# ITL BULLETIN FOR AUGUST 2012

## SECURITY OF BLUETOOTH SYSTEMS AND DEVICES: UPDATED GUIDE ISSUED BY THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology, which is used primarily to establish wireless personal area networks (WPANs), has been integrated into many types of business and consumer devices; examples include cell phones, laptops, automobiles, medical devices, printers, keyboards, computer mouse devices, and headsets. Bluetooth technology enables users to establish ad hoc networks supporting voice and data communications between a wide variety of devices that can be conveniently interconnected without the need for cables or wired connections.

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently issued Special Publication (SP) 121, Revision 1, *Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology,* to help organizations effectively protect their Bluetooth devices from security threats and vulnerabilities. The revised publication updates the original version of SP 800-121, which was issued in October 2008. Since the publication of the original version, many changes and improvements in Bluetooth technology have been implemented in commercial devices. These changes offer new capabilities and services for users, but also may introduce new threats and vulnerabilities to information systems.

### Bluetooth Technology and Specifications

Bluetooth is a low-cost, low-power technology that provides a mechanism for creating small wireless networks on an ad hoc basis. The mechanism, known as a *piconet,* allows two or more Bluetooth devices in close physical proximity to operate on the same channel using the same frequency hopping sequence. An example of a piconet is a Bluetooth-based connection between a cell phone and a headset.

Bluetooth piconets are often established on a temporary and changing basis. This allows for communications flexibility and scalability between mobile devices, and for easy file sharing and synchronization of information between Bluetooth devices. For example, a Bluetooth-enabled device can form a piconet to support file sharing with a laptop computer. With a Bluetooth connection, a laptop computer user can direct a cell phone to establish a connection to the Internet through the phone.

Bluetooth operates in the unlicensed 2.4000 gigahertz (GHz) to 2.4835 GHz Industrial, Scientific, and Medical (ISM) frequency band. Bluetooth devices share this frequency band with other technologies, including wireless local area networks (WLANs) that implement the Institute of Electrical and Electronics Engineers (IEEE) 802.11b/g standard. Bluetooth employs frequency hopping spread spectrum (FHSS) technology for transmissions. FHSS reduces interference and transmission errors but provides for minimal transmission security. A channel is used for a very short period (e.g., 625 microseconds for data/voice links), followed by a hop to another channel designated by a predetermined pseudo-random sequence; this process is repeated continuously in the frequency hopping sequence.

Bluetooth also provides for radio link power control, which allows 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 request that the other network device adjust its relative radio power level by increasing or decreasing the transmission power. This process conserves power and keeps the received signal characteristics within a preferred range.

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 that fosters the development of Bluetooth products and manages the establishment of Bluetooth specifications. The IEEE Wireless Personal Area Networks (WPAN) Task Group 15.1 processed the original technical specifications that were developed for Bluetooth technology. These specifications were approved as a voluntary industry standard and issued as IEEE 802.15.1-2002.

As the technology has advanced, the Task Group has developed new and revised specifications. Bluetooth 1.2 (adopted November 2003) and 2.0 + Enhanced Data Rate (EDR, adopted November 2004) are commonly used versions. The version Bluetooth 2.1 + EDR (adopted July 2007) has been widely implemented. It provides for improved security and supports cryptographic key establishment in the form of Secure Simple Pairing (SSP). The most recent versions include Bluetooth 3.0 + High Speed (HS, adopted April 2009), which provides significant data rate improvements, and Bluetooth 4.0 (adopted June 2010), which includes Low Energy (LE) technology that supports smaller, resource-constrained devices and associated applications.

**NIST Special Publication (SP) 121, Revision 1, *Guide to Bluetooth Security: Recommendations of the National Institute of Standards and Technology***

This updated guide was revised by John Padgette of Accenture, Karen Scarfone of Scarfone Cybersecurity, and Lily Chen of NIST. The Bluetooth versions that are covered in the revised publication are versions 1.1, 1.2, 2.0 + Enhanced Data Rate (EDR), 2.1 + EDR, 3.0 + High Speed (HS), and 4.0, which includes Low Energy (LE) technology.The publication includes the latest vulnerability mitigation information for Secure Simple Pairing, introduced in Bluetooth v2.1 + Enhanced Data Rate (EDR). It also includes an introduction to and discussion of Bluetooth v3.0 + High Speed and security mechanisms and recommendations for Bluetooth v4.0.

The publication provides an overview of Bluetooth technology, including its benefits, technical characteristics, and architecture. The security features that are defined in the Bluetooth specifications and their limitations are discussed. SP 800-121 Rev. 1 analyzes the common vulnerabilities and threats involving Bluetooth technology and recommends countermeasures to improve Bluetooth security. The appendices to the publication include a glossary of terms, a list of acronyms and abbreviations, a reference list, and a compilation of online resources.

NIST SP 800-121 Rev. l is available from the NIST web page here.

**Security Services Available in Bluetooth Specifications**

The Bluetooth specifications provide for three basic security services:

- **Authentication:** verifying the identity of communicating devices based on their Bluetooth device address. Bluetooth does not provide native user authentication.

- **Confidentiality:** protecting information from eavesdropping by ensuring that only authorized devices can access and view transmitted data.

- **Authorization:** allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

Bluetooth does not provide for other security services such as audit, integrity, and non-repudiation; these services should be implemented by other means if they are needed.

**Four security modes** are defined for the family of Bluetooth BR/EDR/HS (basic rate/enhanced data rate/high speed) specifications. Bluetooth devices must operate in one of the security modes. The modes specify when a Bluetooth device initiates security protection, but do not specify whether the device supports security features.

- **Security Mode 1** describes devices that have no capabilities for security authentication and encryption, leaving the devices and connections vulnerable to attackers. These devices do not prevent other Bluetooth-enabled devices from establishing connections, and they can respond to security requests such as for authentication or encryption that are initiated by a remote device. All v2.0 and earlier devices can support Security Mode 1, and v2.1 and later devices can use Security Mode 1 for backward compatibility with older devices.

- **Security Mode 2** is a service level-enforced security mode; security procedures may be initiated after link establishment but before logical channel establishment. A local security manager, as specified in the Bluetooth architecture, controls access to specific services. 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 can 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 provides for authorization to determine whether a specific device is allowed to have access to a specific service. Bluetooth service discovery can be performed prior to any security challenges for authentication, encryption, and/or authorization.

The authentication and encryption mechanisms used for Security Mode 2 are implemented in the controller. All v2.0 and earlier devices can support Security Mode 2, but v2.1 and later devices can only support it for backward compatibility with v2.0 or earlier devices.

- **Security Mode 3** requires Bluetooth devices 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. Service discovery cannot be performed until after authentication, encryption, and authorization have been performed.

Once a device has been authenticated, service-level authorization is not typically performed by a Security Mode 3 device. However, NIST recommends that service-level authorization should be performed to prevent *authentication abuse*, which occurs when an authenticated remote device uses a Bluetooth service without the knowledge of the user of the local device.

All v2.0 and earlier devices can support Security Mode 3, but v2.1 and later devices can only support it for backward compatibility purposes.

- **Security Mode 4** (introduced in Bluetooth v2.1 + EDR) is a service level-enforced security mode in which security procedures are initiated after physical and logical links are established. Security Mode 4 uses Secure Simple Pairing (SSP), in which Elliptic Curve Diffie-Hellman (ECDH) key agreement replaces legacy key agreement for link key generation. The device authentication and encryption algorithms are identical to the algorithms in Bluetooth v2.0 + EDR and earlier versions. Security requirements for services protected by Security Mode 4 must be classified as requiring authenticated link key, requiring unauthenticated link key, or requiring no security.

Authentication of a link key depends on the SSP association model used. Security Mode 4 requires encryption for all services (except Service Discovery) and is mandatory for communication between v2.1 and later BR/EDR devices. Security Mode 4 devices can be backward compatible with any of the other three Security Modes when communicating with Bluetooth v2.0 and earlier devices that do not support Security Mode 4. The use of Security Mode 3 is recommended in this particular case.

Bluetooth technology allows for **different levels of trust and service security.**

The two Bluetooth levels of trust are *trusted* and *untrusted*. A *trusted device* has a fixed relationship with another device and has full access to all services. An *untrusted device* does not have an established relationship with another Bluetooth device, and can only receive restricted access to services.

Available service security levels depend on the security mode being used. For Security Modes 1 and 3, no service security levels are specified. For Security Mode 2, requirements for authentication, encryption, and authorization can be applied.

For Security Mode 4, the Bluetooth specification specifies four levels of security for Bluetooth services for use during Secure Simple Pairing (SSP):

- **Service Level 3** requires man-in-the-middle (MITM) protection and encryption; user interaction is acceptable.
- **Service Level 2** requires encryption only; MITM protection is not necessary.
- **Service Level 1** does not require MITM protection and encryption; user interaction is minimal.
- **Service Level 0** does not require MITM protection, encryption, or user interaction.

The Bluetooth architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices can gain access only to specific services. Although Bluetooth core protocols can only authenticate devices and not users, user-based authentication can be achieved. The Bluetooth security architecture (through the security manager) allows applications to enforce other security procedures.

## Security Threats and Vulnerabilities

Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service (DoS) attacks, eavesdropping, MITM 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 with unauthorized use of Bluetooth devices and other systems or networks to which the devices are connected.

## NIST's Recommendations to Improve the Security of Bluetooth Implementations

NIST recommends that organizations implement the following practices to protect their Bluetooth implementations from security threats and vulnerabilities:

- **Use the strongest Bluetooth security mode that is available for organizational Bluetooth devices.**

The Bluetooth specifications define several security modes, and each version of Bluetooth supports some, but not all, of these modes. The modes differ primarily by the point at which the device initiates security; these modes define how well they protect Bluetooth communications and devices from potential attack.

For Bluetooth Basic Rate (BR), EDR, and HS, Security Mode 3 is the strongest mode because it requires establishment of authentication and encryption before the Bluetooth physical link is completely established. However, Security Mode 4 is the default mode for Bluetooth 2.1+EDR and later devices. If both devices support Security Mode 4, then they must use it. Security Modes 2 and 4 can also use authentication and encryption, but these modes do not initiate them until after the Bluetooth physical link has already been fully established and logical channels have been partially established. Since Security Mode 1 devices never initiate security, NIST recommends that devices operating in Security Mode 1 not be used.

For Bluetooth LE (introduced in Version 4.0), LE Security Mode 1 Level 3 is considered the strongest mode because it requires authenticated pairing and encryption. Other security modes/levels allow unauthenticated pairing, and provide no man-in-the-middle protection during cryptographic key establishment. Some modes do not require any security at all.

The available modes vary based on the Bluetooth specification version supported by the device. Organizations should choose the most secure mode that is available for each device.

- **Address Bluetooth technology in organizational security policies and change default settings of Bluetooth devices to support the adopted policies.**

A security policy that defines 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), where applicable. After establishing a Bluetooth security policy, organizations should ensure that the default settings of Bluetooth devices are reviewed and changed as needed for compliance with the security policy requirements. Unneeded Bluetooth profiles and services should be disabled to reduce the number of vulnerabilities that attackers might exploit. When available, a centralized approach to security policy management should be used to ensure that device configurations are compliant.

- **Ensure that all Bluetooth users in an organization are informed about their responsibilities regarding the secure use of Bluetooth devices.**

A security awareness program helps educate and train users to follow security practices that protect the assets of an organization and prevent security incidents. 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 advised of other actions that they should take; for example, ensure that Bluetooth devices are turned off when they are not needed to minimize exposure to malicious activities, and perform Bluetooth device pairing infrequently and preferably in a physically secure area where attackers cannot observe passkey entry and eavesdrop on Bluetooth pairing-related communications.

**For More 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) 140-2, *Security Requirements for Cryptographic Modules*
FIPS 180-4, *Secure Hash Standard (SHS)*
FIPS 197, *Advanced Encryption Standard (AES)*
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
NIST SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
NIST SP 800-53, Rev. 3, *Recommended Security Controls for Federal Information Systems and Organizations*
NIST SP 800-63, Rev. 1, *Electronic Authentication Guideline*
NIST SP 800-64, Rev. 2, *Security Considerations in the System Development Life Cycle*
NIST SP 800-70, Rev. 2, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*
NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*

For information about the NIST standards and guidelines that are listed above, as well as other security-related publications, see here.

Bluetooth-related information and links to other sources of information about Bluetooth are available from the Bluetooth SIG website here.

Information about IEEE activities that support standards for Bluetooth technology can be found on the IEEE website here.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

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.