EDR and earlier versions. Security requirements for services protected by Security Mode 4 must be classified as one of the following: authenticated link key required, unauthenticated link key required, or no security required. Whether or not a link key is authenticated depends on the Secure Simple Pairing association model used.

Bluetooth does not address other security services such as audit and non-repudiation; if such services are needed, they must be provided through additional means.

Vulnerabilities and Threats

Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth

implementations can provide attackers with unauthorized access to sensitive information and unauthorized usage of Bluetooth devices and other systems or networks to which the devices are connected.

Organizations should assess the risks to their wireless networks as part of their overall risk management processes, and select controls that are based on their assessments and that address specific threats and vulnerabilities. Some of the needed controls cannot be achieved through the security features built into the Bluetooth specifications, and may have to be supplemented by the selection of security controls based on the organization's risk assessments and its specific requirements. Bluetooth security should be managed throughout the entire life cycle of Bluetooth devices and networks.

NIST SP 800-121 lists the currently known vulnerabilities of Bluetooth technology and recommends that organizations monitor the development of new vulnerabilities as version 2.1 of the Bluetooth specification becomes more widely adopted. New vulnerabilities and threats will require the implementation of additional security controls.

NIST's Recommendations for Bluetooth Security

NIST recommends that organizations carry out the following activities to protect their Bluetooth networks and devices:

Use the strongest Bluetooth security mode available for their Bluetooth devices.

All versions of Bluetooth technology support some, but not all, of the four security modes defined by the Bluetooth specifications. The modes vary primarily by how well they protect Bluetooth communications from potential attacks. Security Mode 3 is considered the strongest mode because it requires authentication and encryption to be established before the Bluetooth physical link is completely established. Security Modes 2 and 4 also use authentication and encryption, but only after the Bluetooth physical link has already been fully established and logical channels partially established. Security Mode 1 provides no security functionality. The available modes vary based on the Bluetooth specification versions of the devices being used; therefore, organizations should choose the most secure mode available for each case.

Address the use of Bluetooth technology in organizational security policies and change the default settings of Bluetooth devices to reflect the policies.

A security policy that defines the requirements for Bluetooth security is the foundation for all other Bluetooth-related countermeasures. The policy should include a list of approved uses for Bluetooth, a list of the types of information that may be transferred over Bluetooth networks, and requirements for selecting and using Bluetooth personal identification numbers (PINs). After establishing their Bluetooth security policies, organizations should ensure that default settings of Bluetooth devices are reviewed and changed as needed to assure that the settings comply with the security policy requirements. For example, organizations may require that unneeded Bluetooth profiles

and services be disabled to reduce the number of vulnerabilities that attackers could attempt to exploit. When available, a centralized security policy management approach should be used to ensure device configurations are compliant.

Ensure that the Bluetooth users are made aware of their organization's policies for security-related responsibilities regarding Bluetooth use.

A security awareness program helps users to follow security practices that help prevent security incidents. For example, users should be provided with a list of precautionary measures that they should take to better protect handheld Bluetooth devices from theft. Users should also be made aware of other actions to take involving Bluetooth device security, such as ensuring that Bluetooth devices are turned off when they are not needed to minimize exposure to malicious activities, and performing Bluetooth device pairing as infrequently as possible and ideally in a physically secure area where attackers cannot observe key entry and eavesdrop on Bluetooth pairing-related communications.

More Information

Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to wireless technologies, organizations are strongly encouraged to take advantage of the resources that are listed in the appendices to SP 800-121 for current and detailed information.

Publications developed by NIST help information management and information security personnel in planning and implementing a comprehensive approach to information security. The security of Bluetooth devices depends upon attention to basic issues such as security planning, security awareness and training, risk management, application of cryptographic methods, and use of security controls. Organizations can draw upon NIST standards and guidelines on these issues, and other issues related to the protection of networks and devices, including:

Federal Information Processing Standard (FIPS) 199, Standards for the Security Categorization of Federal Information and Information Systems

FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

NIST SP 800-30, Risk Management Guide for Information Technology Systems

NIST SP 800-32, Introduction to Public Key Technology and the Federal PKI

NIST SP 800-48, Rev. 1, Guide to Securing Legacy IEEE 802.11 Wireless Networks

NIST SP 800-50, Building an Information Technology Security Awareness and Training Program

NIST SP 800-53, Recommended Security Controls for Federal Information Systems

NIST SP 800-64, Security Considerations in the System Development Life Cycle

NIST SP 800-70, Security Configuration Checklists Program for IT Products: Guidance for Checklists Users and Developer

NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

NIST SP 800-111, Guide to Storage Encryption Technologies for End User Devices

NIST SP 800-114, User's Guide to Securing External Devices for Telework and Remote Access

For information about NIST standards and guidelines that are listed above, as well as other security-related publications, see NIST's web page:

http://csrc.nist.gov/publications/index.html

Disclaimer
Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.