Withdrawn NIST Technical Series Publication

Warning Notice

The attached publication has been withdrawn (archived), and is provided solely for historical purposes. It may have been superseded by another publication (indicated below).

Withdrawn Publication	
Series/Number	NIST Special Publication 800-121 Rev. 2
Title	Guide to Bluetooth Security
Publication Date(s)	May 2017
Withdrawal Date	January 19, 2022
Withdrawal Note	SP 800-121 Rev. 2 has been updated, and is superseded in its entirety by the publication of SP 800-121 Rev. 2 (1/19/22 update).

Superseding Publication(s) *(if applicable)*

The attached publication has been **superseded by** the following publication(s):

Series/Number	NIST Special Publication 800-121 Rev. 2 (update 1)
Title	Guide to Bluetooth Security
Author(s)	John Padgette; John Bahr; Mayank Batra; Marcel Holtmann; Rhonda Smithbey; Lily Chen; Karen Scarfone
Publication Date(s)	May 2017 (includes updates as of 1/19/2022)
URL/DOI	https://doi.org/10.6028/NIST.SP.800-121r2-upd1

Additional Information *(if applicable)*

Contact	Computer Security Division (Information Technology Laboratory)
Latest revision of the attached publication	
Related Information	https://csrc.nist.gov/publications/detail/sp/800-121/rev-2/final
Withdrawal Announcement Link	

Date updated: January 19, 2022

National Institute of Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-121
Revision 2

Guide to Bluetooth Security

John Padgette
John Bahr
Mayank Batra
Marcel Holtmann
Rhonda Smithbey
Lily Chen
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

C O M P U T E R S E C U R I T Y

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-121
Revision 2

Guide to Bluetooth Security

John Padgette
Accenture Federal Services
Arlington, VA

Rhonda Smithbey
Spanalytics
Richmond, VA

John Bahr
Bahr Engineering
Superior, CO

Lily Chen
Computer Security Division
Information Technology Laboratory

Mayank Batra
Qualcomm Tech. Intl., Ltd.
Cambridge, United Kingdom

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

Marcel Holtmann
Intel Corporation
Munich, Germany

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

May 2017

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-121 Revision 2
Natl. Inst. Stand. Technol. Spec. Publ. 800-121 Rev. 2, 67 pages (May 2017)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-121r2

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: 800-121r2comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Bluetooth wireless technology is an open standard for short-range radio frequency communication used primarily to establish wireless personal area networks (WPANs), and has been integrated into many types of business and consumer devices. This publication provides information on the security capabilities of Bluetooth and gives recommendations to organizations employing Bluetooth wireless technologies on securing them effectively. The Bluetooth versions within the scope of this publication are versions 1.1, 1.2, 2.0 + Enhanced Data Rate (EDR), 2.1 + EDR, 3.0 + High Speed (HS), 4.0, 4.1, and 4.2. Versions 4.0 and later support the low energy feature of Bluetooth.

Keywords

Bluetooth; information security; network security; wireless networking; wireless personal area networks

Acknowledgments

The authors, John Padgette of Accenture, John Bahr of Bahr Engineering (representing Philips Healthtech), Mayank Batra of Qualcomm, Marcel Holtmann of Intel, Rhonda Smithbey of Spanalytics, Lily Chen of the National Institute of Standards and Technology (NIST), and Karen Scarfone of Scarfone Cybersecurity, wish to thank their colleagues in the Bluetooth Security Experts Group (SEG) who contributed technical content and reviewed drafts of this document. The authors greatly appreciate the comments and feedback provided by Mark Nichols of Spanalytics, and the contributions of Alan Kozlay of Biometric Associates, LP. The authors would also like to acknowledge Catherine Brooks of the Bluetooth SIG technical staff for providing the new graphics.

Note to Readers

This document is the second revision to NIST SP 800-121, Guide to Bluetooth Security. Updates in this revision include an introduction to and discussion of Bluetooth 4.1 and 4.2 security mechanisms and recommendations, including Secure Connections for BR/EDR and low energy.

Executive Summary

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth wireless technology 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, medical devices, printers, keyboards, mice, headsets, and, more recently, medical devices and personal devices (such as smart watches, music speakers, home appliances, fitness monitors, and trackers). This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data. This document provides an overview of Bluetooth wireless technology and discusses related security concerns.

Several Bluetooth versions are currently in use in commercial devices, while the most current version can be found at bluetooth.com. At the time of writing, Bluetooth 4.0 (adopted June 2010) is the most prevalent. The most recent versions include Bluetooth 4.1 and Bluetooth 4.2. Bluetooth 4.1 (adopted 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 December 2014) improved the strength of the low energy technology cryptographic key by making use of FIPS-approved algorithms, and provided means to convert BR/EDR technology keys to low energy technology keys and vice versa. This publication addresses the security of all versions of Bluetooth.

Bluetooth wireless technology and associated devices are susceptible to general wireless networking threats, such as denial of service (DoS) attacks, eavesdropping, man-in-the-middle (MITM) attacks, message modification, and resource misappropriation. They 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.

To improve the security of Bluetooth implementations, organizations should implement the following recommendations:

Organizations should use the strongest Bluetooth security mode that is available for their 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; 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.

For Bluetooth 4.1 devices that have BR, EDR, and High Speed (HS) features, Security Mode 4, Level 4 is recommended because it requires Secure Connections, which uses authenticated pairing and encryption using 128-bit strength keys generated using FIPS-approved Advanced Encryption Standard (AES) encryption. For Bluetooth 2.1 through 4.0 devices, Security Mode 4, Level 3 is the

most secure, and for Bluetooth 2.0 and older devices Security Mode 3 is recommended. Security Modes 2 and 4 can also use authentication and encryption, but do not initiate them until after the Bluetooth physical link has already been fully established and logical channels partially established. Security Mode 1 devices never initiate security and therefore should never be used.

For the low energy feature of Bluetooth (introduced in Version 4.0 and updated in 4.1 and 4.2), Security Mode 1 Level 4 is the strongest mode because it requires authenticated low energy Secure Connections pairing with Elliptic Curve Diffie-Hellman (ECDH) based encryption. Security Mode 1 Level 3 requires authenticated pairing and encryption but does not use ECDH-based cryptography and thus provides limited eavesdropping protection due to weak encryption. Other security modes/levels allow unauthenticated pairing (meaning no MITM protection is provided during cryptographic key establishment), and some do not require any security at all.

The available modes vary based on the Bluetooth specification version supported by the device, so organizations should choose the most secure mode available for each case.

Organizations should address Bluetooth wireless technology in their security policies and change default settings of Bluetooth devices to reflect the 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, if they are used, requirements for selecting and using Bluetooth personal identification numbers (PINs).[1] A baseline configuration for Bluetooth default settings should accompany the security policy. The checklist in Table 4-2 provides a "Technical Recommendations" section which may be used as a guide. After establishing a Bluetooth security policy, organizations should ensure that Bluetooth devices' default settings are reviewed and changed as needed so that they comply with the security policy requirements. For example, a typical requirement is to disable unneeded Bluetooth profiles and services 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.

Organizations should ensure that their Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use.

Annual required security awareness programs should be updated to include Bluetooth security policy guidelines. A security awareness program helps educate and train users to follow security practices that protect the assets of an organization and prevent security incidents. For example, users should be provided with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft. Users should also be made aware of other actions to take regarding 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

[1] Starting with Simple Secure Pairing in Bluetooth 2.1, PINs are not used for pairing any more.

pairing as infrequently as possible and ideally in a physically secure area where attackers cannot observe passkey entry and eavesdrop on Bluetooth pairing-related communications.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide information to organizations on the security capabilities of Bluetooth and provide recommendations to organizations employing Bluetooth wireless technologies on securing them effectively. The Bluetooth versions within the scope of this publication are versions 1.1, 1.2, 2.0 + Enhanced Data Rate (EDR), 2.1 + EDR, 3.0 + High Speed (HS), 4.0, 4.1, and 4.2. Bluetooth with low energy functionality is present in 4.0 and later. Bluetooth 5.0 is not in the scope of this document.

1.2 Audience and Assumptions

This document discusses Bluetooth wireless technologies and security capabilities in technical detail. This document assumes that the readers have at least some operating system, wireless networking, and security knowledge. Because of the constantly changing nature of the wireless security industry and the threats and vulnerabilities to the technologies, readers are strongly encouraged to take advantage of other resources (including those listed in this document) for more current and detailed information.

The following list highlights people with differing roles and responsibilities that might use this document:

- Government managers (e.g., chief information officers and senior managers) who oversee the use and security of Bluetooth within their organizations
- Systems engineers and architects who design and implement Bluetooth wireless technologies
- Auditors, security consultants, and others who perform security assessments of wireless environments
- Researchers and analysts who are trying to understand the underlying wireless technologies.

1.3 Document Organization

The remainder of this document is composed of the following sections and appendices:

- Section 2 provides an overview of Bluetooth wireless technology, including its benefits, technical characteristics, and architecture.
- Section 3 discusses the security features defined in the Bluetooth specifications and highlights their limitations.
- Section 4 examines common vulnerabilities and threats involving Bluetooth wireless technologies and makes recommendations for countermeasures to improve Bluetooth security.
- Appendix A provides a glossary of terms.
- Appendix B provides a list of acronyms and abbreviations used in this document.
- Appendix C lists Bluetooth functions.

- Appendix D lists Bluetooth references.
- Appendix E lists Bluetooth online resources.

2 Overview of Bluetooth Wireless Technology

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth 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, music speakers, home appliances, fitness monitors, and trackers). This allows users to form ad hoc networks between a wide variety of devices to transfer voice and data. 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 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 connection between a cell phone and a headset using Bluetooth wireless technology.

Bluetooth piconets are often established on a temporary and changing basis, which offers communications flexibility and scalability 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, cell phones, etc.
- **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 automobiles.
- **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.[3] 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.[4]

This section provides an overview of Bluetooth, including frequency and data rates, range, and architecture.

---

2 As discussed in Section 2.2, the term “piconet” applies to both ad hoc and infrastructure Bluetooth networks.

3 The Bluetooth SIG website (https://www.bluetooth.com/) is a resource for Bluetooth related information and provides numerous links to other sources of information.

4 For more information, see the IEEE website at http://grouper.ieee.org/groups/802/15/.

2.1 Bluetooth Wireless Technology Characteristics

Bluetooth operates in the unlicensed 2.4000 gigahertz (GHz) to 2.4835 GHz Industrial, Scientific, and Medical (ISM) frequency band. Numerous technologies operate in this band, including the IEEE 802.11b/g/n wireless local area network (WLAN) standard, making it somewhat crowded from the standpoint of the volume of wireless transmissions. Bluetooth employs frequency hopping spread spectrum (FHSS) technology for transmissions. FHSS reduces interference and transmission errors but provides minimal transmission security.

With FHSS technology, communications between Bluetooth Basic Rate (BR)/EDR devices use 79 different 1 megahertz (MHz) radio channels by hopping (i.e., changing) frequencies about 1600 times per second for data/voice links and 3200 times per second during page and inquiry scanning. A channel is used for a very short period (e.g., 625 μs for data/voice links), followed by a hop to another channel designated by a pre-determined pseudo-random sequence; this process is repeated continuously in the frequency hopping sequence.

Bluetooth low energy communication uses the same frequency range as BR/EDR devices but splits it instead into 40 channels of 2 MHz width. Three of these channels are used for advertising (broadcasting data and for connection setup) and the other 37 are data channels. These 40 channels, combined with a time division multiple access (TDMA) scheme, provide the two multiple access schemes for the low energy feature of Bluetooth. A polling scheme is used in which the first device sends a packet at a predetermined time and a corresponding device responds after a predetermined interval. These exchanges of data are known as either Advertising or Connection Events.

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 (i.e., incrementally increase or decrease the transmission power). This is performed to conserve power and/or to keep the received signal characteristics within a preferred range.

The combination of a frequency hopping scheme and radio link power control provides Bluetooth with some additional, albeit limited, protection from eavesdropping and malicious access. The frequency-hopping scheme, primarily a technique to avoid interference, makes it slightly more difficult for an adversary to locate and capture Bluetooth transmissions than to capture transmissions from fixed-frequency technologies, like those used in IEEE 802.11b/g. Research has shown that the Bluetooth frequency hopping sequence for an active piconet can be determined using relatively inexpensive hardware and free open source software.[5]

The range of Bluetooth BR/EDR devices is characterized by three classes that define power management. Table 2-1 summarizes the classes, including their power levels in milliwatts (mW) and decibels referenced to one milliwatt (dBm), and their operating ranges in meters (m).[6] Most small, battery-powered devices are Class 2, while Class 1 devices are typically universal serial bus (USB)

---

5 Spill, Dominic and Bittau, Andrea, *BlueSniff: Eve meets Alice and Bluetooth,* 2007.

6 The ranges listed in Table 2-1 are the designed operating ranges. Attackers may be able to intercept communications at significantly larger distances, especially if they use high-gain antennas and high-sensitivity receivers.

adapters for desktops and laptops, as well as access points and other mains powered devices. Many Bluetooth low energy devices are designed to run on very small batteries for a long period of time.

Table 2-1. Bluetooth Device Classes of Power Management

Type	Power	Max Power Level	Designed Operating Range	Sample Devices
Class 1	High	100 mW (20 dBm)	Up to 100 m (328 feet)	USB adapters, access points
Class 1.5 (low energy)[7]	Med-High	10 mW (10 dBm)	Up to 30 m (100 feet), but typically 5 m (16 feet)	Beacons, wearable sensors
Class 2	Medium	2.5 mW (4 dBm)	Up to 10 m (33 feet)	Mobile devices, Bluetooth adapters, smart card readers
Class 3	Low	1 mW (0 dBm)	Up to 1 m (3 feet)	Bluetooth adapters

To allow Bluetooth devices to find and establish communication with each other, discoverable and connectable modes are specified. A device in *discoverable mode* periodically monitors an inquiry scan physical channel (based on a specific set of frequencies) and responds to an inquiry on that channel with its device address, local clock (counter) value, and other characteristics needed to page and subsequently connect to it. A device in *connectable mode* periodically monitors its page scan physical channel and responds to a page on that channel to initiate a network connection. The frequencies associated with the page scan physical channel for a device are based on its Bluetooth address. Therefore, knowing a device's address and local clock[8] is important for paging and subsequently connecting to the device.

The following sections cover Bluetooth BR/EDR/HS data rates, low energy technology, and dual mode devices.

2.1.1 Basic, Enhanced, and High Speed Data Rates

Bluetooth devices can support multiple data rates using native Bluetooth and alternate Media Access Control (MAC) and Physical (PHY) Layers. Bluetooth specifications are designed to be backward compatible; a later specification device that supports higher data rates also supports the lower data rates supported by earlier specification devices (e.g., an EDR device also supports rates specified for BR devices). The following sections provide an overview for Bluetooth and alternate MAC/PHYs, as well as associated data rates and modulation schemes.

2.1.1.1 Basic Rate/Enhanced Data Rate

Bluetooth versions 1.1 and 1.2 only support transmission speeds of up to 1 megabit per second (Mbps), which is known as Basic Rate (BR), and can achieve payload throughput of approximately

[7] Bluetooth Core Specification Addendum (CSA) v5 introduced Power Class 1.5 (10mW), which was the maximum output power of Bluetooth low energy 4.0-4.2 devices. CSA v5 also increased the maximum output power for low energy devices to 100mW as long as local regulatory bodies allow it.

[8] Having a remote device's clock information is not needed to make a connection, but it will speed up the connection process.

720 kilobits per second (kbps). Introduced in Bluetooth version 2.0, EDR specifies data rates up to 3 Mbps and throughput of approximately 2.1 Mbps.

BR uses Gaussian Frequency-Shift Keying (GFSK) modulation to achieve a 1 Mbps data rate. EDR uses π/4 rotated Differential Quaternary Phase Shift Keying (DQPSK) modulation to achieve a 2 Mbps data rate, and 8 Phase Differential Phase Shift Keying (8DPSK) to achieve a 3 Mbps data rate.

Note that EDR support is not required for devices compliant with the Bluetooth 2.0 specification or later. Therefore, there are devices on the market that are "Bluetooth 2.0 compliant" versus "Bluetooth 2.0 + EDR compliant." The former are devices that support required version 2.0 features but only provide the BR data rate.

2.1.1.2 High Speed with Alternate MAC/PHY

Introduced in the Bluetooth 3.0 + HS specification, devices can support faster data rates by using Alternate MAC/PHYs (AMP). This is known as Bluetooth high speed technology.

In the Bluetooth 3.0 + HS specification, IEEE 802.11-2007 was introduced as the first supported AMP. IEEE 802.11-2007 is a rollup of the amendments IEEE 802.11a through 802.11j. For the 802.11 AMP, IEEE 802.11g PHY support is mandatory, while IEEE 802.11a PHY support is optional. The 802.11 AMP is designed to provide data rates up to 24 Mbps using Orthogonal Frequency-Division Multiplexing (OFDM) modulation.

Note that this AMP is IEEE 802.11 compliant but not Wi-Fi compliant. Therefore, Wi-Fi Alliance specification compliance is not required for Bluetooth 3.0 + HS devices.

2.1.2 Low Energy

Bluetooth low energy was introduced in the Bluetooth 4.0 specification and updated in 4.1 and 4.2. Formerly known as "Wibree" and "Ultra Low Power Bluetooth," low energy is primarily designed to bring Bluetooth to coin cell battery-powered devices such as medical devices and other sensors. The key technology goals of Bluetooth low energy (compared with Bluetooth BR/EDR) include lower power consumption, reduced memory requirements, efficient discovery and connection procedures, short packet lengths, and simple protocols and services.

Table 2-2 provides the key technical differences between BR/EDR and low energy.

Table 2-2. Key Differences Between Bluetooth BR/EDR and Low Energy

Characteristic	Bluetooth BR/EDR		Bluetooth Low Energy	
	Prior to 4.1	4.1 onwards	Prior to 4.2	4.2 onwards
RF Physical Channels	79 channels with 1 MHz channel spacing		40 channels with 2 MHz channel spacing	
Discovery/Connect	Inquiry/Paging		Advertising	
Number of Piconet Slaves	7 (active)/255 (total)		Unlimited	
Device Address Privacy	None		Private device addressing available	
Max Data Rate	1–3 Mbps		1 Mbps via GFSK modulation	
Pairing Algorithm	Prior to 2.1: E21/E22/SAFER+ 2.1-4.0: P-192 Elliptic Curve[9], HMAC-SHA-256	P-256 Elliptic Curve, HMAC-SHA-256	AES-128	P-256 Elliptic Curve, AES-CMAC
Device Authentication Algorithm	E1/SAFER	HMAC-SHA-256	AES-CCM[10]	
Encryption Algorithm	E0/SAFER+	AES-CCM	AES-CCM	
Typical Range	30 m		50 m	
Max Output Power	100 mW (20 dBm)		10 mW (10 dBm)[11]	

2.1.3 Dual Mode Devices (Concurrent Low Energy & BR/EDR/HS Support)

A Bluetooth 4.0 or later device may support both BR/EDR/HS and low energy as a "dual mode" Bluetooth device. An example is a cell phone that uses an EDR link to a Bluetooth headset and a concurrent low energy link to a sensor that unlocks and starts the user's automobile. Figure 2-1 shows the device architecture for Bluetooth 4.x devices, and includes BR/EDR, HS, and low energy technologies. New terms included in the figure related to security are discussed in subsequent sections.

[9] For more information about P-192, see FIPS 186-4, *Digital Signature Standards (DSS)*.

[10] There is no dedicated device authentication algorithm in low energy. Encrypting the link also successfully authenticates the remote device.

[11] Core Specification Addendum 5 (CSA5) changed this to 100 mW (20 dBm) as long as the regulatory bodies permit it.

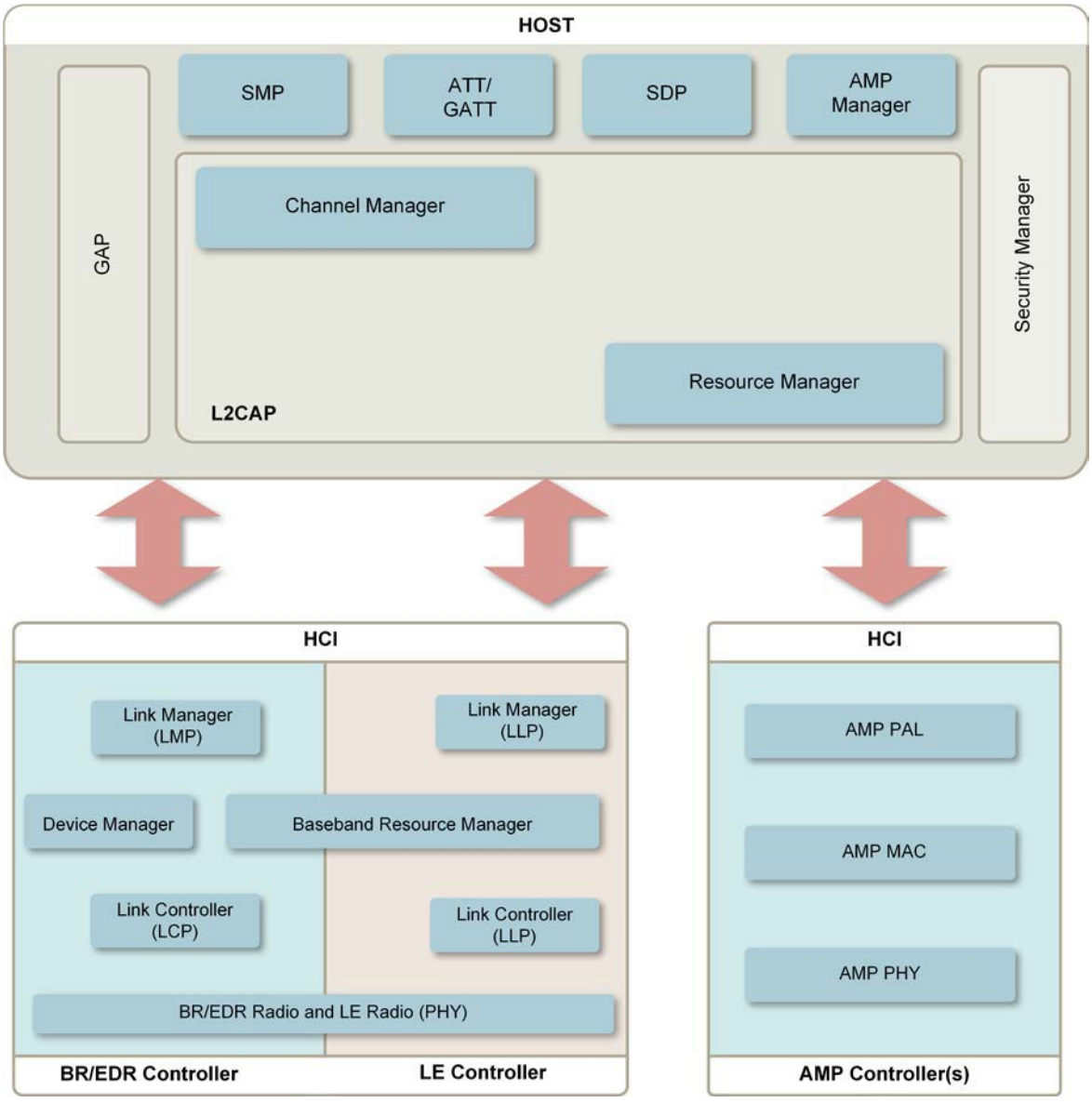

Figure 2-1. Bluetooth 4.x Device Architecture

2.2 Bluetooth Architecture

Bluetooth permits devices to establish ad hoc networks. Ad hoc networks allow easy connection establishment between devices in the same physical area (e.g., the same room) without the use of any infrastructure devices. A Bluetooth client is simply a device with a Bluetooth radio and software incorporating the Bluetooth protocol stack and interfaces.

The Bluetooth specification provides separation of duties for performing stack functions between a host and a controller. The host is responsible for the higher layer protocols, such as Logical Link Control and Adaptation Protocol (L2CAP) and Service Discovery Protocol (SDP). The host functions are performed by a computing device like a laptop or smartphone. The controller is responsible for the lower layers, including the Radio, Baseband, and Link Control/Management.

The controller functions are performed by an integrated or external (e.g., USB) Bluetooth adapter. The host and controller send information to each other using standardized communications over the Host Controller Interface (HCI). This standardized HCI allows hosts and controllers from different product vendors to interoperate. In some cases, the host and controller functions are integrated into a single device; Bluetooth headsets are a prime example.

Figure 2-2 depicts the basic Bluetooth network topology. In a piconet one device serves as the master, with all other devices in the piconet acting as slaves. BR/EDR piconets can scale to include up to 7 active slave devices and up to 255 inactive slave devices. Bluetooth low energy (see Section 2.1.2) allows an unlimited number of slaves, which is known as the low energy Peripheral role, with the master being the low energy Central role. The other two low energy device roles, Broadcaster and Observer, are discussed below in this section.

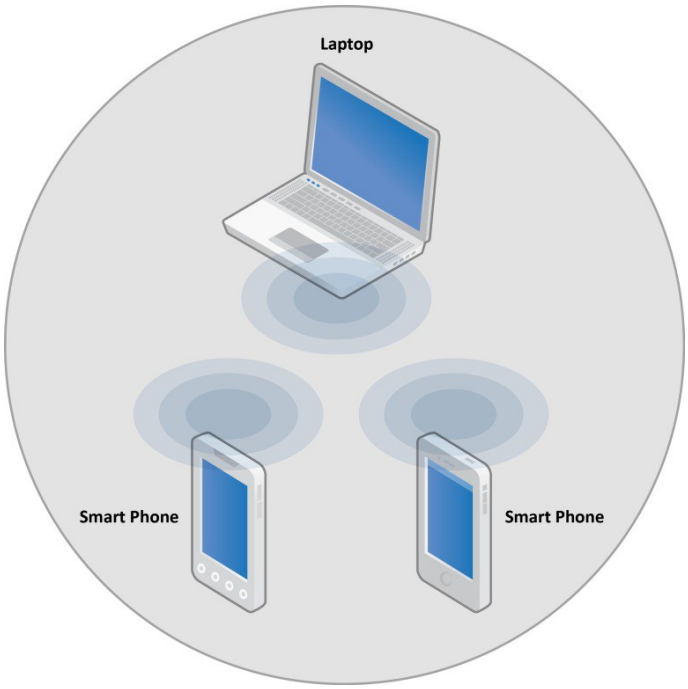

Figure 2-2. Bluetooth Ad Hoc Topology

The master device controls and establishes the network, including defining the network's frequency hopping scheme. Although only one device can serve as the master for each piconet, time division multiplexing (TDM) allows a slave in one piconet to act as the master for another piconet simultaneously, thus creating a chain of networks.[12] This chain, called a *scatternet*, allows networking of several devices over an extended distance in a dynamic topology that can change during any given session. As a device moves toward or away from the master device the topology may change, along with the relationships of the devices in the immediate network. Figure 2-3 depicts a scatternet that involves three piconets.

[12] Note that a particular device can only be the master of one piconet at any given time.

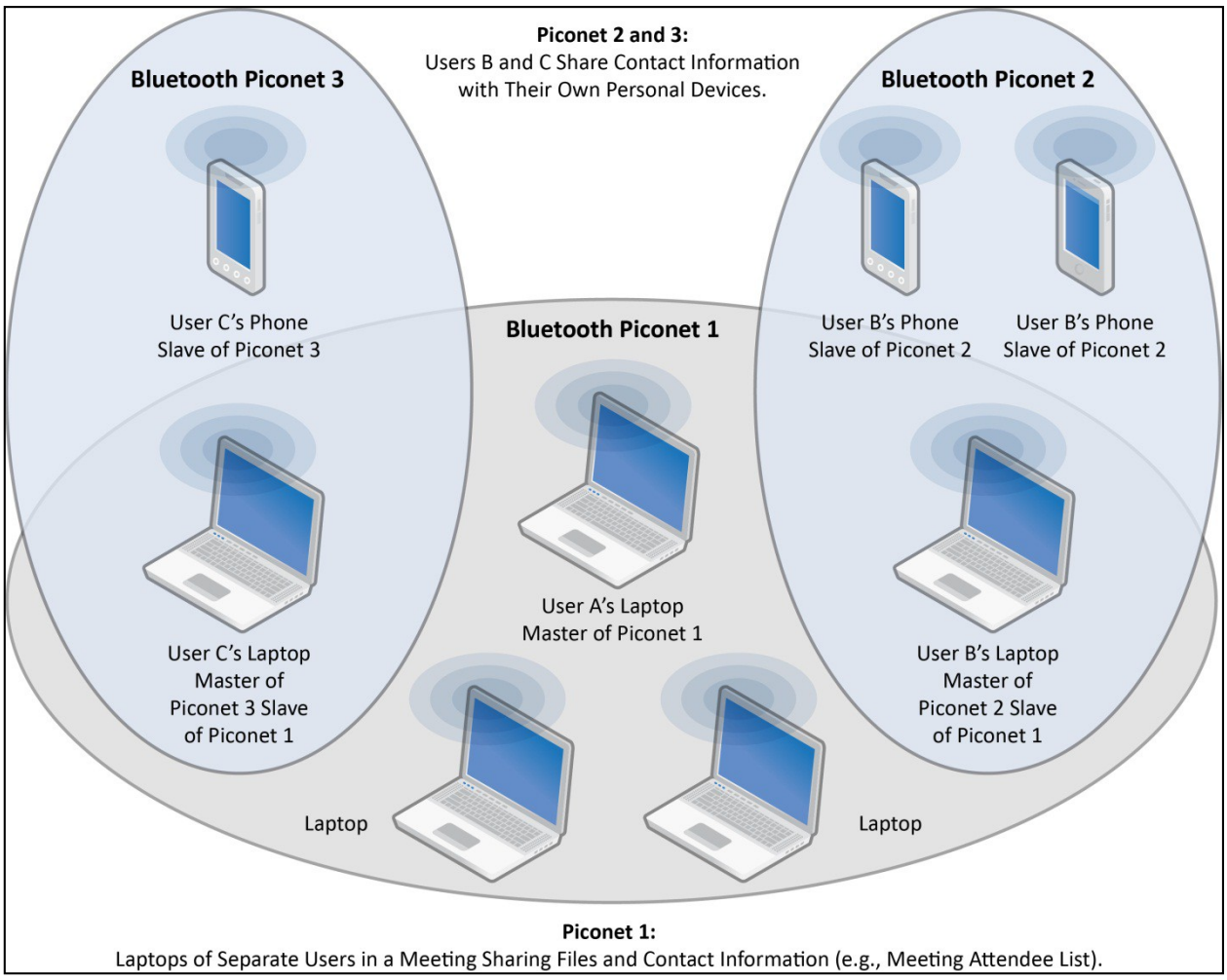

Figure 2-3. Bluetooth Networks (Multiple Scatternets)

The Bluetooth core protocols provide no multi-hop network routing capabilities for devices involved in scatternets. For example, in Figure 2-3, User C's phone in Piconet 3 cannot communicate with User B's phones in Piconet 2 without establishing an additional piconet between them.

Scatternets are supported by both BR/EDR and low energy technologies.

Low energy functionality also supports a connectionless broadcast architecture where Broadcasters (low energy device role) periodically send data, and Observers (low energy device role) listen and consume that data. This allows a device to transmit data to more than one peer at a time. The broadcasting function is a subset of the Advertising capability used in the low energy connection architecture.

3 Bluetooth Security Features

This section provides an overview of the security mechanisms included in the Bluetooth specifications to illustrate their limitations and provide a foundation for the security recommendations in Section 4. A high-level example of the scope of the security for the Bluetooth radio path is depicted in Figure 3-1. In this example, Bluetooth security is provided between the phone and the laptop, while IEEE 802.11 security protects the WLAN link between the laptop and the IEEE 802.11 access point (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 atop the security features included in Bluetooth and IEEE 802.11.

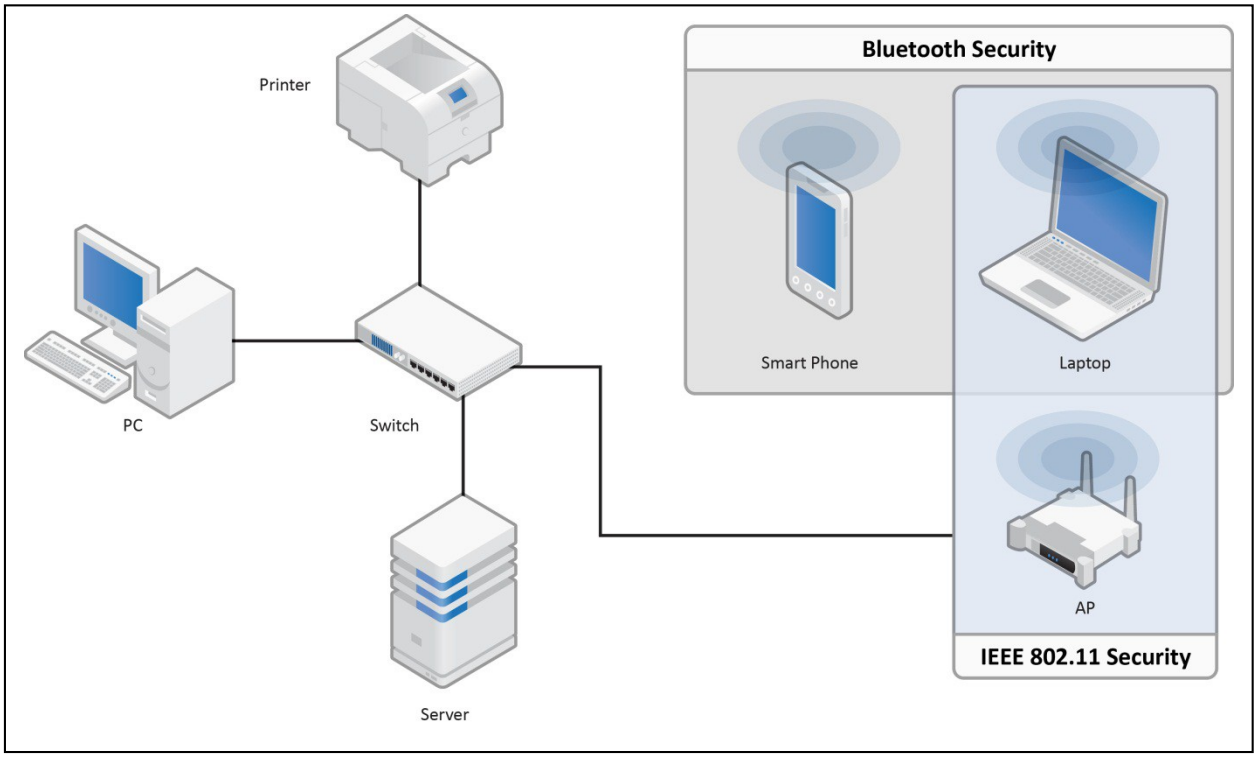

Figure 3-1. Bluetooth Air-Interface Security

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 in order to form a trusted device pair.

The security services offered by Bluetooth and details about the modes of security are described below. 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.

3.1 Security Features of Bluetooth BR/EDR/HS

Bluetooth BR/EDR/HS defines authentication and encryption security procedures that can be enforced during different stages of communication setup between peer devices. Link-level enforced refers to authentication and encryption setup procedures which occur before the Bluetooth physical link is completely established. Service-level enforced refers to authentication and encryption setup procedures which occur after the Bluetooth physical link has already been fully established and logical channels partially established.

Until Bluetooth 2.0, three modes were defined which specified whether authentication and encryption would be link-level enforced or service-level enforced and that enforcement was configurable.

In Bluetooth 2.1, a fourth mode was added which redefined the user experience during pairing, and required that if both devices are Bluetooth 2.1 or later, they are required to use the fourth mode.

Cumulatively, the family of Bluetooth BR/EDR/HS specifications defines four security modes. Each Bluetooth device must operate in one of these modes, called Security Modes 1 through 4. These modes dictate when a Bluetooth device initiates security, not whether it supports security features.

Table 3-1. BR/EDR/HS Security Modes

Mode	Security procedures occur during the setup of a
4	Service
3	Link
2	Service
1	Never

Security Mode 1 devices are considered non-secure. Security functionality (authentication and encryption) is never initiated, leaving the device and connections susceptible to attackers. In effect, Bluetooth devices in this mode are “indiscriminate” and do not employ any mechanisms to prevent other Bluetooth-enabled devices from establishing connections. However, if a remote device initiates security—such as a pairing, authentication, or encryption request—a Security Mode 1 device will participate. Per their respective Bluetooth specification versions, all 2.0 and earlier devices can support Security Mode 1, and 2.1 and later devices can use Security Mode 1 for backward compatibility with older devices. However, NIST recommends never using Security Mode 1.

In Security Mode 2, a service level-enforced security mode, security procedures may be initiated after link establishment but before logical channel establishment. For this security mode, 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. In this mode, the notion of authorization—the process of deciding whether a specific device is allowed to have access to a specific service—is introduced. Typically, Bluetooth service discovery can be performed prior to any security challenges (i.e., authentication, encryption, and/or authorization). However, all other Bluetooth services should require all of those security mechanisms.

It is important to note that the authentication and encryption mechanisms used for Security Mode 2 are implemented in the controller, as with Security Mode 3 described below. All 2.0 and earlier devices can support Security Mode 2, but 2.1 and later devices can only support it for backward compatibility with 2.0 or earlier devices.

Security Mode 3 is the link level-enforced security mode, in which a Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandate authentication and encryption for all connections to and from the device. Therefore, even 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"—that is, an authenticated remote device using a Bluetooth service without the local device owner's knowledge.

All 2.0 and earlier devices can support Security Mode 3, but 2.1 and later devices can only support it for backward compatibility purposes.

Similar to Security Mode 2, Security Mode 4 (introduced in Bluetooth 2.1 + EDR) is a service-level-enforced security mode in which security procedures are initiated after physical and logical link setup. Security Mode 4 uses Secure Simple Pairing (SSP), in which ECDH key agreement is utilized for link key generation (see Section 3.1.1). Until Bluetooth 4.0, the P-192 Elliptic Curve was used for the link key generation, and the device authentication and encryption algorithms were identical to the algorithms in Bluetooth 2.0 + EDR and earlier versions. Bluetooth 4.1 introduced the Secure Connections feature, which allowed the use of the P-256 Elliptic Curve for link key generation. In Bluetooth 4.1 the device authentication algorithm was upgraded to the FIPS-approved Hash Message Authentication Code Secure Hash Algorithm 256-bit (HMAC-SHA-256). The encryption algorithm was upgraded to the FIPS-approved AES-Counter with CBC-MAC (AES-CCM), which also provides message integrity. Security requirements for services protected by Security Mode 4 must be classified as one of the following:

- Level 4: Authenticated link key using Secure Connections required
- Level 3: Authenticated link key required
- Level 2: Unauthenticated link key required
- Level 1: No security required
- Level 0: No security required. (Only allowed for SDP)

Whether or not a link key is authenticated depends on the SSP association model used (see Section 3.1.1.2). When both the local and remote device support the Secure Connections feature, the link key

is said to be generated using Secure Connections, which is the NIST recommended security. Security Mode 4 requires encryption for all services (except Service Discovery) and is mandatory for communication between 2.1 and later BR/EDR devices. However, for backward compatibility, a Security Mode 4 device can fall back to any of the other three security modes when communicating with Bluetooth 2.0 and earlier devices that do not support Security Mode 4. In this case, NIST recommends using Security Mode 3.

Table 3-2. BR/EDR/HS Security Mode 4 Levels Summary

Mode 4 Level	FIPS approved algorithms	Provides MITM protection	User interaction during pairing	Encryption required
4	Yes	Yes	Acceptable	Yes
3	No	Yes	Acceptable	Yes
2	No	No	Minimal	Yes
1	No	No	Minimal	Yes
0	No	No	None	No

A device can be in Secure Connections Only Mode when all services (except Service Discovery) require an Authenticated link key using Secure Connections. In this mode, the device will refuse service level connections from devices that do not support the Secure Connections feature. As a result, backwards compatibility with older devices will not be maintained. If a device must operate using only FIPS-approved algorithms, except for Service Discovery, then it should enter Secure Connections Only Mode.

Table 3-3 summarizes the most secure Mode which can be achieved, depending on the Bluetooth version of the two peers, assuming that the 4.1 and later devices support the BR/EDR Secure Connections Feature.

Table 3-3. Most Secure Mode for a Pair of Bluetooth Devices

<table>
<tr><th rowspan="2">Local Bluetooth Version</th><th colspan="2">Most secure Mode connecting to a peer which is</th></tr>
<tr><th>2.0 or lower</th><th>2.1 or higher</th></tr>
<tr><td>4.2</td><td rowspan="9">Mode 3</td><td rowspan="5">Mode 4 (Mandatory)</td></tr>
<tr><td>4.1</td></tr>
<tr><td>4.0</td></tr>
<tr><td>3.0</td></tr>
<tr><td>2.1</td></tr>
<tr><td>2.0</td><td rowspan="4">Mode 3</td></tr>
<tr><td>1.2</td></tr>
<tr><td>1.1</td></tr>
<tr><td>1.0</td></tr>
</table>

Table 3-4 summarizes the most secure Level which can be achieved in Mode 4, depending on the Bluetooth version of the two peers.

Table 3-4. Most Secure Level in Mode 4 for a Pair of Bluetooth Devices

Local Bluetooth Version	Most secure Mode 4 Level connecting to a peer which is	
	2.1 – 4.0	4.1 or higher
4.2	Level 3	Level 4
4.1		
4.0		Level 3
3.0		
2.1		
2.0	N/A	N/A
1.2		
1.1		
1.0		

The remainder of this section discusses specific Bluetooth security components in more detail—pairing and link key generation, authentication, confidentiality, and other Bluetooth security features

3.1.1 Pairing and Link Key Generation

Essential to the authentication and encryption mechanisms provided by Bluetooth is the generation of a secret symmetric key. In Bluetooth BR/EDR this key is called the Link Key and in Bluetooth low energy this key is called the Long Term Key. In legacy low energy pairing, a Short Term Key is generated, which is used to distribute the Slave and/or Master Long Term Key, while in low energy Secure Connections, the Long Term Key is generated by each device and not distributed. As mentioned in Section 3.1, Bluetooth BR/EDR performs pairing (i.e., link key generation) in one of two ways. Security Modes 2 and 3 initiate link key establishment via a method called Personal Identification Number (PIN) Pairing (i.e., Legacy or Classic Pairing), while Security Mode 4 uses SSP. Both methods are described in Sections 3.1.1.1 and 3.1.1.2 below.

In Bluetooth version 4.0 and 4.1, pairing is performed using authenticated or unauthenticated procedures. In Bluetooth 4.2, Secure Connections can be used during pairing to authenticate devices. These methods (also known as security modes and levels) are described in Section 3.2.2 below.

3.1.1.1 PIN/Legacy Pairing

For PIN/legacy pairing, two Bluetooth devices simultaneously derive link keys when the user(s) enter an identical secret PIN into one or both devices, depending on the configuration and device type. The PIN entry and key derivation are depicted conceptually in Figure 3-2. Note that if the PIN is less than 16 bytes, the initiating device's address (BD_ADDR) supplements the PIN value to generate the initialization key. The E_x boxes represent encryption algorithms that are used during the Bluetooth link key derivation processes. More details on the Bluetooth authentication and encryption procedures are outlined in Sections 3.1.2 and 3.1.3, respectively.

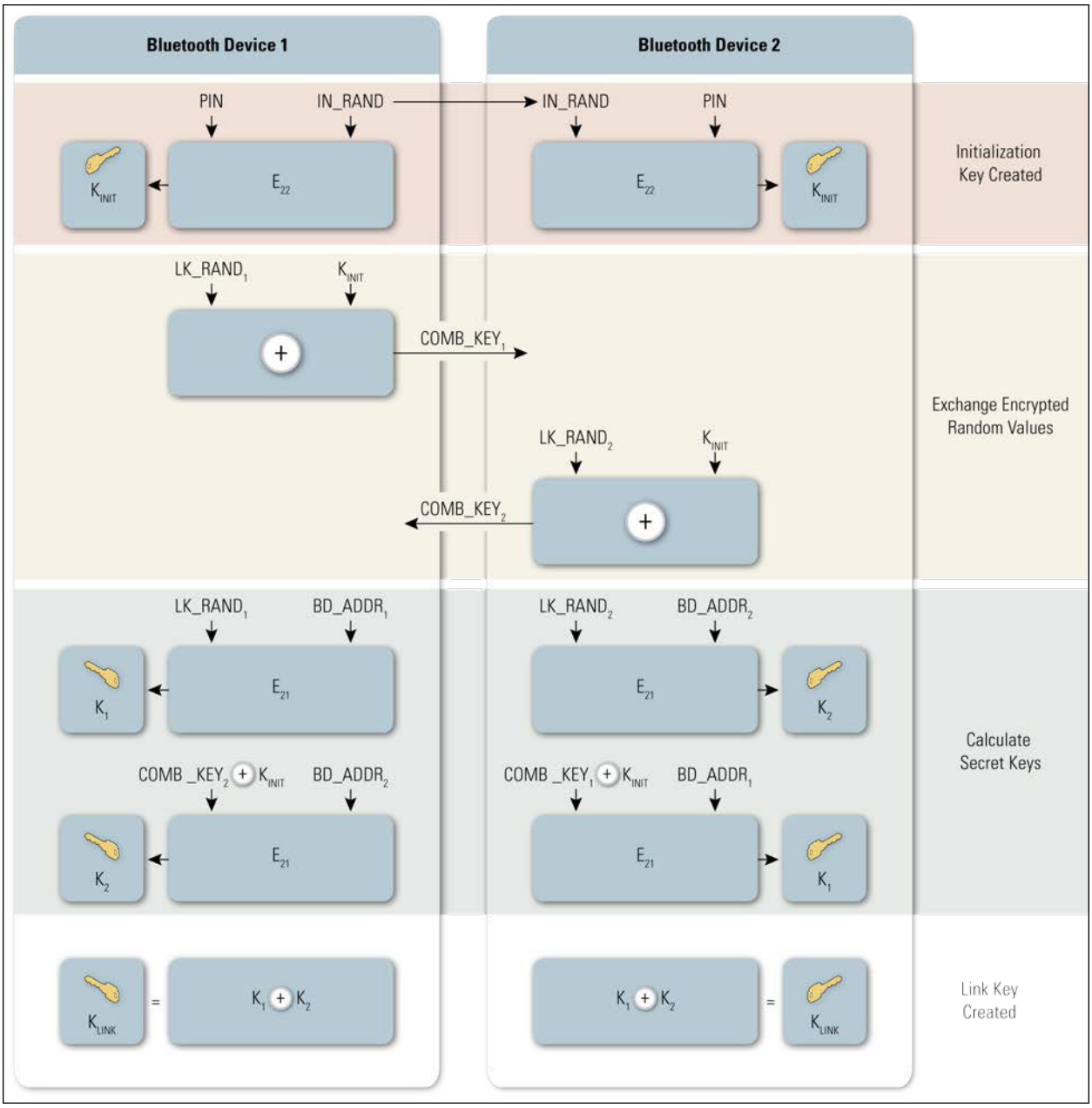

Figure 3-2. Link Key Generation from PIN

After link key generation is complete, the devices complete pairing by mutually authenticating each other to verify they have the same link key. The PIN code used in Bluetooth pairing can vary between 1 and 16 bytes of binary or, more commonly, alphanumeric characters. The typical four-digit PIN may be sufficient for low-risk situations; a longer PIN (e.g., 8-character alphanumeric) should be used for devices that require a higher level of security.[13]

[13] Bluetooth SIG, "Bluetooth Security White Paper," 2002.

3.1.1.2 Secure Simple Pairing

SSP was first introduced in Bluetooth 2.1 + EDR for use with Security Mode 4, and then improved in Bluetooth 4.1. When compared to PIN/Legacy Pairing, SSP simplifies the pairing process by providing a number of association models that are flexible in terms of device input/output capability. SSP also improves security through the addition of ECDH public key cryptography for protection against passive eavesdropping and man-in-the-middle (MITM) attacks during pairing. The Elliptic Curve used during the pairing process can be one of two types: P-192 or P-256[14] (Secure Connections).

The four association models offered in SSP are as follows:[15]

- **Numeric Comparison** was designed for the situation where both Bluetooth devices are capable of displaying a six-digit number and allowing a user to enter a "yes" or "no" response. During pairing, a user is shown a six-digit number on each display and provides a "yes" response on each device if the numbers match. Otherwise, the user responds "no" and pairing fails. A key difference between this operation and the use of PINs in legacy pairing is that the displayed number is not used as input for link key generation. Therefore, an eavesdropper who is able to view (or otherwise capture) the displayed value could not use it to determine the resulting link or encryption key.

- **Passkey Entry** was designed for the situation where one Bluetooth device has input capability (e.g., keyboard), while the other device has a display but no input capability. In this model, the device with only a display shows a six-digit number that the user then enters on the device with input capability. As with the Numeric Comparison model, the six-digit number used in this transaction is not incorporated into link key generation and is of no use to an eavesdropper.

- **Just Works** was designed for the situation where at least one of the pairing devices has neither a display nor a keyboard for entering digits (e.g., headset). It performs Authentication Stage 1 (see Figure 3-3) in the same manner as the Numeric Comparison model, except that a display is not available. The user is required to accept a connection without verifying the calculated value on both devices, so Just Works provides no MITM protection.

- **Out of Band (OOB)** was designed for devices that support a common additional wireless (e.g., Near Field Communication (NFC)) or wired technology for the purposes of device discovery and cryptographic value exchange. In the case of NFC, the OOB model allows devices to pair by simply "tapping" one device against the other, followed by the user accepting the pairing via a single button push. It is important to note that to keep the pairing process as secure as possible, the OOB technology should be designed and configured to mitigate eavesdropping and MITM attacks.

Security Mode 4 requires Bluetooth services to mandate an authenticated link key using Secure Connections (Level 4), an authenticated link key (Level 3), an unauthenticated link key (Level 2), or

[14] For more information about P-256, see FIPS 186-4, *Digital Signature Standards (DSS).*
[15] This information is derived from the Bluetooth 2.1 specification: Bluetooth Special Interest Group, Bluetooth specifications

no security at all (Level 1). Of the association models described above, all but the Just Works model provide authenticated link keys.

Figure 3-3 shows how the link key is established for SSP. Note how this technique uses ECDH public/private key pairs rather than generating a symmetric key via a PIN.

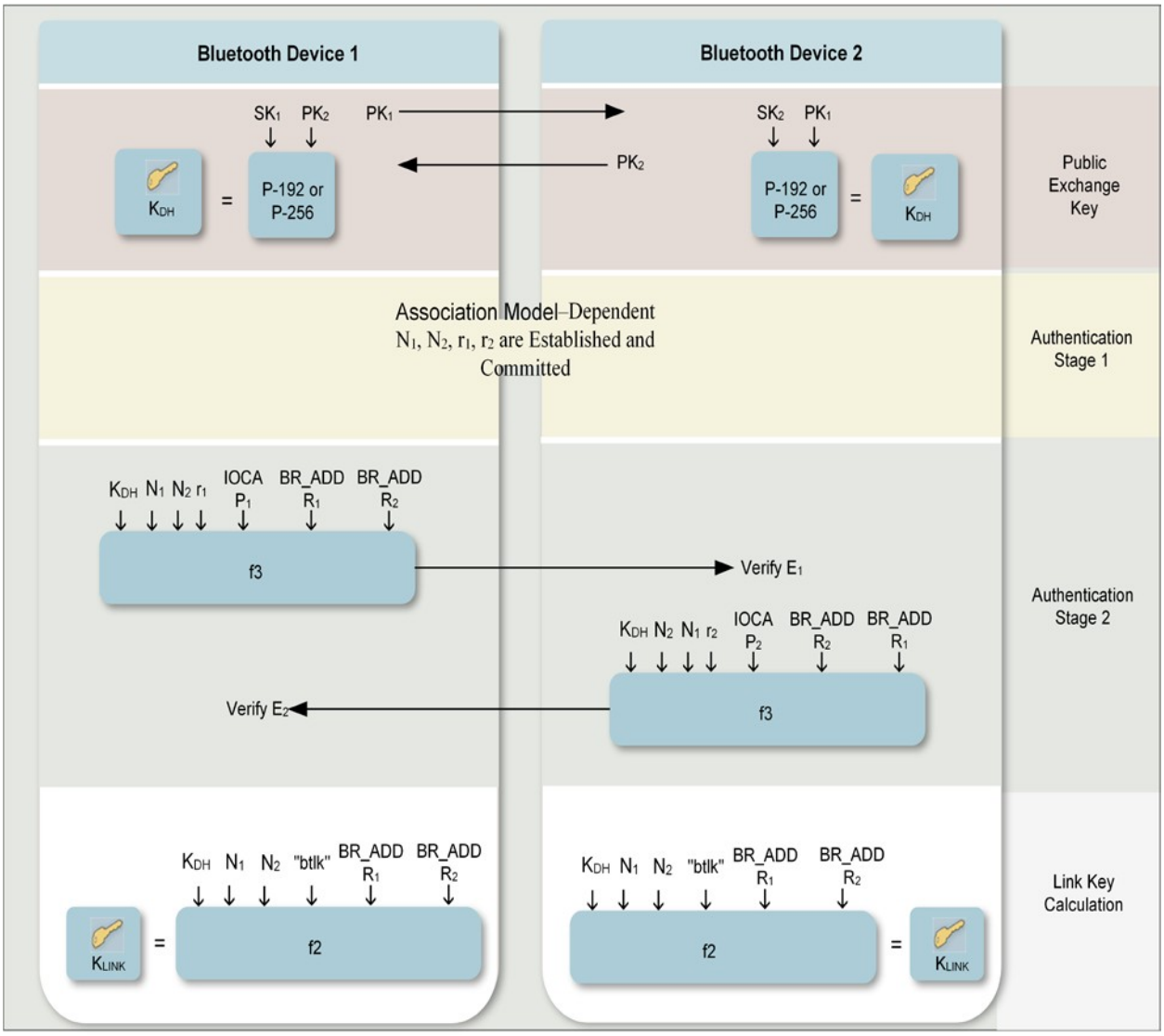

Figure 3-3. Link Key Establishment for Secure Simple Pairing

Each device generates its own ECDH public-private key pair. When both devices support Secure Connections, P-256 elliptic curves are used, else P-192 curves are used. Each device sends the public key to the other device. The devices then perform stage 1 authentication which is dependent on the association model, as described above. After this the first device computes a confirmation value E1 and sends it to the second device which checks the value. If this succeeds, the second device does the same and sends its confirmation value E2 to the first device. Assuming the E2 confirmation value checks out correctly, both devices compute the Link Key.

3.1.1.3 AMP Link Key Derivation from Bluetooth Link Key

For AMP link security (e.g., IEEE 802.11, as introduced in Bluetooth 3.0), an AMP link key is derived from the Bluetooth link key. A Generic AMP Link Key (GAMP_LK) is generated by the AMP Manager in the host stack whenever a Bluetooth link key is created or changed. As shown in Figure 3-4, the GAMP_LK is generated using the Bluetooth link key (concatenated with itself) and an extended ASCII key identifier (keyID) of "gamp" as inputs to an HMAC-SHA-256 function. Subsequently, a Dedicated AMP Link Key (for a specific AMP and Trusted Device combination) is derived from the Generic AMP Link Key and keyID. For the 802.11 AMP Link Key, the keyID is "802b".

For IEEE 802.11 AMPs, the Dedicated AMP Link Key is used as the 802.11 Pairwise Master Key.[16]

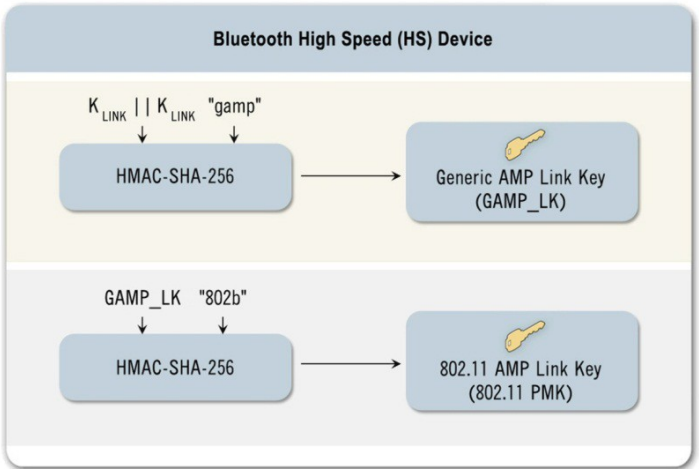

Figure 3-4. AMP Link Key Derivation

3.1.2 Authentication

The Bluetooth device authentication procedure is in the form of a challenge–response scheme. Each device interacting in an authentication procedure can take the role of either the *claimant* or the *verifier* or both. The *claimant* is the device attempting to prove its identity, and the *verifier* is the device validating the identity of the claimant. The challenge–response protocol validates devices by verifying the knowledge of a secret key—the Bluetooth link key.

The authentication procedure is of two types: Legacy Authentication (Section 3.1.2.1) and Secure Authentication (Section 3.1.2.2). Legacy Authentication is performed when at least one device does not support Secure Connections. If both devices support Secure Connections, Secure Authentication is performed.

If authentication fails, a Bluetooth device waits an interval of time before making a new attempt. This time interval increases exponentially to prevent an adversary from attempting to gain access by defeating the authentication scheme through trial-and-error with different link keys. It is important to

[16] NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*.

note that this technique does not provide security against offline attacks to determine the link key using eavesdropped pairing frames and exhaustively guessing PINs.

Note that the security associated with authentication is solely based on the secrecy of the link key. While the Bluetooth device addresses and random challenge value are considered public parameters, the link key is not. The link key is derived during pairing and should never be disclosed outside the Bluetooth device or transmitted over wireless links. However, the link key is passed in the clear from the host to the controller (e.g., PC to USB adapter) and the reverse when the host is used for key storage. The challenge value, which is a public parameter associated with the authentication process, must be random and unique for every transaction. The challenge value is derived from a pseudo-random generator within the Bluetooth controller.

3.1.2.1 Legacy Authentication

This procedure is used when the link key has been generated using PIN/Legacy Pairing or Secure Simple Pairing using the P-192 Elliptic Curve. Each device interacting in an authentication procedure is referred to as either the claimant or the verifier. Figure 3-5 conceptually depicts the Legacy Authentication scheme.

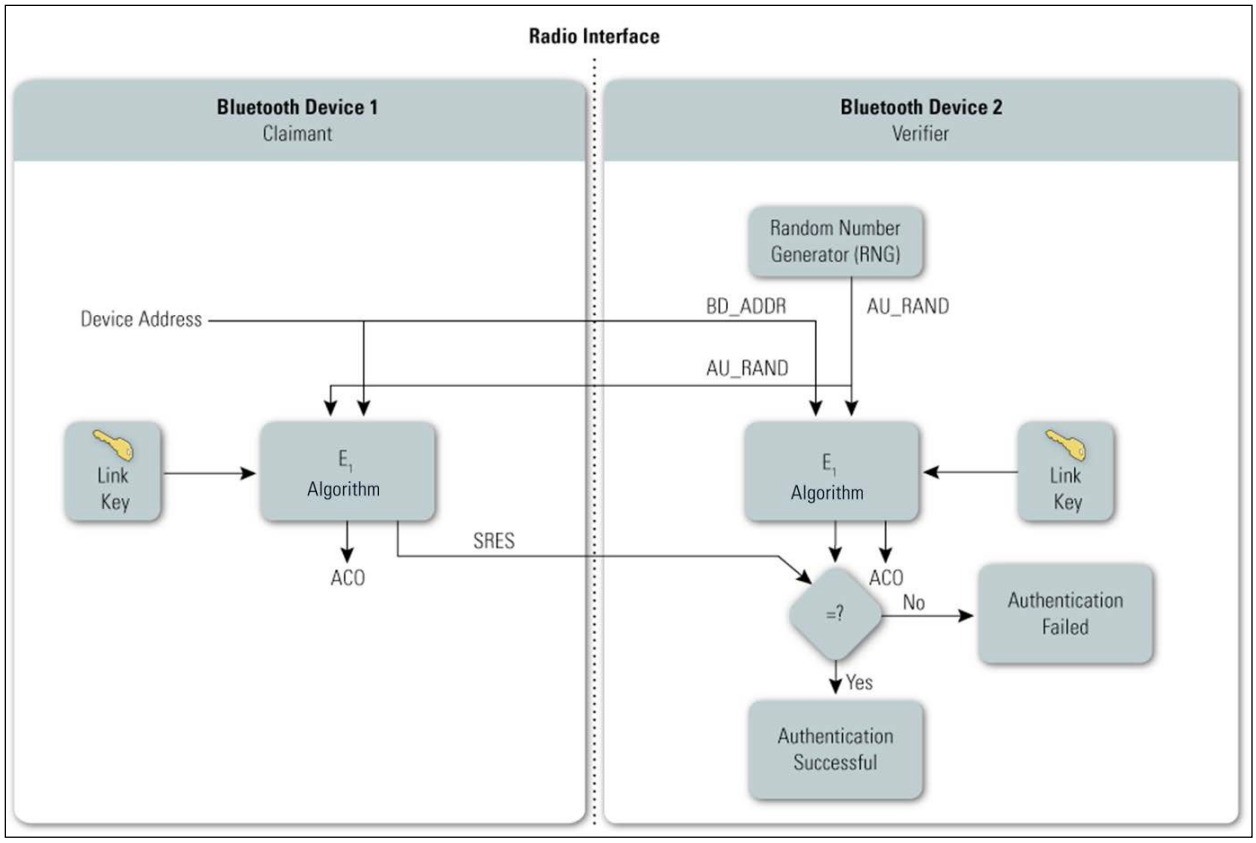

Figure 3-5. Bluetooth Legacy Authentication

The steps in the authentication process are as follows:

- **Step 1.** The verifier transmits a 128-bit random challenge (AU_RAND) to the claimant.

- **Step 2.** The claimant uses the E_1 algorithm[17] to compute an authentication response using his or her unique 48-bit Bluetooth device address (BD_ADDR), the link key, and AU_RAND as inputs. The verifier performs the same computation. Only the 32 most significant bits of the E_1 output are used for authentication purposes. The remaining 96 bits of the 128-bit output are known as the ACO value, which will be used later as input to create the Bluetooth encryption key.
- **Step 3.** The claimant returns the most significant 32 bits of the E_1 output as the computed response, the Signed Response (SRES), to the verifier.
- **Step 4.** The verifier compares the SRES from the claimant with the value that it computed.
- **Step 5.** If the two 32-bit values are equal, the authentication is considered successful. If the two 32-bit values are not equal, the authentication fails.

Performing these steps once accomplishes one-way authentication. The Bluetooth standard allows both one-way and mutual authentication to be performed. For mutual authentication, the above process is repeated with the verifier and claimant switching roles.

3.1.2.2 Secure Authentication

This procedure is used when the link key has been generated using Secure Simple Pairing with the P-256 Elliptic Curve. Each device interacting in an authentication procedure acts as both the claimant and the verifier. Figure 3-6 conceptually depicts the Secure Authentication scheme.

[17] The E_1 authentication function is based on the SAFER+ algorithm. SAFER stands for Secure And Fast Encryption Routine.

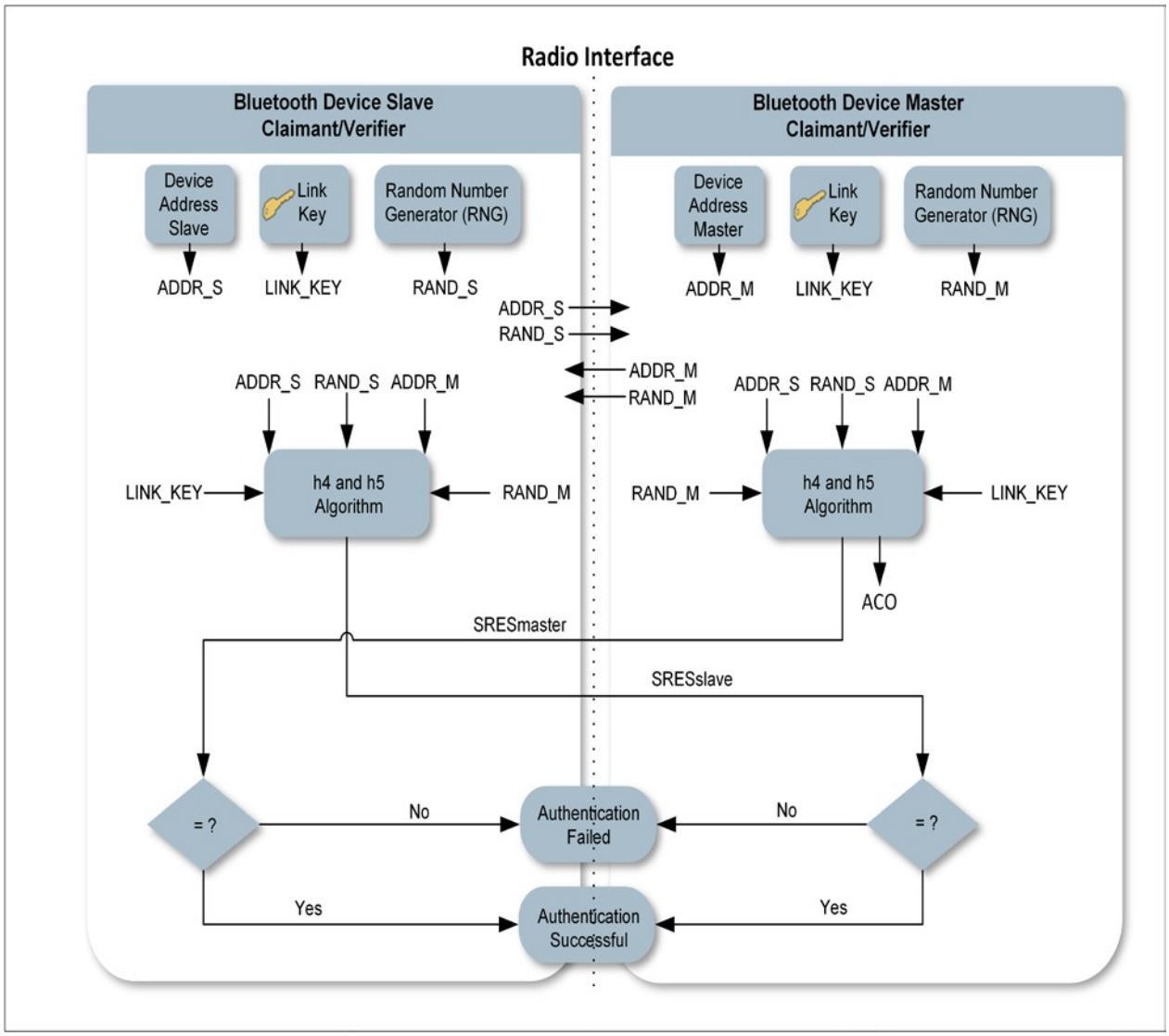

Figure 3-6. Bluetooth Secure Authentication

When the master initiates this authentication process, the steps are as follows:

- **Step 1.** The master transmits a 128-bit random challenge (RAND_M) to the slave.
- **Step 2:** The slave transmits a 128-bit random challenge (RAND_S) to the master.
- **Step 3:** Both the master and slave use the h4 and h5 algorithms[18] to compute their authentication responses using the unique 48-bit Bluetooth device address of the master (ADDR_M), the unique 48-bit Bluetooth device address of the slave (ADDR_S), the link key, the RAND_M, and the RAND_S as inputs. Only the 32 most significant bits of the

[18] The h4 and h5 authentication functions are based on the HMAC-SHA-256 algorithm. HMAC-SHA stands for Hash Message Authentication Code calculated using the Secure Hash Algorithm. The HMAC-SHA-256 is an iterative hash function, which breaks up a message into blocks of a fixed size and iterates over them with the SHA-256 function. The size of the output of HMAC is the same as that of the underlying hash function.

h5 output are used for authentication purposes. The remaining 96 bits of the 128-bit output are known as the Authenticated Ciphering Offset (ACO) value, which will be used later as input to create the Bluetooth encryption key.

- **Step 4.** The slave returns the most significant 32 bits of the h5 output as the computed response, the Signed Response (SRESslave), to the master.
- **Step 5:** The master returns the most significant 32 bits of the h5 output as the computed response, the Signed Response (SRESmaster), to the slave.
- **Step 6:** The master and slave compare the SRES from each other with the value that they computed.
- **Step 7:** If the two 32-bit values are equal on both the master and slave, the authentication is considered successful. If the two 32-bit values are not equal on either the master or the slave, the authentication fails.

When the slave initiates the authentication process, the steps followed are identical to the steps above except that the order of Step 1 and Step 2 is swapped.

Note that Secure Authentication is always mutual in nature irrespective of whether the master or slave initiates it.

3.1.3 Confidentiality

In addition to the Security Modes for pairing and authentication, Bluetooth provides a separate confidentiality service to thwart attempts to eavesdrop on the payloads of the packets exchanged between Bluetooth devices. Bluetooth has three Encryption Modes, but only two of them actually provide confidentiality. The modes are as follows:

- **Encryption Mode 1**—No encryption is performed on any traffic.
- **Encryption Mode 2**—Individually addressed traffic is encrypted using encryption keys based on individual link keys; broadcast traffic is not encrypted.
- **Encryption Mode 3**—All traffic is encrypted using an encryption key based on the master link key.

The encryption mechanism used in Encryption Modes 2 and 3 can be based on either the E0 stream cipher (Section 3.1.3.1) or AES-CCM (Section 3.1.3.2).

The encryption key (K_C) derived using either mechanism may vary in length in single byte increments from 1 byte to 16 bytes in length, as set during a negotiation process that occurs between the master and slave devices. During this negotiation, a master device makes a key size suggestion for the slave. The initial key size suggested by the master is programmed into the controller by the manufacturer and is not always 16 bytes. In product implementations, a “minimum acceptable” key size parameter can be set to prevent a malicious user from driving the key size down to the minimum of 1 byte, which would make the link less secure.

Security Mode 4 introduced in Bluetooth 2.1 + EDR requires that encryption be used for all data traffic, except for service discovery.

3.1.3.1 E0 Encryption Algorithm

As shown in Figure 3-7, the encryption key provided to the encryption algorithm is produced using an internal key generator (KG). The KG produces stream cipher keys based on the 128-bit link key, which is a secret that is held in the Bluetooth devices; a 128-bit random number (EN_RAND); and the 96-bit ACO value. The ACO is produced during the authentication procedure, as shown in Figure 3-5. The COF is the 96-bit Ciphering Offset Number and is a concatenation of the Master and Slave BD_ADDR for Master Link Keys, and is the ACO for other Link Keys.

The Bluetooth E0 encryption procedure is based on a stream cipher, E_0. A key stream output is *exclusive-OR-ed* with the payload bits and sent to the receiving device. This key stream is produced using a cryptographic algorithm based on linear feedback shift registers (LFSRs).[19] The encryption function takes the following as inputs: the master device address (BD_ADDR), the 128-bit random number (EN_RAND), a slot number based on the piconet clock, and an encryption key, which when combined initialize the LFSRs before the transmission of each packet, if encryption is enabled. The slot number used in the stream cipher changes with each packet; the ciphering engine is also reinitialized with each packet while the other variables remain static.

[19] LFSRs are used in coding (error control coding) theory and cryptography. LFSR-based key stream generators (KSG), composed of exclusive-OR gates and shift registers, are common in stream ciphers and are very fast in hardware.

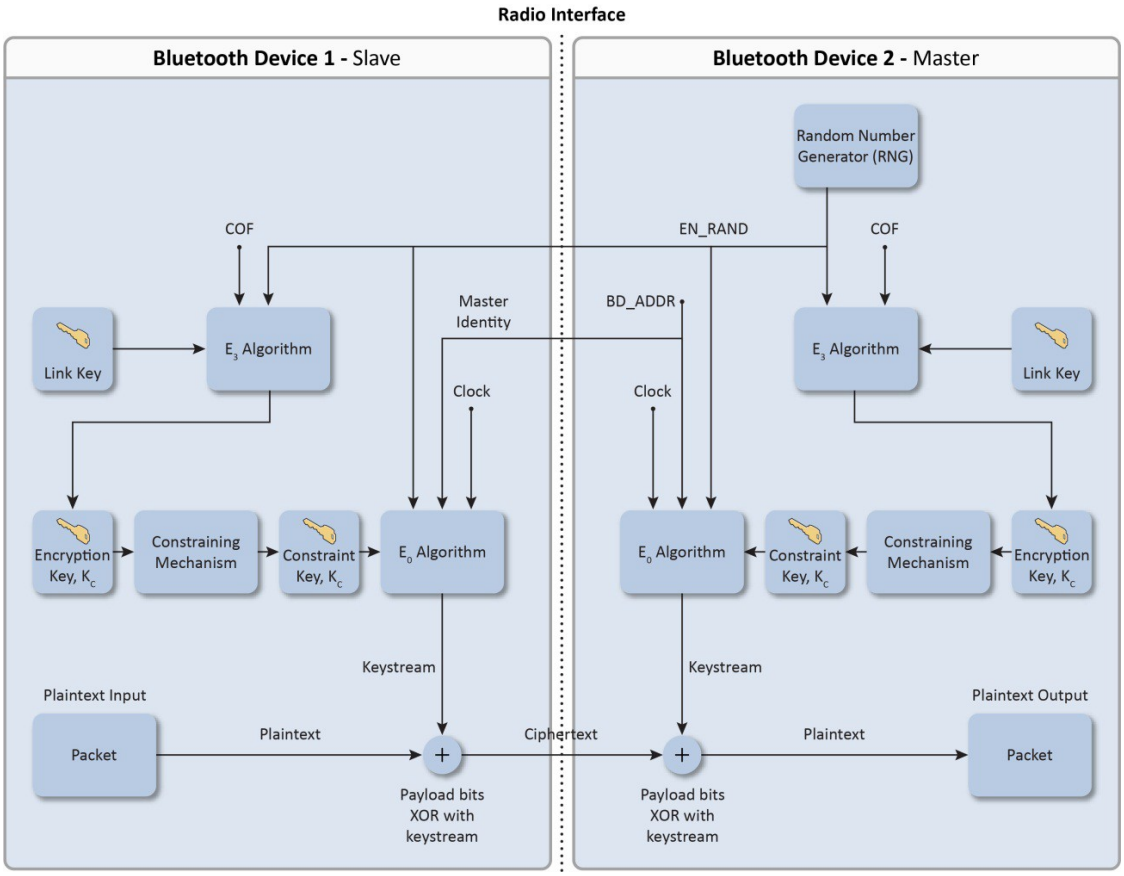

Figure 3-7. Bluetooth E0 Encryption Procedure

It is important to note that E_0 is not a FIPS-approved algorithm and has come under scrutiny in terms of algorithmic strength.[20] A published theoretical known-plaintext attack can recover the encryption key in 2^{38} computations, compared with a brute force attack, which would require testing 2^{128} possible keys. If communications require FIPS-approved cryptographic protection (e.g., to protect sensitive information transmitted by Federal agencies), this protection can be achieved by layering application-level FIPS-approved encryption over the native Bluetooth encryption.

3.1.3.2 AES-CCM Encryption Algorithm

As shown in Figure 3-8, the encryption key provided to the encryption algorithm is produced using the h3 function. The h3 function produces stream cipher keys based on the 128-bit link key, which is a secret that is held in the Bluetooth devices; the unique 48-bit Bluetooth device address of the master; the unique 48-bit Bluetooth device address of the slave; a fixed key ID "btak"; and the 96-bit ACO value. The ACO is produced during the authentication procedure, as shown in Figure 3-6. The encryption key is shortened by taking the 128 most significant bits of the original encryption key.

The Bluetooth AES-CCM encryption procedure is based on Request for Comment (RFC) 3610, *Advanced Encryption Standard - Counter with Cipher Block Chaining-Message Authentication Code*. The AES-CCM encryption function takes the following as inputs: the encryption key, the encryption

[20] Y. Lu, W. Meier, and S. Vaudenay. "The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption."

nonce, and the payload bits. The nonce format is of two types: the payload counter format which is used for Asynchronous Connection-Less (ACL) packets, and the clock format (which also includes an 11-bit day counter) which is used for enhanced Synchronous Connection Oriented (eSCO) packets. When AES-CCM encryption is enabled, ACL packets include a 4-octet Message Integrity Check (MIC). eSCO packets do not include a MIC.

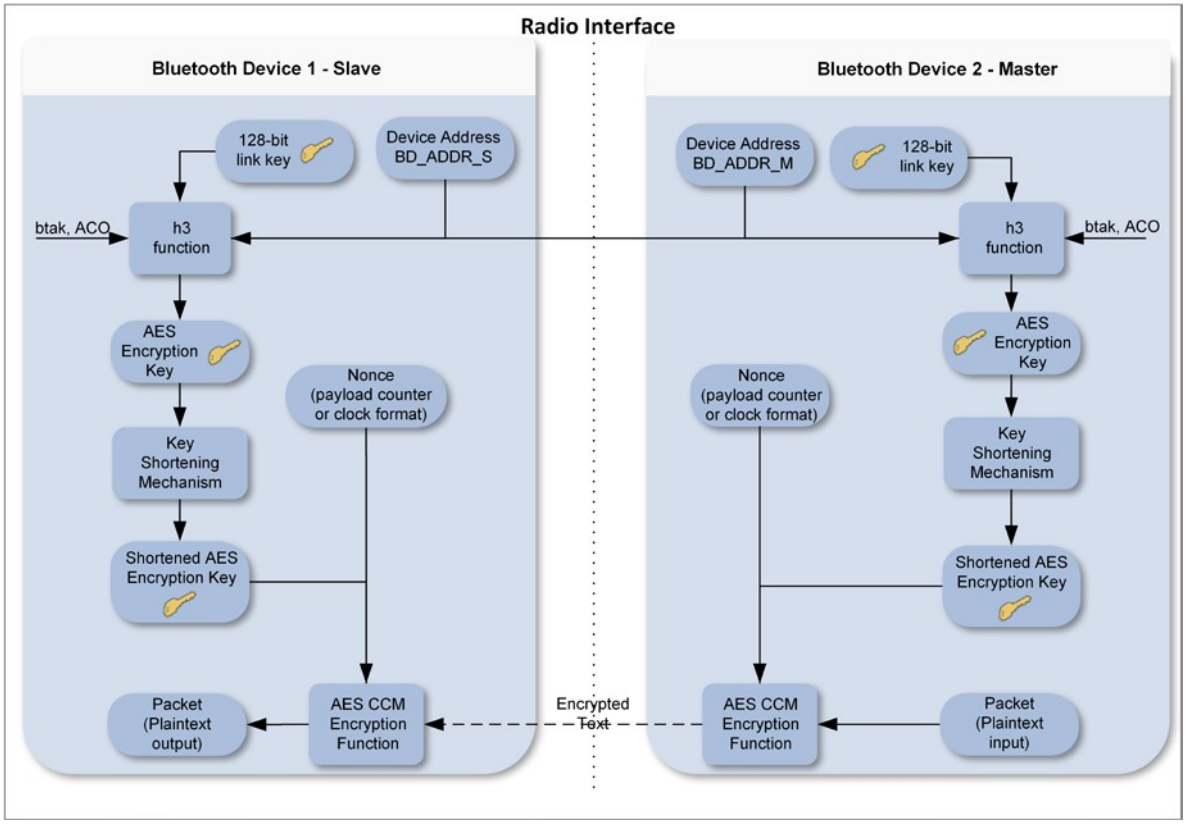

Figure 3-8. Bluetooth AES-CCM Encryption Procedure

3.1.4 Trust Levels, Service Security Levels, and Authorization

In addition to the four security modes, Bluetooth allows 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, which results in the untrusted device receiving 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, the following security requirements can be enforced:

- Authentication required
- Encryption required

- Authorization required

Thus, the available service security levels include any combination of the above, including the lack of security (typically only used for service discovery). Note that BR/EDR encryption cannot be performed without authentication, because the encryption key is derived from an artifact of the authentication process (see Section 3.1.3).

For Security Mode 4, the Bluetooth specification defines five levels of security for Bluetooth services for use during SSP. The service security levels are as follows:

- **Service Level 4 –** Requires MITM protection and encryption using 128-bit equivalent strength for link and encryption keys; user interaction is acceptable.
- **Service Level 3—**Requires MITM protection and encryption; user interaction is acceptable.
- **Service Level 2—**Requires encryption only; MITM protection is not necessary.
- **Service Level 1—**MITM protection and encryption not required. Minimal user interaction.
- **Service Level 0—**No MITM protection, encryption, or user interaction required.

The Bluetooth architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices could gain access only to specific services. Although Bluetooth core protocols can only authenticate devices and not users, user-based authentication is still possible. The Bluetooth security architecture (through the security manager) allows applications to enforce more granular security policies. The link layer at which Bluetooth-specific security controls operate is transparent to the security controls imposed by the application layers. Thus, user-based authentication and fine-grained access control within the Bluetooth security framework are possible through the application layers, although doing so is beyond the scope of the Bluetooth specification.

3.2 Security Features of Bluetooth Low Energy

Because of the intent for Bluetooth low energy to support computationally and storage-constrained devices, and because Bluetooth low energy did not evolve from BR/EDR/HS[21], low energy security is different from Bluetooth BR/EDR/HS. However, with the Bluetooth 4.1 and 4.2 releases, the differences have been minimized.

One remaining difference is that low energy pairing results in the generation of a Long-Term Key (LTK) rather than a Link Key. While fundamentally performing the same secret key function as the Link Key, the LTK is established in a different manner. In low energy Legacy Pairing, the LTK is generated and then distributed using a key transport protocol rather than key agreement as with BR/EDR. That is, one device determines the LTK and securely sends it over to the other device during pairing—instead of both devices generating the same key individually.[22] In low energy Secure

[21] The predecessor to Bluetooth low energy was originally introduced by Nokia in 2006 as Wibree, which was incorporated into the Bluetooth 4.0 specification as Bluetooth low energy in 2010.

[22] Low energy Legacy Pairing potentially can have Master LTK and Slave LTK. So if devices can act in multiple roles, devices might actually have two LTKs. With low energy Secure Connections, there is only one LTK.

Connections the key is generated at each device as a result of a key agreement and thus does not need to be distributed over the link.

Bluetooth specification 4.0 with low energy functionality introduced the use of Advanced Encryption Standard–Counter with CBC-MAC (AES-CCM) encryption for the first time in a Bluetooth specification. In addition to providing strong, standards-based encryption, the inclusion of AES-CCM paved the way for native FIPS-140 validation of Bluetooth low energy devices. 4.2 added the low energy Secure Connections feature which upgraded low energy pairing to utilize FIPS-approved algorithms (AES-CMAC and P-256 elliptic curve). 4.2 also renamed low energy pairing to low energy Legacy Pairing.

Also new in 4.2 is the ability to reuse keys generated via Secure Connections on either physical transport (low energy or BR/EDR) to be used on the other physical transport – alleviating the need for the user to pair on both low energy and BR/EDR. The low energy LTK Key can be derived from the BR/EDR Link Key (using the h6 AES-CMAC-128 function), and the BR/EDR Link Key can likewise be derived from the low energy LTK (using the same h6 function). See Sections 3.2.6 and 3.2.7 for details.

4.0 also introduced features such as low energy private device addresses and data signing. New cryptographic keys called the Identity Resolving Key (IRK) and Connection Signature Resolving Key (CSRK) support these features, respectively. These features remained unchanged in 4.1 and 4.2.

With low energy's privacy feature enabled, the IRK is used to map a Resolvable Private Address (RPA) to an Identity Address. The Identity Address can be either a static random address or a public address. This allows a trusted device to determine another device's Identity Address from a periodically-changing RPA. Previously, a device would be assigned a static "public" address that would be made available during discovery. If that device remained discoverable, its location could easily be tracked by an adversary. The use of a periodically-changing random address (a hashed and randomized address created with the IRK) mitigates this threat. Since a discoverable low energy device transmits ("advertises") identity information, this privacy feature is especially useful. Even without low energy privacy the device will get assigned an Identity Address (either a public BD_ADDR or static random address). But with low energy Privacy the RPA is transmitted over the air instead of the Identity Address.

The CSRK is used to verify cryptographically-signed Attribute Protocol (ATT) data frames from a particular device over unencrypted links. This allows a Bluetooth connection to use data signing (providing integrity and authentication) to protect the connection instead of data encryption (which, in the case of AES-CCM, provides confidentiality, integrity, and authentication). If a link is encrypted, the usage of ATT Signed Write is not allowed.[23]

In low energy Legacy Pairing all of these cryptographic keys (i.e., LTK, IRK, CSRK) are generated and securely distributed during low energy pairing. For low energy Secure Connections the LTK is generated while the IRK and CSRK are generated and securely distributed. See Section 3.2.2 for details.

[23] This feature is not widely used and is optional to support.

3.2.1 Low Energy Security Modes and Levels

Low energy security modes are similar to BR/EDR service-level security modes (i.e., Security Modes 2 and 4) in that each service can have its own security requirements. However, Bluetooth low energy also specifies that each service request can have its own security requirements as well. A device enforces the service-related security requirements by following the appropriate security mode and level.

- Low energy Security Mode 1 has multiple levels associated with encryption. Level 1 specifies no security, meaning no authentication and no encryption will be initiated. Level 2 requires unauthenticated pairing with encryption. Level 3 requires authenticated pairing with encryption. 4.2 added Level 4 which requires authenticated low energy Secure Connections pairing with encryption.
- Low energy Security Mode 2 has multiple levels associated with data signing. Data signing provides strong data integrity but not confidentiality. Level 1 requires unauthenticated pairing with data signing. Level 2 requires authenticated pairing with data signing.

If a particular service request and the associated service have different security modes and/or levels, the stronger security requirements prevail. For example, if either requires Security Mode 1 Level 3, then the requirements for Security Mode 1 Level 3 are enforced.

Because Security Mode 1 Level 4 requires low energy Secure Connections authenticated pairing and encryption using AES-CMAC and P-256 elliptic curve, NIST considers this the most secure of these modes/levels and strongly recommends its use for all low energy connections in 4.2. For 4.0 and 4.1 low energy connections, NIST strongly recommends using Security Mode 1 Level 3 as it requires authenticated pairing and encryption although not as strong (not using P-256 elliptical curve) encryption as Level 4. Security Mode 1 Level 1 is the least secure and should never be used. Also, because Security Mode 2 does not provide encryption, Security Mode 1 Level 4 and 3 are strongly preferred over Security Mode 2.

Low energy 4.2 added a Secure Connections Only Mode which requires that only low energy Security Mode 1 Level 4 may be used for all services except for those that only require Security Mode 1 Level 1. This will ensure that only FIPS-approved algorithms are used on the low energy physical transport. Secure Connections Only Mode is not backwards compatible with 4.0 or 4.1 low energy devices as they do not support P-256 elliptic curve.

3.2.2 Low Energy Pairing Methods

4.2 added the low energy Secure Connection pairing which upgraded low energy pairing to utilize FIPS-approved algorithms (AES-CMAC and P-256 elliptic curve). 4.0 and 4.1 low energy pairing was renamed to low energy Legacy Pairing in 4.2.

Although low energy Legacy Pairing uses similar pairing method names to BR/EDR SSP, it does not use ECDH-based cryptography and provides no eavesdropping protection. Therefore, for all pairing methods except OOB with a 128-bit TK, the low energy Legacy Pairing should be considered broken because if an attacker can capture the pairing frames, he or she can determine the resulting LTK. For

this reason, low energy Secure Connection pairing should be used when eavesdropping protection is required.

Low energy Legacy pairing uses key transport rather than key agreement for all keys (LTK, IRK, and CSRK), thus a key distribution step is required during low energy Legacy pairing. In low energy Secure Connection pairing, each device independently generates the LTK, therefore an optional key distribution step allows for the exchange of the IRK and CSRK keys in low energy Secure Connection pairing.

As shown in Figure 3-9, low energy Legacy Pairing begins with the two devices agreeing on a Temporary Key (TK) during pairing, whose value depends on the pairing method being used. The devices then exchange random values and generate a Short Term Key (STK) based on these values and the TK. The link is then encrypted using the STK, which allows secure distribution of the LTK, IRK, and CSRK.

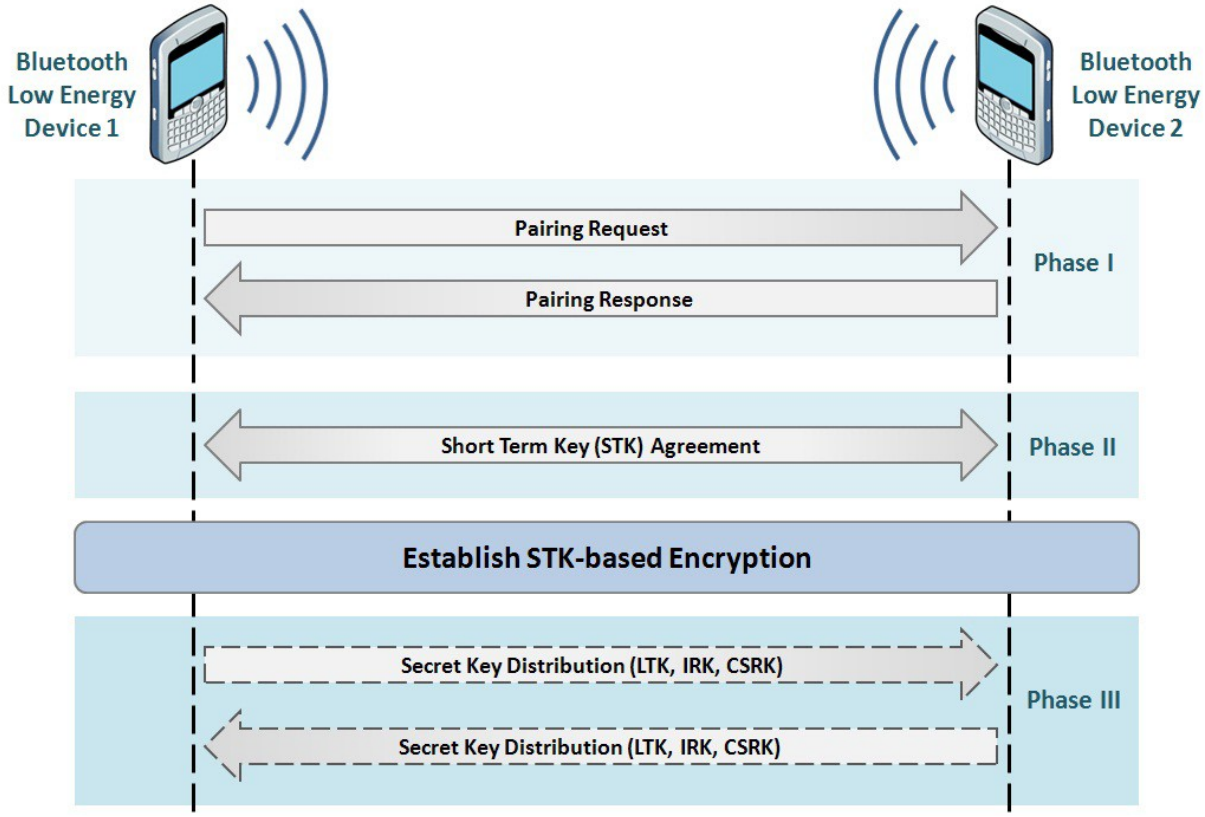

Figure 3-9. Bluetooth Low Energy Legacy Pairing

As shown in Figure 3-10, low energy Secure Connections pairing begins with the two devices sharing their I/O capabilities and security requirements. After that, public keys are shared. Note that low energy Secure Connections pairing only generates the low energy LTK. The Link is encrypted with the LTK which allows secure distribution of the IRK and CSRK.

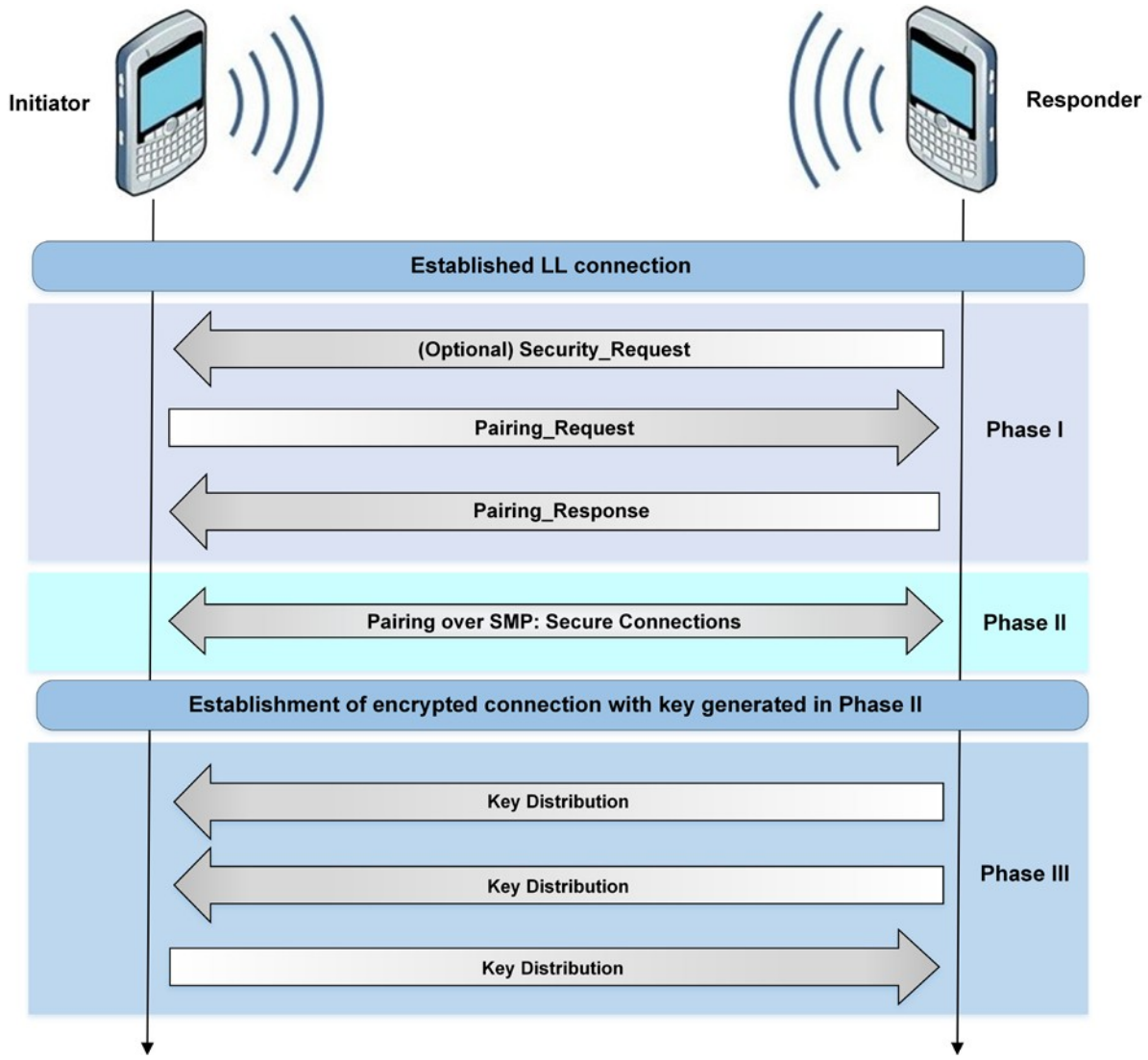

Figure 3-10. Bluetooth Low Energy Secure Connections Pairing

The following subsections describe the low energy pairing association models, both Legacy Pairing and Secure Connections. As with BR/EDR SSP, the association model that is used for a particular connection is based on the input/output capabilities of both devices.

4.0 and 4.1 allow three low energy pairing methods: Out of Band, Passkey Entry, and Just Works. 4.2 adds Numeric Comparison as a low energy pairing method which is available only for low energy Secure Connections. It is important to note that while the low energy pairing association model names are similar to those from BR/EDR Simple Secure Pairing models, for low energy Secure Connection, the security provided is functionally equivalent to that of the BR/EDR SSP models, but for low energy Legacy Pairing the security provided is different.

3.2.2.1 Out of Band

If both devices support a common OOB technology, such as NFC or tethering, they will use the OOB method to pair. In low energy Legacy Pairing, the TK is passed over the OOB technology from one

device to the other. The TK must be a unique, random, 128-bit number. NIST strongly recommends use of a full 128-bit random binary (non-alphanumeric) value when practical.

Because OOB pairing results in an authenticated LTK, it should provide about one-in-a-million protection against MITM attacks—based on the premise that an attacker would have to successfully guess the six-digit TK value if low energy Legacy Pairing is used. However, the actual protection provided by OOB pairing depends on the MITM protection provided by the OOB technology itself because a successful OOB eavesdropper would know the TK value instead of having to guess it. In OOB low energy Secure Connection pairing, the device address is passed OOB[24], which, even if discovered by an OOB eavesdropper, provides no value towards decrypting the encoded data.

If the devices do not support a common OOB technology, the pairing method to be used is determined based on the input/output capabilities of both devices.

3.2.2.2 Numeric Comparison

Low energy 4.2 adapted the BR/EDR/HS numeric comparison pairing method to be used by low energy in Secure Connections pairing. There is no numeric comparison method with low energy Legacy Pairing.

If both devices are capable of displaying a six-digit number and both are capable of having the user enter “yes” or “no”, then numeric comparison can be used.

During pairing, a user is shown a six-digit number on each display and provides a “yes” response on each device if the numbers match. Otherwise, the user responds “no” and pairing fails. An important difference between this operation and the use of PINs in legacy pairing is that the displayed number is not used as input for link key generation. Therefore, an eavesdropper who is able to view (or otherwise capture) the displayed value could not use it to determine the resulting link or encryption key.

Numeric comparison provides MITM protection as well as provides confirmation to the user that they are pairing the intended two devices.

3.2.2.3 Passkey Entry

If, at a minimum, one device supports keyboard input and the other a display output (or keyboard input as well), then the Passkey Entry pairing method is used to pair.

In this model for low energy Legacy Pairing, the TK is generated from the passkey generated and/or entered in each device. The specification requires the passkey size to be 6 numeric digits; therefore, a maximum of 20 bits of entropy can be provided.

For low energy Secure Connections pairing, after the public keys have been exchanged, the passkey (6 numeric digits) is generated and/or entered into each device. The devices then take turns sending a

[24] Optionally, the low energy Secure Connections Confirmation Value and the low energy Secure Connections Random Value are passed OOB as well during low energy Secure Connections OOB pairing.

hash of each bit of the passkey, the nonce, and both public keys (repeated 20 times for each of the 20 bits of the passkey) until the entire passkey has been sent and agreed upon.

Passkey Entry pairing also results in an authenticated LTK. Because a six-digit passkey is used, an attacker would have a one-in-a-million chance of guessing the correct passkey to perform a MITM attack. NIST recommends using a unique, random passkey for each pairing to provide this level of protection across multiple pairings.

3.2.2.4 Just Works

If none of the OOB, Numeric Comparison, or Passkey Entry association models are possible because of device input/output limitations, then the Just Works pairing method is used.

As with SSP in BR/EDR/HS, the Just Works pairing method for low energy is the weakest of the pairing options from a security perspective. In this model for low energy Legacy Pairing, the TK is set to all zeros (0x00). Therefore, an eavesdropper or MITM attacker does not need to guess the TK to generate the STK.

For low energy Secure Connections pairing, after the public keys have been exchanged, the Numeric Comparison procedure is used, but the user is not shown the 6-digit values and the final commitment checks are not performed.

The Just Works pairing method results in an unauthenticated LTK because no MITM protection is provided during pairing.

3.2.3 Legacy Low Energy Key Generation and Distribution

Once the link is encrypted using the STK, the two devices distribute secret keys such as LTK, IRK, and CSRK. Two options are specified for key generation prior to distribution. A device may simply generate random 128-bit values and store them in a local database (called “Database Lookup” in the specification). The other option is to use a single 128-bit static but random value called Encryption Root (ER) along with a 16-bit Diversifier (DIV) unique to each trusted device to generate the keys. This option is called “Key Hierarchy” in the specification. For example, the keys can be derived from ER, DIV, and the Identity Root (IR) using the following formulas:

LTK = d1(ER, DIV, 0)
CSRK = d1(ER, DIV, 1)
IRK = d1(IR, 1, 0)

The d1 function is a called a Diversifying Function and is based on AES-128 encryption. However, the specification allows the use of other key derivation functions.[25]

Using this Key Hierarchy method,[26] the device does not need to store multiple 128-bit keys for each trusted device; rather, it only needs to store its ER and the unique DIVs for each device. During reconnection, the remote device sends its EDIV, which is a masked version of DIV.[27] The local

[25] NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions.*
[26] Using Key Hierarchy is no longer possible with low energy Secure Connections.
[27] DIV = dm(DHK, rand) xor EDIV where DHK is the Diversifier Hiding Key.

device can then regenerate the LTK and/or CSRK from its ER and the passed EDIV. If data encryption or signing is set up successfully, it is verified that the remote device had the correct LTK or CSRK. If unsuccessful, the link is dropped.

Note in the above example that the IRK is static and device-specific, and therefore could be generated prior to pairing (e.g., during manufacturing).

3.2.4 Low Energy Secure Connection Key Generation

Low energy Secure Connections security introduced in Bluetooth 4.2 improves low energy security through the addition of ECDH public key cryptography (using the P-256 Elliptic Curve) for protection against passive eavesdropping and MITM during pairing.

Unlike Legacy low energy Pairing, low energy Secure Connections pairing does not involve generation of an STK. Instead, the LTK is directly generated during the pairing.

Low energy Secure Connections pairing begins with the two devices exchanging their pairing features: I/O capabilities, authentication requirements, and maximum encryption key size requirements. The devices then exchange their public keys.

The LTK is generated using the f5 function (which is an AES-CMAC-128 based function) using the following inputs:

- The shared secret Diffie-Hellman Key (DHkey) generated during pairing phase 2,
- Random number generated and sent by the Master,
- Random number generated and sent by the Slave,
- Bluetooth address of the Master, and
- Bluetooth address of the Slave.

After independent generation in each device, the LTK is stored locally by each device - the LTKs do not need to be distributed in Secure Connections mode. Once the LTK has been generated, the link is encrypted using an encryption key derived from the LTK. Thereafter keys such as the IRK and the CSRK can be distributed by both the devices, similar to the key distribution step of Legacy low energy Pairing (see Figure 3-9).

3.2.5 Confidentiality, Authentication, and Integrity

AES-CCM is used in Bluetooth low energy to provide confidentiality as well as per-packet authentication and integrity. There is no separate authentication challenge/response step as with BR/EDR/HS to verify that they both have the same LTK or CSRK.

Because the LTK is used as input for the encryption key, successful encryption setup provides implicit authentication. Similarly, data signing provides implicit authentication that the remote device holds the correct CSRK—although confidentiality is not provided.

3.2.6 Low Energy Long Term Key Derivation from Bluetooth Link Key

The low energy LTK can be derived from the Bluetooth BR/EDR Link Key. As shown in Figure 3-11, the Intermediate LTK (ILTK) is generated using the Bluetooth link key and an extended ASCII key identifier (keyID) of "tmp2" as inputs to an AES-CMAC function h7. Subsequently, the LTK is derived using ILTK and keyID of "brle" as inputs to h6.[28]

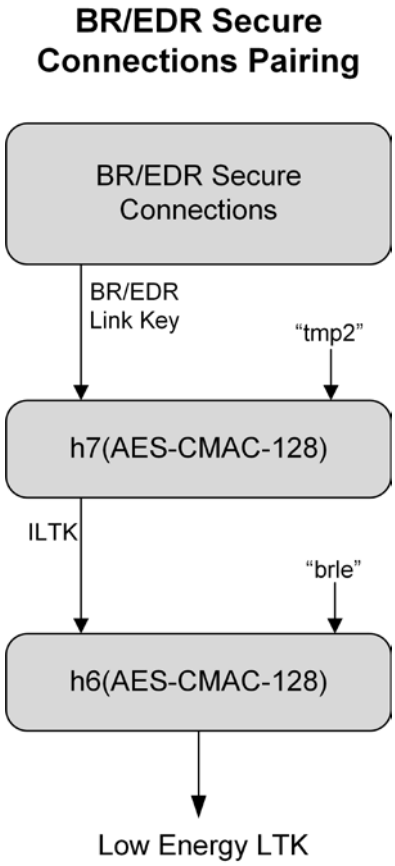

Figure 3-11. Low Energy Long Term Key Derivation from Bluetooth Link Key

3.2.7 Bluetooth Link Key Derivation from Low Energy Long Term Key

The Bluetooth BR/EDR Link Key can also be derived from the low energy Long Term Key. As shown in Figure 3-12, the Intermediate Link Key (ILK) is generated using the low energy LTK and an extended ASCII key identifier (keyID) of "tmp1" as inputs to an AES-CMAC function h7. Subsequently, the Bluetooth Link Key is derived using ILK and keyID of "lebr" as inputs to h6.[29]

[28] Function h7 replaces h6, by reversing the parameter order of h6, as an errata to 4.2.
[29] Function h7 replaces h6, by reversing the parameter order of h6, as an errata to 4.2.

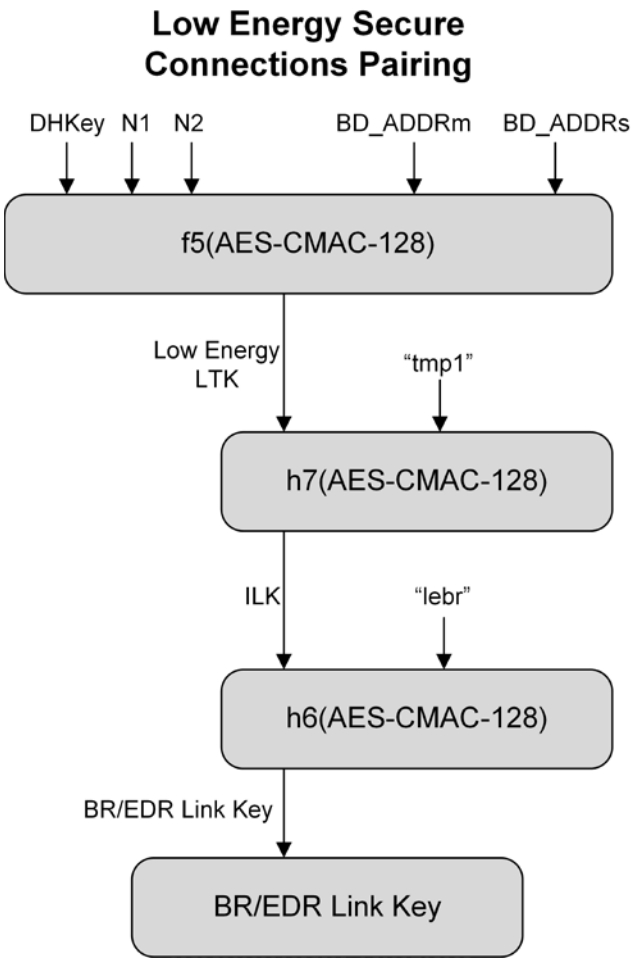

Figure 3-12. Bluetooth Link Key Derivation from Low Energy Long Term Key

4 Bluetooth Vulnerabilities, Threats, and Countermeasures

This section describes vulnerabilities in Bluetooth and threats against those vulnerabilities. Based on these identified common vulnerabilities and threats, as well as the Bluetooth security features described in Section 3, this section also recommends possible countermeasures that can be used to improve Bluetooth security.

Organizations that are planning to use products that use the 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 this writing, one significant security vulnerability related to 4.0 has been discovered (see Table 4-1 below). 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.

4.1 Bluetooth Vulnerabilities

Table 4-1 provides an overview of a number of known security vulnerabilities associated with Bluetooth. The Bluetooth security checklist in Section 4.4 addresses these vulnerabilities.

NOTE: As mentioned previously, depending on the Bluetooth hardware of a device, it may be able to perform both BR/EDR/HS and low energy functionalities (dual-mode) or only low energy functionalities.

Table 4-1. Key Problems with Native Bluetooth Security

	Security Issue or Vulnerability	Remarks	Connections Using Version(s)…
1	**Link keys based on unit keys are static and reused for every pairing.**	A device that uses unit keys will use the same link key for every device with which it pairs. This is a serious cryptographic key management vulnerability.	1.0 1.1
2	**Use of link keys based on unit keys can lead to eavesdropping and spoofing.**	Once a device's unit key is divulged (i.e., upon its first pairing), any other device that has the key can spoof that device or any other device with which it has paired. Further, it can eavesdrop on that device's connections whether they are encrypted or not.	1.0 1.1 1.2
3	**Security Mode 1 devices never initiate security mechanisms.**	Devices that use Security Mode 1 are inherently insecure. For 2.0 and earlier devices, Security Mode 3 (link level security) is highly recommended.	1.0 1.1 1.2 2.0
4	**PINs can be too short.**	Weak PINs, which are used to protect the generation of link keys during pairing, can be easily guessed. People have a tendency to select short PINs.	1.0 1.1 1.2 2.0

	Security Issue or Vulnerability	Remarks	Connections Using Version(s)…
5	**PIN management and randomness is lacking.**	Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems. The best alternative is for one of the devices being paired to generate the PIN using its random number generator.	1.0 1.1 1.2 2.0
6	**The encryption keystream repeats after 23.3 hours of use.**	As shown in Figure 3-7, the encryption keystream is dependent on the link key, EN_RAND, Master BD_ADDR, and Clock. Only the Master's clock will change during a particular encrypted connection. If a connection lasts more than 23.3 hours, the clock value will begin to repeat, hence generating an identical keystream to that used earlier in the connection. Repeating a keystream is a serious cryptographic vulnerability that would allow an attacker to determine the original plaintext.	1.0 1.1 1.2 2.0
7	**Just Works association model does not provide MITM protection during pairing, which results in an unauthenticated link key.**	For highest security, BR/EDR devices should require MITM protection during SSP and refuse to accept unauthenticated link keys generated using Just Works pairing.	2.1 3.0 4.0 4.1 4.2
8	**SSP ECDH key pairs may be static or otherwise weakly generated.**	Weak ECDH key pairs minimize SSP eavesdropping protection, which may allow attackers to determine secret link keys. All devices should have unique, strongly-generated ECDH key pairs that change regularly.	2.1 3.0 4.0 4.1 4.2
9	**Static SSP passkeys facilitate MITM attacks.**	Passkeys provide MITM protection during SSP. Devices should use random, unique passkeys for each pairing attempt.	2.1 3.0 4.0 4.1 4.2
10	**Security Mode 4 devices (i.e., 2.1 or later) are allowed to fall back to any other security mode when connecting with devices that do not support Security Mode 4 (i.e., 2.0 and earlier).**	The worst-case scenario would be a device falling back to Security Mode 1, which provides no security. NIST strongly recommends that a Security Mode 4 device fall back to Security Mode 3 in this scenario.	2.1 3.0 4.0 4.1 4.2
11	**Attempts for authentication are repeatable.**	A mechanism needs to be included in Bluetooth devices to prevent unlimited authentication requests. The Bluetooth specification requires an exponentially increasing waiting interval between successive authentication attempts. However, it does not require such a waiting interval for authentication challenge requests, so an attacker could collect large numbers of challenge responses (which are encrypted with the secret link key) that could leak information about the secret link key.	All
12	**The master key used for broadcast encryption is shared among all piconet devices.**	Secret keys shared amongst more than two parties facilitate impersonation attacks.	1.0 1.1 1.2 2.0 2.1 3.0

	Security Issue or Vulnerability	Remarks	Connections Using Version(s)…
13	**The E0 stream cipher algorithm used for Bluetooth BR/EDR encryption is relatively weak.**	FIPS-approved encryption can be achieved by layering application-level FIPS-approved encryption over the Bluetooth BR/EDR encryption. Note that Bluetooth low energy uses AES-CCM.	1.0 1.1 1.2 2.0 2.1 3.0 4.0
14	**BR/EDR privacy may be compromised if the Bluetooth device address (BD_ADDR) is captured and associated with a particular user.**	Once the BD_ADDR is associated with a particular user, that user's activities and location could be tracked. For low energy, address privacy can be implemented to reduce this risk.	1.0 1.1 1.2 2.0 2.1 3.0
15	**Low energy privacy may be compromised if the Bluetooth address is captured and associated with a particular user.**	For low energy, address privacy can be implemented to reduce this risk.	4.0 4.1 4.2
16	**Device authentication is simple shared-key challenge/response.**	One-way-only challenge/response authentication is subject to MITM attacks. Bluetooth provides for mutual authentication, which should be used to provide verification that devices are legitimate.	1.0 1.1 1.2 2.0 2.1 3.0
17	**Low energy legacy pairing provides no passive eavesdropping protection.**	If successful, eavesdroppers can capture secret keys (i.e., LTK, CSRK, IRK) distributed during low energy pairing.[30]	4.0 4.1
18	**Low energy Security Mode 1 Level 1 does not require any security mechanisms (i.e., no authentication or encryption).**	Similar to BR/EDR Security Mode 1, this is inherently insecure. Low energy Security Mode 1 Level 4 (authenticated pairing and encryption) is highly recommended instead.	4.0 4.1 4.2
19	**Link keys can be stored improperly.**	Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls.	All
20	**Strengths of the pseudo-random number generators (PRNG) are not known.**	The Random Number Generator (RNG) may produce static or periodic numbers that may reduce the effectiveness of the security mechanisms. Bluetooth implementations should use strong PRNGs based on NIST standards. See NIST SP 800-90A, SP 800-90B, SP 800-90C.	All
21	**Encryption key length is negotiable.**	The 3.0 and earlier specifications allow devices to negotiate encryption keys as small as one byte. Bluetooth low energy requires a minimum key size of seven bytes. NIST strongly recommends using Secure Connections Only Mode which requires the full 128-bit key strength (AES-CCM) for both BR/EDR and low energy.	1.0 1.1 1.2 2.0 2.1 3.0

[30] Just capturing the Pairing procedure lets you crack the STK and decrypt the "securely" transmitted LTK, CSRK, and IRK for low energy. For more information see Crackle, Project Ubertooth and the work from Mike Ryan referenced in Appendix D.

	Security Issue or Vulnerability	Remarks	Connections Using Version(s)…
22	**No user authentication exists.**	Only device authentication is provided by the specification. Application-level security, including user authentication, can be added via overlay by the application developer.	All
23	**End-to-end security is not performed.**	Only individual links are encrypted and authenticated. Data is decrypted at intermediate points. End-to-end security on top of the Bluetooth stack can be provided by use of additional security controls.	All
24	**Security services are limited.**	Audit, non-repudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.	All
25	**Discoverable and/or connectable devices are prone to attack.**	Any BR/EDR/HS device that must go into discoverable or connectable mode to pair or connect should only do so for a minimal amount of time. A device should not be in discoverable or connectable mode all the time.	All
26	**The Just Works pairing method provides no MITM protection.**	MITM attackers can capture and manipulate data transmitted between trusted devices. Low energy devices should be paired in a secure environment to minimize the risk of eavesdropping and MITM attacks. Just Works pairing should not be used for low energy.	4.0 4.1 4.2
27	**With two already paired BR/EDR/HS devices, mutual authentication may not always happen with Security Mode 3 and 4**	With two devices already paired, if device A is the authentication initiator to B, encryption setup will begin after that initial authentication. If the encryption setup being successful is good enough to satisfy B, then B may never bother to attempt to authenticate A.	1.0 1.1 1.2 2.0 2.1 3.0

4.2 Bluetooth Threats

Bluetooth offers several benefits and advantages, but the benefits are not provided without risk. Bluetooth and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, MITM attacks, message modification, and resource misappropriation,[31] and are also threatened by more specific Bluetooth related attacks, such as the following:

- **Bluesnarfing.** Bluesnarfing[32] enables attackers to gain access to a Bluetooth-enabled device by exploiting a firmware flaw in older (circa 2003) devices. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device including the device's international mobile equipment identity (IMEI). The IMEI is a unique identifier for each device that an attacker could potentially use to route all incoming calls from the user's device to the attacker's device.

[31] Additional information on general wireless security threats is available in Section 3 of NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks* (https://doi.org/10.6028/NIST.SP.800-48r1).

[32] https://trifinite.org/trifinite_stuff_bluesnarf.html

- **Bluejacking.** Bluejacking is an attack conducted on Bluetooth-enabled mobile devices, such as cell phones. An attacker initiates bluejacking by sending unsolicited messages to the user of a Bluetooth-enabled device. The actual messages do not cause harm to the user's device, but they may entice the user to respond in some fashion or add the new contact to the device's address book. This message-sending attack resembles spam and phishing attacks conducted against email users. Bluejacking can cause harm when a user initiates a response to a bluejacking message sent with a harmful intent.

- **Bluebugging.** Bluebugging[33] exploits a security flaw in the firmware of some older (circa 2004) Bluetooth devices to gain access to the device and its commands. This attack uses the commands of the device without informing the user, allowing the attacker to access data, place phone calls, eavesdrop on phone calls, send messages, and exploit other services or features offered by the device.

- **Car Whisperer.** Car Whisperer[34] is a software tool developed by European security researchers that exploits the use of a standard (non-random) passkey in hands-free Bluetooth car kits installed in automobiles. The Car Whisperer software allows an attacker to send to or receive audio from the car kit. An attacker could transmit audio to the car's speakers or receive audio (eavesdrop) from the microphone in the car.

- **Denial of Service.** Like other wireless technologies, Bluetooth is susceptible to DoS attacks. Impacts include making a device's Bluetooth interface unusable and draining the device's battery. These types of attacks are not significant and, because of the proximity required for Bluetooth use, can usually be easily averted by simply moving out of range.

- **Fuzzing Attacks.** Bluetooth fuzzing attacks consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts. If a device's operation is slowed or stopped by these attacks, a serious vulnerability potentially exists in the protocol stack.

- **Pairing Eavesdropping**. PIN/Legacy Pairing (Bluetooth 2.0 and earlier) and low energy Legacy Pairing are susceptible to eavesdropping attacks. The successful eavesdropper who collects all pairing frames can determine the secret key(s) given sufficient time, which allows trusted device impersonation and active/passive data decryption.

- **Secure Simple Pairing Attacks.** A number of techniques can force a remote device to use Just Works SSP and then exploit its lack of MITM protection (e.g., the attack device claims that it has no input/output capabilities). Further, fixed passkeys could allow an attacker to perform MITM attacks as well.

4.3 Risk Mitigation and Countermeasures

Organizations should mitigate risks to their Bluetooth implementations by applying countermeasures to address specific threats and vulnerabilities. Some of these countermeasures cannot be achieved through security features built into the Bluetooth specifications. The countermeasures recommended in the checklist in Section 4.4 do not guarantee a secure Bluetooth environment and cannot prevent all

[33] https://trifinite.org/trifinite_stuff_bluebug.html
[34] https://trifinite.org/trifinite_stuff_carwhisperer.html

adversary penetrations. In addition, security comes at a cost—expenses related to security equipment, inconvenience, maintenance, and operation. Each organization should evaluate the acceptable level of risk based on numerous factors, which will affect the level of security implemented by that organization. To be effective, Bluetooth security should be incorporated throughout the entire lifecycle of Bluetooth solutions.[35]

FIPS Publication (PUB) 199 establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system. NIST SP 800-53 provides recommendations for minimum security controls for information systems based on the FIPS PUB 199 impact categories.[36] The recommendations in NIST SP 800-53 should be helpful to organizations in identifying the controls needed to protect Bluetooth implementations in general, which should be used in addition to the specific recommendations for Bluetooth implementations listed in this document.

The first line of defense is to provide an adequate level of knowledge and understanding for those who will deal with Bluetooth-enabled devices. Organizations using Bluetooth should establish and document security policies that address the use of Bluetooth-enabled devices and users' responsibilities. Organizations should include awareness-based education to support staff understanding and knowledge of Bluetooth. Policy documents should include a list of approved uses for Bluetooth and the type of information that may be transferred over Bluetooth networks. The security policy should also specify a proper password usage scheme. When feasible, a centralized security policy management approach should be used in coordination with an endpoint security product installed on the Bluetooth devices to ensure that the policy is locally and universally enforced.

The general nature and mobility of Bluetooth-enabled devices increases the difficulty of employing traditional security measures across the enterprise. Nevertheless, a number of countermeasures can be enacted to secure Bluetooth devices and communications, ranging from distance and power output to general operation practices. Several countermeasures that could be employed are provided in the checklist in Section 4.4.

4.4 Bluetooth Security Checklist

Table 4-2 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 column 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. In addition, for each recommendation three checklist columns are provided.

---

[35] For more information about technology lifecycles, see NIST SP 800-64 Revision 2, *Security Considerations in the Information System Development Life Cycle* (https://doi.org/10.6028/NIST.SP.800-64r2).

[36] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, is available at https://doi.org/10.6028/NIST.FIPS.199. NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, is available at https://doi.org/10.6028/NIST.SP.800-53r4.

- The first column, the *Recommended Practice* column, if checked, means that this entry represents a recommendation for all organizations.
- The second column, the *Should Consider* column, if checked, means that the entry's recommendation should be considered carefully by an organization for one or more of the following reasons:
- First, implementing the recommendation may provide a higher level of security for the wireless environment by offering some additional protection.
- Second, the recommendation supports a defense-in-depth strategy.
- Third, it may have significant performance, operational, or cost impacts. In summary, if the *Should Consider* column is checked, organizations should carefully consider the option and weigh the costs versus the benefits.
- The last column, *Status*, is intentionally left blank to allow organization representatives to use this table as a true checklist. For instance, an individual performing a wireless security audit in a Bluetooth environment can quickly check off each recommendation for the organization, asking, "Have I done this?"

Table 4-2. Bluetooth Piconet Security Checklist

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
Management Recommendations					
1	Develop an organizational wireless security policy that addresses Bluetooth wireless technology.	A security policy is the foundation for all other countermeasures.	✓		
2	Ensure that Bluetooth users on the network are made aware of their security-related responsibilities regarding Bluetooth use.	A security awareness program helps users to follow practices that help prevent security incidents.	✓		
3	Perform comprehensive security assessments at regular intervals to fully understand the organization's Bluetooth security posture.	Assessments help identify Bluetooth devices being used within the organization and help ensure the wireless security policy is being followed.	✓		
4	Ensure that wireless devices and networks involving Bluetooth are fully understood from an architecture perspective and documented accordingly.	Bluetooth-enabled devices can contain various networking technologies and interfaces, allowing connections to local and wide area networks. An organization should understand the overall connectivity of each device to identify possible risks and vulnerabilities. These risks and vulnerabilities can then be addressed in the wireless security policy.	✓		

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
5	Provide users with a list of precautionary measures they should take to better protect handheld Bluetooth devices from theft.	The organization and its employees are responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resources.	✓		
6	Maintain a complete inventory of all Bluetooth-enabled wireless devices and addresses (BD_ADDRs).	A complete inventory list of Bluetooth-enabled wireless devices can be referenced when conducting an audit that searches for unauthorized use of wireless technologies.	✓		
Technical Recommendations					
7	Change the default settings of the Bluetooth device to reflect the organization's security policy.	Because default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organizational security policy. For example, the default device name should usually be changed to be non-descriptive (i.e., so that it does not reveal the platform type).	✓		
8	Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the organization.	Setting Bluetooth devices to the lowest necessary and sufficient power level ensures a secure range of access to authorized users. The use of Class 1 devices, as well as external amplifiers or high-gain antennas, should be avoided because of their extended range.	✓		
9	Choose PIN codes that are sufficiently random, long and private. Avoid static and weak PINs, such as all zeroes.	PIN codes should be random so that malicious users cannot easily guess them. Longer PIN codes are more resistant to brute force attacks. For Bluetooth 2.0 (or earlier) devices, an eight-character alphanumeric PIN should be used, if possible. The use of a fixed PIN is not acceptable.	✓		
10	Ensure that link keys are not based on unit keys.	The use of shared unit keys can lead to successful spoofing, MITM, and eavesdropping attacks. The use of unit keys for security was deprecated in Bluetooth v1.2.	✓		

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
11	For 2.1 and later devices using SSP, avoid using the "Just Works" association model. The device must verify that an authenticated link key was generated during pairing.	The "Just Works" association model does not provide MITM protection. Devices that only support Just Works (e.g., devices that have no input/output capability) should not be procured if similarly qualified devices that support one of the other association models (i.e., Numeric Comparison, OOB, or Passkey Entry) are available.	✓		
12	For 2.1 and later devices using SSP, random and unique passkeys must be used for each pairing based on the Passkey Entry association model.	If a static passkey is used for multiple pairings, the MITM protection provided by the Passkey Entry association model is reduced.	✓		
13	A Bluetooth 2.1 or later device using Security Mode 4 must fall back to Security Mode 3 for backward compatibility with 2.0 and earlier devices (i.e., for devices that do not support Security Mode 4).	The Bluetooth specifications allow a 2.1 device to fall back to any security mode for backward compatibility. This allows the option of falling back to Security Modes 1-3. As discussed earlier, Security Mode 3 provides the best security.	✓		
14	4.0 and 4.1 devices and services using low energy technologies should use Security Mode 1 Level 3 whenever possible. Low energy Security Mode 1 Level 3 provides the highest security available for 4.0 and 4.1 low energy devices.	Other low energy security modes allow unauthenticated pairing and/or no encryption.	✓		
15	Bluetooth 4.2 devices and services using low energy functionality should use Security Mode 1 Level 4 whenever possible. Low energy Security Mode 1 Level 4 implements Secure Connections mode and provides the highest security available for 4.2 low energy devices.	If Security Mode 1 Level 4 is not available, recommend using Security Mode 1 Level 3 instead	✓		
16	4.1 BR/EDR devices and services should use Security Mode 4, Level 4 whenever possible, as it provides the highest security available for 4.1 and later BR/EDR devices.	If Security Mode 4 Level 4 is not available, recommend using Security Mode 3.	✓		
17	Unneeded and unapproved service and profiles should be disabled.	Many Bluetooth stacks are designed to support multiple profiles and associated services. The Bluetooth stack on a device should be locked down to ensure only required and approved profiles and services are available for use.	✓		

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
18	Bluetooth devices should be configured by default as undiscoverable and remain undiscoverable except as needed for pairing.	This prevents visibility to other Bluetooth devices except when discovery is absolutely required. In addition, the default Bluetooth device names sent during discovery should be changed to non-identifying values.	✓		
19	Invoke link encryption for all Bluetooth connections.	Link encryption should be used to secure all data transmissions during a Bluetooth connection; otherwise, transmitted data is vulnerable to eavesdropping.	✓		
20	If multi-hop wireless communication is being used, ensure that encryption is enabled on every link in the communication chain.	One unsecured link results in compromising the entire communication chain.	✓		
21	Ensure device mutual authentication is performed for all connections.	Mutual authentication is required to provide verification that all devices on the network are legitimate.	✓		
22	Enable encryption for all broadcast transmissions (Encryption Mode 3).	Broadcast transmissions secured by link encryption provide a layer of security that protects these transmissions from user interception for malicious purposes.	✓		
23	Configure encryption key sizes to the maximum allowable.	Using maximum allowable key sizes provides protection from brute force attacks.	✓		
24	Bluetooth devices must prompt the user to authorize all incoming Bluetooth connection requests before allowing any incoming connection request to proceed.	Users must also never accept connections, files, or other objects from unexpected, unknown, or untrusted sources.	✓		
25	Use application-level authentication and encryption atop the Bluetooth stack for sensitive data communication.	Bluetooth devices can access link keys from memory and automatically connect with previously paired devices. Incorporating application-level software that implements authentication and encryption will add an extra layer of security. Passwords and other authentication mechanisms, such as biometrics and smart cards, can be used to provide user authentication for Bluetooth devices. Employing higher layer encryption (particularly FIPS 140 validated) over the native encryption will further protect the data in transit.		✓	

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
26	Deploy user authentication overlays such as biometrics, smart cards, two-factor authentication, or public key infrastructure (PKI).	Implementing strong authentication mechanisms can minimize the vulnerabilities associated with passwords and PINs.		✓	
27	If using a Mobile Device Management (MDM) solution, ensure the organization's Bluetooth security policy is appropriately enforced through the technical controls of the management solution.	Security policies can be enforced by MDM solutions. The default settings are generally not secure, a careful review of those settings should be performed to ensure that they comply with the organizational security policy.		✓	
Operational Recommendations					
28	Ensure that Bluetooth capabilities are disabled when they are not in use.	Bluetooth capabilities should be disabled on all Bluetooth devices, except when the user explicitly enables Bluetooth to establish a connection. This minimizes exposure to potential malicious activities. For devices that do not support disabling Bluetooth (e.g., headsets), the entire device should be shut off when not in use.	✓		
29	Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry and intercept Bluetooth pairing messages. (Note: A "secure area" is defined as a non-public area that is indoors away from windows in locations with physical access controls.) Users should not respond to any messages requesting a PIN, unless the user has initiated a pairing and is certain the PIN request is being sent by one of the user's devices.	Pairing is a vital security function and requires that users maintain a security awareness of possible eavesdroppers. If an attacker can capture the transmitted frames associated with pairing, determining the link key is straightforward for pre-2.1 and 4.0 devices since security is solely dependent on PIN entropy and length. This recommendation also applies to 2.1/3.0 devices, although similar eavesdropping attacks against SSP have not yet been documented.	✓		
30	A BR/EDR service-level security mode (i.e., Security Mode 2 or 4) should only be used in a controlled and well-understood environment.	Security Mode 3 provides link-level security prior to link establishment, while Security Modes 2 and 4 allow link-level connections before any authentication or encryption is established. NIST highly recommends that devices use Security Mode 3.	✓		
31	Ensure that portable devices with Bluetooth interfaces are configured with a password.	This helps prevent unauthorized access if the device is lost or stolen.	✓		

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
32	In the event a Bluetooth device is lost or stolen, users should immediately delete the missing device from the paired device lists of all other Bluetooth devices.	This policy will prevent an attacker from using the lost or stolen device to access another Bluetooth device owned by the user(s).	✓		
33	Install antivirus software on Bluetooth-enabled hosts that support such host-based security software.	Antivirus software should be installed to ensure that known malware is not introduced to the Bluetooth network.	✓		
34	Fully test and regularly deploy Bluetooth software and firmware patches and upgrades.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should be fully tested before implementation to confirm that they are effective.	✓		
35	Users should not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions include messages, files, and images.	With the increase in the number of Bluetooth-enabled devices, it is important that users only establish connections with other trusted devices and only accept content from these trusted devices.	✓		
36	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements prior to implementation.	✓		
37	Designate an individual to track the progress of Bluetooth security products and standards (perhaps via the Bluetooth SIG) and the threats and vulnerabilities with the technology.	An individual designated to track the latest technology enhancements, standards (perhaps via Bluetooth SIG), and risks will help to ensure the continued secure use of Bluetooth.		✓	

Table 4-3 lists the security controls from NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*,[37] that map to the recommendations in Table 4-2. The left column gives the number and name of the control from NIST SP 800-53, and the right column provides the Table 4-2 recommendation numbers that correspond to the NIST SP 800-53 control.

The list of controls in Table 4-3 is not intended to be fully comprehensive or authoritative. Rather, it lists those controls that are most directly supported by the Table 4-2 recommendations.

[37] https://doi.org/10.6028/NIST.SP.800-53r4

Table 4-3. Recommendation Mappings to NIST SP 800-53 Security Controls

NIST SP 800-53 Control Number and Name	Recommendation Numbers from Table 4-2
AT-2, Security Awareness Training	2, 5
CA-2, Security Assessments	3
CM-6, Configuration Settings	7
CM-7, Least Functionality	17, 18, 27
CM-8, Information System Component Inventory	6
IA-2, Identification and Authentication (Organizational Users)	25, 26
IA-3, Device Identification and Authentication	9, 11, 12, 13, 14, 16, 21, 28, 29, 30, 31
IR-4, Incident Handling	31
RA-3, Risk Assessment	4, 35
SC-1, System and Communications Protection Policy and Procedures	1
SC-12, Cryptographic Key Establishment and Management	10, 15, 16, 23, 25
SC-40, Wireless Link Protection	8, 28
SC-8, Transmission Confidentiality and Integrity	13, 14, 16, 19, 20, 22, 29
SI-2, Flaw Remediation	33
SI-3, Malicious Code Protection	32
SI-5, Security Alerts, Advisories, and Directives	36

Appendix A—Glossary

Selected terms used in the publication are defined below.

Access Point (AP)	A device that logically connects wireless client devices operating in infrastructure to one another and provides access to a distribution system, if connected, which is typically an organization's enterprise wired network.
Ad Hoc Network	A wireless network that allows easy connection establishment between wireless client devices in the same physical area without the use of an infrastructure device, such as an access point or a base station.
Claimant	The Bluetooth device attempting to prove its identity to the verifier during the Bluetooth connection process.
Media Access Control (MAC)	A unique 48-bit value that is assigned to a particular wireless network interface by the manufacturer.
Piconet	A small Bluetooth network created on an ad hoc basis that includes two or more devices.
Range	The maximum possible distance for communicating with a wireless network infrastructure or wireless client.
Scatternet	A chain of piconets created by allowing one or more Bluetooth devices to each be a slave in one piconet and act as the master for another piconet simultaneously. A scatternet allows several devices to be networked over an extended distance.
Verifier	The Bluetooth device that validates the identity of the claimant during the Bluetooth connection process.
Wireless Local Area Network (WLAN)	A group of wireless access points and associated infrastructure within a limited geographic area, such as an office building or building campus, that is capable of radio communications. WLANs are usually implemented as extensions of existing wired LANs to provide enhanced user mobility.
Wireless Personal Area Network (WPAN)	A small-scale wireless network that requires little or no infrastructure and operates within a short range. A WPAN is typically used by a few devices in a single room instead of connecting the devices with cables.

Appendix B—Acronyms and Abbreviations

Selected acronyms and abbreviations used in the publication are defined below.

8DPSK	8 Phase Differential Phase Shift Keying
ACL	Asynchronous Connection-Less
ACO	Authenticated Ciphering Offset
AES	Advanced Encryption Standard
AES-CCM	Advanced Encryption Standard–Counter with CBC-MAC
AES-CMAC	Advanced Encryption Standard-Cipher-based Message Authentication Code
AMP	Alternate MAC/PHY
AP	Access Point
ATT	Attribute Protocol
BR	Basic Rate
CBC-MAC	Cipher Block Chaining - Message Authentication Code (CMAC)
COF	Ciphering Offset Number
CSA	Core Specification Addendum
CSA5	Core Specification Addendum 5
CSRK	Connection Signature Resolving Key
CTIA	Cellular Telecommunications and Internet Association
dBm	Decibels referenced to one milliwatt
DHK	Diversifier Hiding Key
DHkey	Diffie-Hellman Key
DISA	Defense Information Systems Agency
DIV	Diversifier
DoD	Department of Defense
DoS	Denial of Service
DQPSK	Differential Quaternary Phase Shift Keying
ECDH	Elliptic Curve Diffie-Hellman
EDIV	Encrypted Diversifier
EDR	Enhanced Data Rate
ER	Encryption Root
eSCO	Enhanced Synchronous Connection Oriented
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GFSK	Gaussian Frequency-Shift Keying
GHz	Gigahertz
HCI	Host Controller Interface
HMAC	Hash Message Authentication Code
HS	High Speed
IBC	Iterated Block Cipher
IEEE	Institute of Electrical and Electronics Engineers
ILK	Intermediate Link Key
ILTK	Intermediate Long Term Key
IMEI	International Mobile Equipment Identity

IR	Identity Root
IRK	Identity Resolving Key
ISM	Industrial, Scientific, and Medical
ITL	Information Technology Laboratory
kbps	Kilobits per second
KG	Key Generator
KSG	Key Stream Generator
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
LCP	Link Control Protocol
LFSR	Linear Feedback Shift Register
LLP	Link Layer Protocol
LTK	Long-Term Key
m	Meter
MAC	Media Access Control
Mbps	Megabits per second
MHz	Megahertz
MIC	Message Integrity Check
MITM	Man-in-the-Middle
mW	Milliwatt
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database
OFDM	Orthogonal Frequency-Division Multiplexing
OMB	Office of Management and Budget
OOB	Out of Band
PC	Personal Computer
PHY	Physical Layer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PRNG	Pseudo-Random Number Generator
PUB	Publication
Rand	Random Number
RF	Radio Frequency
RFC	Request for Comment
RNG	Random Number Generator
RPA	Resolvable Private Address
RSSI	Received Signal Strength Indication
SAFER	Secure And Fast Encryption Routine
SDP	Service Discovery Protocol
SEG	Security Experts Group
SHA	Secure Hash Algorithm
SIG	Special Interest Group
SP	Special Publication
SRES	Signed Response
SSP	Secure Simple Pairing

STK	Short Term Key
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TK	Temporary Key
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network

Appendix C—Internal Bluetooth Functions

d1()	Diversifying function based on AES-128 encryption, used in Legacy Low Energy key generation.
dm()	DIV mask generation function, used in EDIV Generation and DIV Recovery
E0()	Stream cipher used to encrypt Bluetooth packet payloads.
E1()	Bluetooth legacy authentication function based.
E3()	Bluetooth key generation function.
E21()	Link key generator function, used when generating a key from the 48-bit address
E22()	Link key generator function, used when generating a key from the user PIN
f2()	BR/EDR and AMP Link key generator function
f3()	Simple Pairing check function, used to compute confirmation values
f5()	Low Energy Secure Connections key generation function
f6()	Low Energy Secure Connections DHKey check generation function
h4()	Secure Connections Device Authentication Key generation function
h5()	Secure Connections Device Confirmation function
h6()	Second Link Key Conversion function, used to create the Low Energy long term key derivation from a Bluetooth BR/EDR key
h7()	First Link Key Conversion function, used to create the Low Energy long term key derivation from a Bluetooth BR/EDR key

Appendix D—References

The list below provides references for the publication.

Bluetooth Special Interest Group, Bluetooth specifications. https://www.bluetooth.com/specifications/adopted-specifications

C. Gehrmann, J. Persson, and B. Smeets, *Bluetooth Security*, Artech House, 2004.

Y. Shaked and A. Wool, *Cracking the Bluetooth PIN*, In *Proc. 3rd USENIX/ACM Conf. Mobile Systems, Applications, and Services (MobiSys)*, pages 39–50, Seattle, WA, June 2005. https://www.usenix.org/event/mobisys05/tech/full_papers/shaked/shaked.pdf

D. Spill and A. Bittau, *BlueSniff: Eve meets Alice and Bluetooth*, 2007. https://www.usenix.org/event/woot07/tech/full_papers/spill/spill.pdf

Bluetooth SIG, *The Bluetooth Security White Paper*, 2002. http://grouper.ieee.org/groups/1451/5/Comparison%20of%20PHY/Bluetooth_24Security_Paper. pdf

Y. Lu, W. Meier, and S. Vaudenay. *The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption*, https://lasec.epfl.ch/pub/lasec/doc/LMV05.pdf

Appendix E—Resources

The lists below provide examples of resources related to Bluetooth that may be helpful to readers.

Documents

Name	URL
Bluetooth SIG Specifications	https://www.bluetooth.com/specifications/adopted-specifications
FIPS 140-2, *Security Requirements for Cryptographic Modules*	https://doi.org/10.6028/NIST.FIPS.140-2
FIPS 180-4, *Secure Hash Standard (SHS)*	https://doi.org/10.6028/NIST.FIPS.180-4
FIPS 186-4, *Digital Signature Standard (DSS)*	https://doi.org/10.6028/NIST.FIPS.186-4
FIPS 197, *Advanced Encryption Standard*	https://doi.org/10.6028/NIST.FIPS.197
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*	https://doi.org/10.6028/NIST.FIPS.199
GAO-05-383, *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*	http://www.gao.gov/new.items/d05383.pdf
NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*	https://doi.org/10.6028/NIST.SP.800-37r1
NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*	https://doi.org/10.6028/NIST.SP.800-53r4
NIST SP 800-63-2, *Electronic Authentication Guideline*	https://doi.org/10.6028/NIST.SP.800-63-2
NIST SP 800-64 Revision 2, *Security Considerations in the System Development Life Cycle*	https://doi.org/10.6028/NIST.SP.800-64r2
NIST SP 800-70 Revision 3, *National Checklist Program for IT Products—Guidelines for Checklists Users and Developers*	https://doi.org/10.6028/NIST.SP.800-70r3
NIST SP 800-90A Revision 1, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*	https://doi.org/10.6028/NIST.SP.800-90Ar1
NIST SP 800-90B (Draft), *Recommendation for the Entropy Sources Used for Random Bit Generation*	http://csrc.nist.gov/publications/drafts/800-90/sp800-90b_second_draft.pdf
NIST SP 800-90C (Draft), *Recommendation for Random Bit Generator (RBG) Constructions*	http://csrc.nist.gov/publications/drafts/800-90/sp800_90c_second_draft.pdf
NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*	https://doi.org/10.6028/NIST.SP.800-97
NIST SP 800-108, *Recommendation for Key Derivation Using Pseudorandom Functions*	https://doi.org/10.6028/NIST.SP.800-108
NIST SP 800-114 Revision 1, *User's Guide to Telework and Bring Your Own Device (BYOD) Security*	https://doi.org/10.6028/NIST.SP.800-114r1

Resource Sites

Name	URL
Bluetooth Special Interest Group	https://www.bluetooth.com/
Cellular Telecommunications and Internet Association (CTIA)	https://www.ctia.org/
Crackle	http://lacklustre.net/projects/crackle/
FIPS-Validated Cryptographic Modules	http://csrc.nist.gov/groups/STM/cmvp/validation.html
IEEE 802.15 Working Group for Wireless Personal Area Networks	http://www.ieee802.org/15/
NIST National Vulnerability Database (NVD)	https://nvd.nist.gov/
NIST's National Checklist Program	https://checklists.nist.gov/
Project Ubertooth	http://ubertooth.sourceforge.net
Trifinite Group (Bluetooth Security Research)	https://trifinite.org/