ITL BULLETIN FOR JULY 2017

UPDATED NIST GUIDANCE FOR BLUETOOTH SECURITY

Lily Chen, Larry Feldman,[1] and Greg Witte,[1] Editors
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

Introduction

NIST's Information Technology Laboratory has published Special Publication (SP) 800-121 Revision 2, Guide to Bluetooth Security, to provide an updated overview of Bluetooth wireless technology and to discuss related security concerns. The publication will help guide Bluetooth implementers, such as systems engineers and architects who design and apply Bluetooth wireless technologies and will also help those who oversee and review use and security of Bluetooth within their organizations.

This article provides an overview of Bluetooth wireless technology and highlights key information from Special Publication (SP) 800-121 Revision 2 about Bluetooth's security features, its vulnerabilities, and ways to address these vulnerabilities and make this technology more secure.

Overview of Bluetooth Wireless Technology

Bluetooth is a technology for short-range radio frequency communication that is used primarily to establish wireless personal area networks (WPANs). Bluetooth has been integrated into many types of business and consumer devices, including cell phones, laptops, automobiles, printers, keyboards, mice, headsets, and, more recently, medical devices, and personal devices (such as smart watches, home appliances, and fitness monitors). Thanks to Bluetooth technology, a wide variety of devices can be connected to the Internet. Devices that are connected to the Internet – whether through Bluetooth technology or another technology – form what is called the Internet of things

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.*[2] A piconet consists 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 connection between a cell phone and a headset using Bluetooth wireless technology.

[1] Larry Feldman and Greg Witte are Guest Researchers from G2, Inc.
[2]The term "piconet" applies to both ad hoc and infrastructure Bluetooth networks.

Bluetooth piconets are often established on a temporary and changing basis, which offers flexibility and scalability in communication between mobile devices. Some key benefits of Bluetooth are:

- **Cable replacement.** Bluetooth replaces a variety of cables, such as those traditionally used for peripheral devices (e.g., mouse and keyboard connections), printers, and wired headsets and earbuds that interface with desktops, laptops, and cell phones.

- **Ease of file sharing.** A Bluetooth-enabled device can form a piconet to support file sharing capabilities with other Bluetooth devices, such as laptops.

- **Wireless synchronization.** Bluetooth can provide automatic synchronization between Bluetooth-enabled devices. For example, Bluetooth allows synchronization of contact information between smartphones and cars.

- **Internet connectivity.** A Bluetooth device with Internet connectivity can share that access with other Bluetooth devices. For example, a laptop can use a Bluetooth connection to leverage the personal hotspot capability of a smartphone to provide Internet access to the laptop.

Bluetooth 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 developed to drive development of Bluetooth products and serve as the governing body for Bluetooth specifications. Bluetooth is standardized within the IEEE 802.15 Working Group for Wireless Personal Area Networks that formed in 1999 as IEEE 802.15.1-2002.

Several Bluetooth versions are currently being used in commercial devices. The most recent version is Bluetooth 5.0 (adopted in December 2016).[3] Other recent versions are Bluetooth 4.1 and Bluetooth 4.2. Bluetooth 4.1 (adopted in December 2013) improved the strengths of the Basic Rate/Enhanced Data Rate (BR/EDR) technology cryptographic key, device authentication, and encryption by making use of Federal Information Processing Standard (FIPS)-approved algorithms. Bluetooth 4.2 (adopted in December 2014) improved the strength of the low-energy technology cryptographic key by making use of FIPS-approved algorithms and provided the means to convert BR/EDR technology keys to low-energy technology keys, and vice versa.

The emergence of the Bluetooth Low-Energy (BLE) standards (version 4.0/4.1/4.2), which complement the BR/EDR standards, made Bluetooth one of the most important communication protocols of the Internet of Things. BLE is supported on every smartphone and smart watch shipped since 2012, allowing users to interact easily and directly with Internet-of-Things applications using their own device without the need for a gateway.

[3] At the time of SP 800-121 Revision 2 publication, Bluetooth 4.0 (adopted June 2010) was the most prevalent.

Bluetooth Security Features

NIST SP 800-121 Revision 2 provides an overview of the security mechanisms included in the Bluetooth specifications, illustrating some limitations and providing a foundation for NIST's security recommendations. A high-level example of the scope of the security for the Bluetooth radio path is shown in Figure 1.

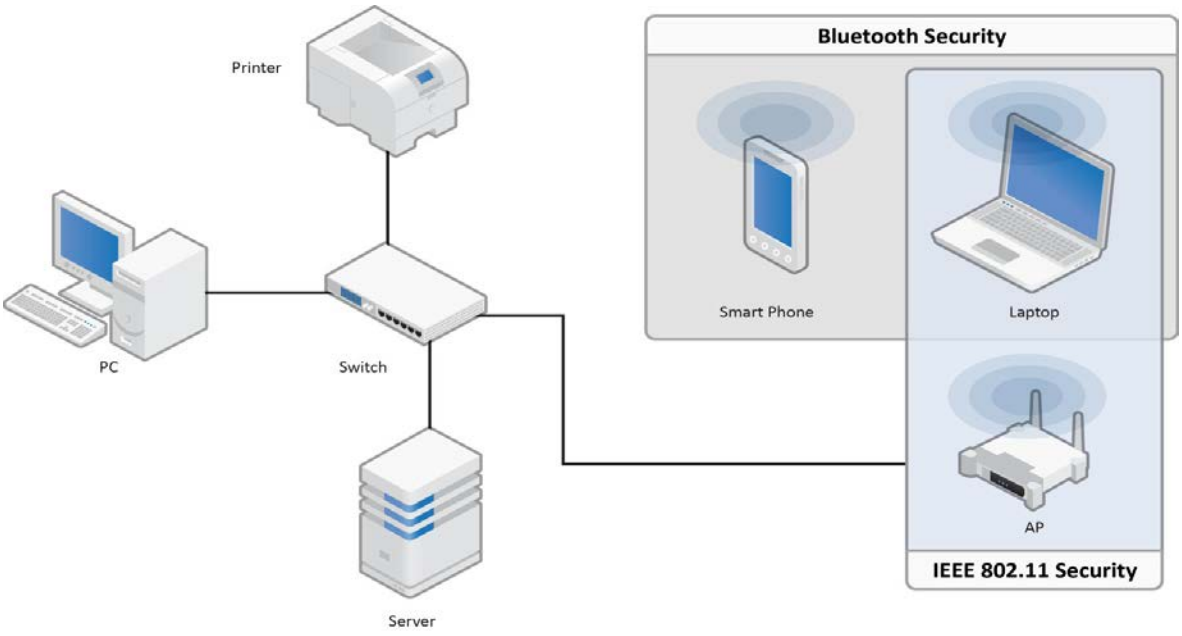

Figure 1. Example of the scope of the security for the Bluetooth radio path. In this example, Bluetooth security is provided between the smartphone and the laptop, while IEEE 802.11 security protects the WLAN link between the laptop and the IEEE 802.11 AP. Communications on the wired network are not protected by Bluetooth or IEEE 802.11 security capabilities. Therefore, end-to-end security is not possible without using higher-layer security solutions in addition to the security features included in Bluetooth and IEEE 802.11.

Five basic security services are specified in the Bluetooth standard:

- **Authentication:** verifying the identity of communicating devices based on their Bluetooth address. Bluetooth does not provide native user authentication.
- **Confidentiality:** preventing information compromise caused by 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.
- **Message Integrity:** verifying that a message sent between two Bluetooth devices has not been altered in transit.
- **Pairing/Bonding:** creating one or more shared secret keys and the storing of these keys for use in subsequent connections to form a trusted device pair.

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; hence, these modes define how well they protect Bluetooth communications and devices from potential attack. Some security modes have configurable security-level settings which affect the security of the connections.

NIST SP 800-121 Revision 2 describes the security services offered by Bluetooth and gives details about its security modes. Bluetooth does not address other security services such as audit and non-repudiation; if such services are needed, they should be provided through additional means.

Bluetooth Vulnerabilities, Threats, and Countermeasures

Security mechanisms recommended in SP 800-121 Revision 2 are critical because Bluetooth wireless technology and associated devices are susceptible to general wireless networking threats, such as denial-of-service attacks, eavesdropping, man-in-the-middle (MITM) attacks, message modification, and resource misappropriation. These devices are also threatened by more specific attacks related to Bluetooth wireless technology 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 use of Bluetooth devices and other systems or networks to which the devices are connected.

Organizations that are planning to use Bluetooth 4.0, 4.1, or 4.2 technologies should carefully consider the security implications. The 4.0 specification was released in mid-2010, and the 4.2 specification was released in December 2014. At the time of writing NIST SP 800-121 Revision 2, one significant security vulnerability related to 4.0 has been discovered. Additionally, few products that support the 4.2 specification are currently available for evaluation. As more compliant products become available, additional vulnerabilities will possibly be discovered, and additional recommendations will be needed for effectively securing Bluetooth low energy devices. Organizations planning to deploy Bluetooth low energy devices should carefully monitor developments involving new vulnerabilities, threats, and additional security-control recommendations.

NIST SP 800-121 Revision 2 provides a Bluetooth security checklist with guidelines and recommendations for creating and maintaining secure Bluetooth piconets. For each recommendation or guideline in the checklist, a justification lists areas of concern for Bluetooth devices, the security threats and vulnerabilities associated with those areas, risk mitigations for securing the devices from these threats, and vulnerabilities. The recommendations can be summarized for users and system administrators as follows:

- Use the strongest Bluetooth security mode that is available for their Bluetooth devices.
- Address Bluetooth wireless technology in their security policies and change default settings of Bluetooth devices to reflect the policies.
- Ensure that Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use.

Summary

NIST SP 800-121 Revision 2 provides an overview of Bluetooth wireless technology and information on the security capabilities of Bluetooth. Based on analysis of possible threats and vulnerabilities, this publication gives recommendations to organizations employing Bluetooth wireless technologies on securing them effectively.

ITL Bulletin Publisher: Elizabeth B. Lennon
Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov