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

Special Publication 800-121

Guide to Bluetooth Security

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
John Padgette

AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

NIST Special Publication 800-121

Guide to Bluetooth Security

Recommendations of the National Institute of Standards and Technology

Karen Scarfone
John Padgette

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

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2008

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology

Dr. Patrick D. Gallagher, Deputy Director

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 analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-121
Natl. Inst. Stand. Technol. Spec. Publ. 800-121, 43 pages (Sep. 2008)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

APPL-1038
APPLE INC./Page 3 of 43

Acknowledgments

The authors, Karen Scarfone of the National Institute of Standards and Technology (NIST) and John Padgette of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Sheila Frankel, Tim Grance, and Tom Karygiannis of NIST, and Derrick Dicoi, Matthew Sexton, and Michael Bang of Booz Allen Hamilton, for their keen and insightful assistance throughout the development of the document. The authors also greatly appreciate the feedback provided by representatives from the Department of State, Gerry Barsczewski (Social Security Administration), and Alex Froede (Defense Information Systems Agency [DISA]).

Note to Readers

This document was originally released for public comment as part of Draft NIST Special Publication (SP) 800-48 Revision 1, *Wireless Network Security for IEEE 802.11a/b/g and Bluetooth*, which also provides information on securing legacy wireless local area networks (WLAN) unable to comply with the IEEE 802.11i security standard. Based on reviewer feedback, the Bluetooth material was removed from SP 800-48 Revision 1 and placed in this publication instead. Readers seeking information on WLAN security should consult the final version of SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks* for legacy WLANs and SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i* for current WLANs.

APPL-1038
APPLE INC./Page 4 of 43

Table of Contents

Executive Summary **ES-1**

1. Introduction **1-1**

1.1 Authority 1-1
1.2 Purpose and Scope 1-1
1.3 Audience and Assumptions 1-1
1.4 Document Organization 1-2

2. Overview of Bluetooth Technology **2-1**

2.1 Bluetooth Technology Characteristics 2-1
2.2 Bluetooth Architecture 2-3

3. Bluetooth Security Features **3-1**

3.1 Security Features of Bluetooth Specifications 3-2
3.2 Link Key Generation 3-2
3.2.1 Security Modes 2 and 3 3-3
3.2.2 Security Mode 4 3-4
3.3 Authentication 3-5
3.4 Confidentiality 3-7
3.5 Trust Levels, Service Levels, and Authorization 3-9

4. Bluetooth Vulnerabilities, Threats, and Countermeasures **4-1**

4.1 Bluetooth Vulnerabilities 4-1
4.2 Bluetooth Threats 4-2
4.3 Risk Mitigation and Countermeasures 4-3
4.4 Bluetooth Security Checklists 4-4

List of Appendices

Appendix A— Glossary of Terms **A-1**

Appendix B— Acronyms and Abbreviations **B-1**

Appendix C— References **C-1**

Appendix D— Online Resources **D-1**

APPL-1038
APPLE INC./Page 5 of 43

List of Figures

Figure 2-1. Bluetooth Ad Hoc Topology 2-3
Figure 2-2. Bluetooth Networks (Multiple Scatternets) 2-4
Figure 3-1. Bluetooth Air-Interface Security 3-1
Figure 3-2. Link Key Generation from PIN (v2.0 & earlier) 3-3
Figure 3-3. Link Key Establishment for Secure Simple Pairing 3-5
Figure 3-4. Bluetooth Authentication 3-6
Figure 3-5. Bluetooth Encryption Procedure 3-8

List of Tables

Table 2-1. Bluetooth Device Classes of Power Management 2-2
Table 4-1. Key Problems with Existing (Native) Bluetooth Security 4-1
Table 4-2. Bluetooth Piconet Security Checklist 4-5
Table 4-3. Bluetooth Headset Security Checklist 4-10
Table 4-4. Bluetooth Smart Card Reader Security Checklist 4-12

APPL-1038
APPLE INC./Page 6 of 43

Executive Summary

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets. 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 technology and discusses related security concerns.

There have been several versions of Bluetooth, with the most recent being 2.0 + Enhanced Data Rate (EDR) (November 2004) and 2.1 + EDR (July 2007). While 2.0 + EDR provided faster transmission speeds than previous versions (up to 3 Mbits/second), 2.1 + EDR provides a significant security improvement for link key generation and management in the form of Secure Simple Pairing (SSP). This publication addresses the security of these versions of Bluetooth, as well as the earlier versions 1.1 and 1.2.

Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation. They are also threatened by more specific Bluetooth-related attacks that target known vulnerabilities in Bluetooth implementations and specifications. Attacks against improperly secured Bluetooth implementations can provide attackers with unauthorized access to sensitive information and unauthorized usage of Bluetooth devices and other systems or networks to which the devices are connected.

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

Organizations should use the strongest Bluetooth security mode available for their Bluetooth devices.

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

Organizations using Bluetooth technology should address Bluetooth 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 requirements for selecting and using Bluetooth personal identification numbers (PIN). After establishing 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 that unneeded Bluetooth profiles and services be disabled to reduce the number of

vulnerabilities that attackers could attempt to exploit. When available, a centralized security policy management approach should be used to ensure device configurations are compliant.

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

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

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; however, such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b (3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, although attribution is desired.

Nothing in this document should be taken to contradict 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.

1.2 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 technologies on securing them effectively.

1.3 Audience and Assumptions

This document discusses Bluetooth 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 technologies within their organizations
- Systems engineers and architects who design and implement Bluetooth 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.

1.4 Document Organization

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

- Section 2 provides an overview of Bluetooth 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 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 references.
- Appendix D lists Bluetooth online resources.

APPL-1038
APPLE INC./Page 10 of 43

2. Overview of Bluetooth Technology

Bluetooth is an open standard for short-range radio frequency (RF) communication. Bluetooth technology is used primarily to establish wireless personal area networks (WPAN), commonly referred to as ad hoc or peer-to-peer (P2P) networks. Bluetooth technology has been integrated into many types of business and consumer devices, including cellular phones, personal digital assistants (PDA), laptops, automobiles, printers, and headsets. 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*.[1] A piconet is composed of two or more Bluetooth devices in close physical proximity that operate on the same channel using the same frequency hopping sequence. An example of a piconet is a Bluetooth-based connection between a cellular phone and a Bluetooth-enabled ear bud.

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

- **Cable replacement.** Bluetooth technology replaces a variety of cables, such as those traditionally used for peripheral devices (e.g., mouse and keyboard connections), printers, and wireless headsets and ear buds that interface with personal computers (PC) or mobile telephones.
- **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 provides automatic synchronization between Bluetooth-enabled devices. For example, Bluetooth allows synchronization of contact information contained in electronic address books and calendars.
- **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 have a mobile phone establish a dial-up connection, so that the laptop can access the Internet through the phone.

Bluetooth technology was originally conceived by Ericsson in 1994. Ericsson, IBM, Intel, Nokia, and Toshiba formed the Bluetooth Special Interest Group (SIG), a not-for-profit trade association developed to drive the development of Bluetooth products and serve as the governing body for Bluetooth specifications.[2] Bluetooth is standardized within the IEEE 802.15 Working Group for Wireless Personal Area Networks that formed in early 1999 as IEEE 802.15.1-2002.[3]

This section provides an overview of Bluetooth technology, such as frequency and data rates, range, and architecture.

2.1 Bluetooth Technology Characteristics

Bluetooth operates in the unlicensed 2.4 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 WLAN standard, making it somewhat crowded from the standpoint of the volume of wireless transmissions. Bluetooth employs frequency hopping spread spectrum (FHSS) technology for all transmissions. FHSS reduces interference and transmission errors and provides a limited level of transmission security. With FHSS technology, communications between Bluetooth devices use 79

---

1 As discussed in Section 2.2, the term "piconet" applies to both ad hoc and infrastructure Bluetooth networks.

2 The Bluetooth SIG web site (http://www.bluetooth.com/) is a resource for Bluetooth-related information and provides numerous links to other sources of information.

3 For more information, see the IEEE web site at http://grouper.ieee.org/groups/802/15/.

APPL-1038
APPLE INC./Page 11 of 43

different 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 microseconds for data/voice links), followed by a hop designated by a pre-determined pseudo-random sequence to another channel; this process is repeated continuously in the frequency-hopping sequence.

Bluetooth also provides for radio link power control, where devices can negotiate and adjust their radio power according to signal strength measurements. Each device in a Bluetooth network can determine its received signal strength indication (RSSI) and make a request of the other network device to adjust its relative radio power level (i.e., have the transmission power incrementally increased or decreased). 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 provide 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 transmission from direct sequence spread spectrum technologies, like those using IEEE 802.11a/b/g. If the Bluetooth power control feature is used appropriately, any potential adversary is forced to be in relatively close proximity to pose a threat to a Bluetooth piconet, especially if the Bluetooth devices are very close to each other.

Bluetooth versions 1.1 and 1.2 specify transmission speeds of up to 1 megabit per second (Mbps) and achieve throughput of approximately 720 kilobits per second (kbps). Bluetooth versions 2.0 + Enhanced Data Rate (EDR) and 2.1 + EDR specify data rates up to 3 Mbps and throughput of approximately 2.1 Mbps.

The range of Bluetooth 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).[4] Most small, battery-powered devices are Class 2, while Class 1 devices are typically USB dongles for desktop and laptop computers, as well as access points and other AC-powered devices.

Table 2-1. Bluetooth Device Classes of Power Management

Type	Power	Power Level	Designed Operating Range	Sample Devices
Class 1	High	100 mW (20 dBm)	Up to 91 meters (300 feet)	AC-powered devices (USB dongles, access points)
Class 2	Medium	2.5 mW (4 dBm)	Up to 9 meters (30 feet)	Battery-powered devices (mobile devices, Bluetooth adapters, smart card readers)
Class 3	Low	1 mW (0 dBm)	Up to 1 meter (3 feet)	Battery-powered devices (Bluetooth adapters)

So that Bluetooth devices can find and establish communication with each other, discoverable and connectable modes are specified. A device in *discoverable mode* periodically listens on an inquiry scan physical channel (based on a specific set of frequencies) and will respond to an inquiry on that channel with its device address, local clock, and other characteristics needed to page and subsequently connect to it. A device in *connectable mode* periodically listens on its page scan physical channel and will respond to a page on that channel to initiate a network connection. The frequencies associated with the page scan

[4] 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.

APPL-1038
APPLE INC./Page 12 of 43

physical channel for a device are based on its Bluetooth device address. Therefore, knowing a device's address and clock[5] is important for paging and subsequently connecting to the device.

2.2 Bluetooth Architecture

Bluetooth permits devices to establish either ad hoc or infrastructure networks. Infrastructure networks use fixed Bluetooth access points (AP), which facilitate communication between Bluetooth devices. This document focuses on ad hoc piconets, which are much more common than infrastructure networks. Ad hoc networks provide easy connection establishment between mobile 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 host 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 desktop computer. The host controller is responsible for the lower layers, including the Radio, Baseband, and Link Manager Protocol (LMP). The host controller functions are performed by an integrated or external (e.g., USB) Bluetooth dongle. The host and host controller send information to each other using the Host Controller Interface (HCI). In many cases, the host and host controller functions are integrated into a single device, with Bluetooth headsets being a prime example.

Figure 2-1 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. Piconets can scale to include up to seven active slave devices and up to 255 inactive slave devices.

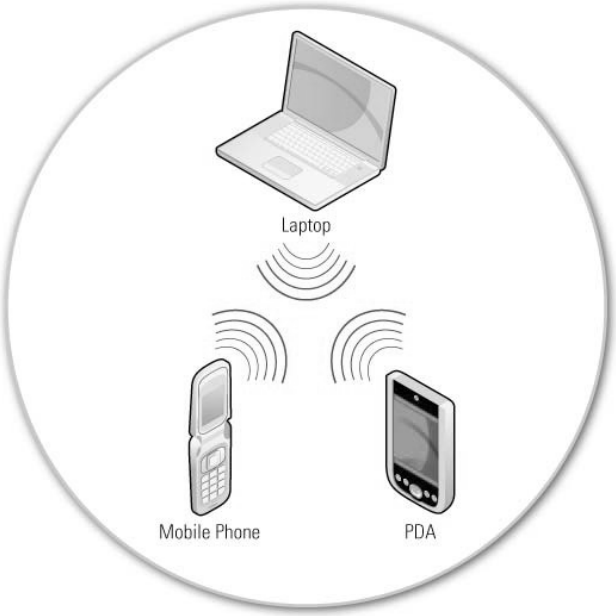

Figure 2-1. Bluetooth Ad Hoc Topology

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

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

multiplexing (TDM) allows a slave in one piconet to act as the master for another piconet simultaneously, thus creating a chain of networks.[6] This chain, called a *scatternet*, allows several devices to be networked 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, and therefore the relationships of the devices in the immediate network, may change. Figure 2-2 depicts a scatternet that connects three piconets.

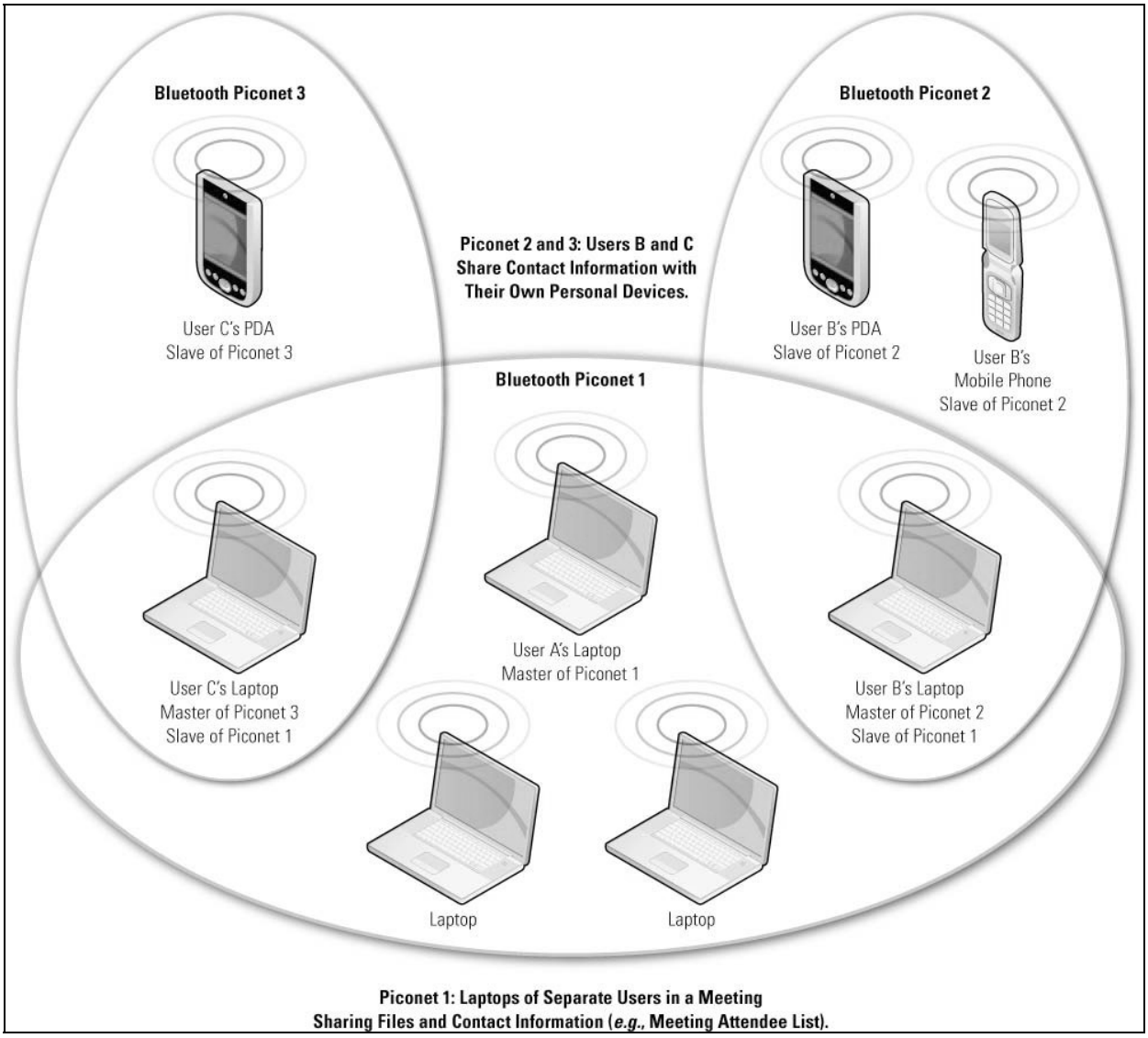

Figure 2-2. Bluetooth Networks (Multiple Scatternets)

Routing capabilities supported by Bluetooth networks control the changing network topologies of piconets and scatternets and assist in controlling the flow of data between networked devices. Bluetooth uses a combination of packet-switching and circuit-switching technologies. The use of packet switching in Bluetooth allows devices to route multiple packets of information over the same data path. This method does not consume all the resources of a data path, thereby allowing Bluetooth devices to maintain data flow throughout a scatternet.

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

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 some of 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 only between the mobile phone and the laptop computer, while IEEE 802.11 security protects the wireless local area network link between the laptop and the IEEE 802.11 AP. However, the communications on the wired network are not protected by Bluetooth or IEEE 802.11 security capabilities. End-to-end security is not possible without using higher-layer security solutions in addition to the security features included in the Bluetooth specification and IEEE 802.11 standards.

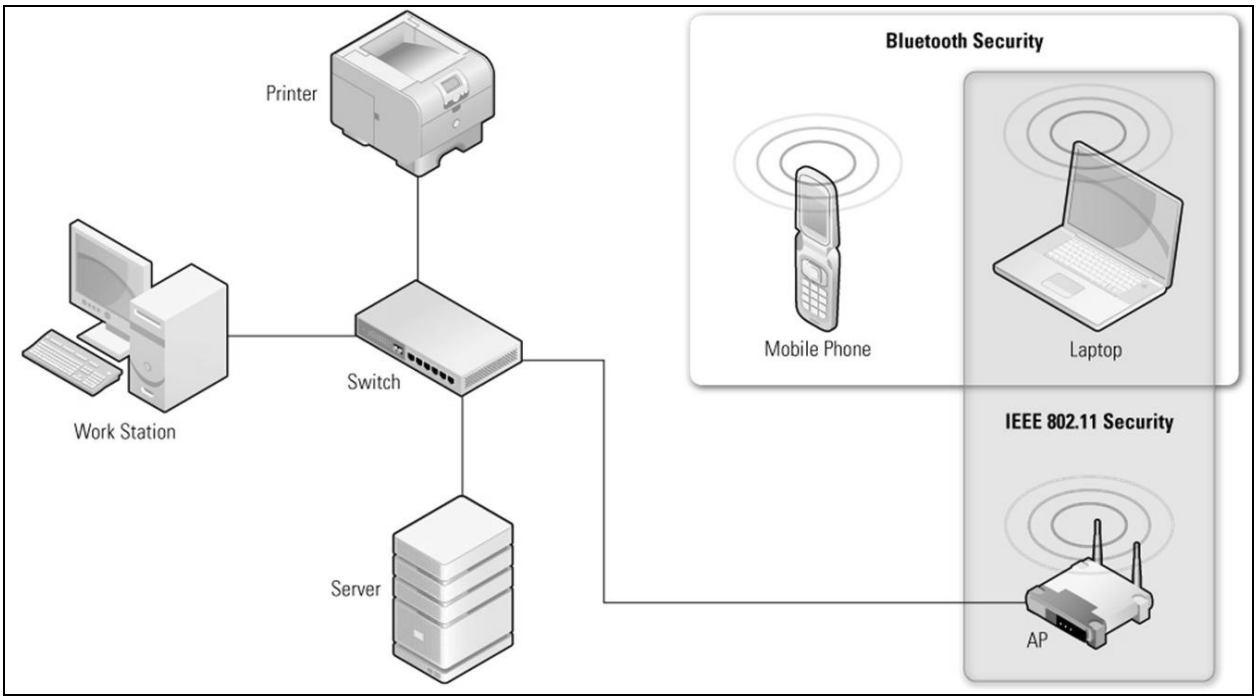

Figure 3-1. Bluetooth Air-Interface Security

The following are the three basic security services specified in the Bluetooth standard:

- **Authentication:** verifying the identity of communicating devices. User authentication is not provided natively by Bluetooth.
- **Confidentiality:** preventing information compromise caused by eavesdropping by ensuring that only authorized devices can access and view data.
- **Authorization:** allowing the control of resources by ensuring that a device is authorized to use a service before permitting it to do so.

The three 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 must be provided through additional means.

3.1 Security Features of Bluetooth Specifications

Cumulatively, the various versions of Bluetooth specifications define four security modes. Each version of Bluetooth supports some, but not all, of the four modes. Each Bluetooth device must operate in one of the four modes, which are described below.

Security Mode 1 is non-secure. Security functionality (authentication and encryption) is bypassed, leaving the device and connections susceptible to attackers. In effect, Bluetooth devices in this mode are "promiscuous" and do not employ any mechanisms to prevent other Bluetooth-enabled devices from establishing connections. Security Mode 1 is only supported in v2.0 + EDR (and earlier) devices.

In Security Mode 2, a service level-enforced security mode, security procedures are initiated after LMP link establishment but before L2CAP channel establishment. L2CAP resides in the data link layer and provides connection-oriented and connectionless data services to upper layers. For this security mode, a security manager (as specified in the Bluetooth architecture) controls access to specific services and devices. The centralized security manager maintains policies for access control and interfaces with other protocols and device users. Varying security policies and trust levels to restrict access may be defined for applications with different security requirements operating in parallel. It is possible to grant access to some services without providing access to other services. In this mode, the notion of authorization—the process of deciding if a specific device is allowed to have access to a specific service—is introduced. It is important to note that the authentication and encryption mechanisms used for Security Mode 2 are implemented at the LMP layer (below L2CAP), just as with Security Mode 3. All Bluetooth devices can support Security Mode 2; however, v2.1 + EDR devices can only support it for backward compatibility with v2.0 + EDR (or earlier) devices.

In Security Mode 3, the link level-enforced security mode, a Bluetooth device initiates security procedures before the physical link is fully established. Bluetooth devices operating in Security Mode 3 mandates authentication and encryption for all connections to and from the device. This mode supports authentication (unidirectional or mutual) and encryption. The authentication and encryption features are based on a separate secret link key that is shared by paired devices, once the pairing has been established. Security Mode 3 is only supported in v2.0 + EDR (or earlier) devices.

Similar to Security Mode 2, Security Mode 4 (introduced in Bluetooth v2.1 + EDR) is a service level enforced security mode in which security procedures are initiated after link setup. Secure Simple Pairing uses Elliptic Curve Diffie Hellman (ECDH) techniques for key exchange and link key generation. Device authentication and encryption algorithms are identical to the algorithms in Bluetooth v2.0 + EDR and earlier versions. Security requirements for services protected by Security Mode 4 must be classified as one of the following: authenticated link key required, unauthenticated link key required, or no security required. Whether or not a link key is authenticated depends on the Secure Simple Pairing association model used. See Section 3.2.2 for a description of Secure Simple Pairing. Security Mode 4 is mandatory for communication between v2.1 + EDR devices.

The rest of this section discusses specific Bluetooth security components in more detail: link key generation, authentication, confidentiality, and other Bluetooth security mechanisms.

3.2 Link Key Generation

As mentioned in Section 3.1, there are two methods in which link key generation is performed for Bluetooth. Security Modes 2 and 3 use one method, while Security Mode 4 uses another. Both methods are described below.

APPL-1038
APPLE INC./Page 16 of 43

3.2.1 Security Modes 2 and 3

For Bluetooth v2.0 + EDR (and earlier), operating in Security Mode 2 or 3, two associated devices simultaneously derive link keys during the initialization phase when users enter an identical PIN into one or both devices, depending on the configuration and device type. The PIN entry, device association, and key derivation are depicted conceptually in Figure 3-2. Note that if the PIN is less than 16 bytes, the BD_ADDR is used to supplement the PIN value used to generate the initialization key. The E_x boxes represent encryption algorithms that are used during the Bluetooth device association and key derivation processes. More details on the Bluetooth authentication and encryption procedures are outlined in Sections 3.4 and 3.5, respectively.

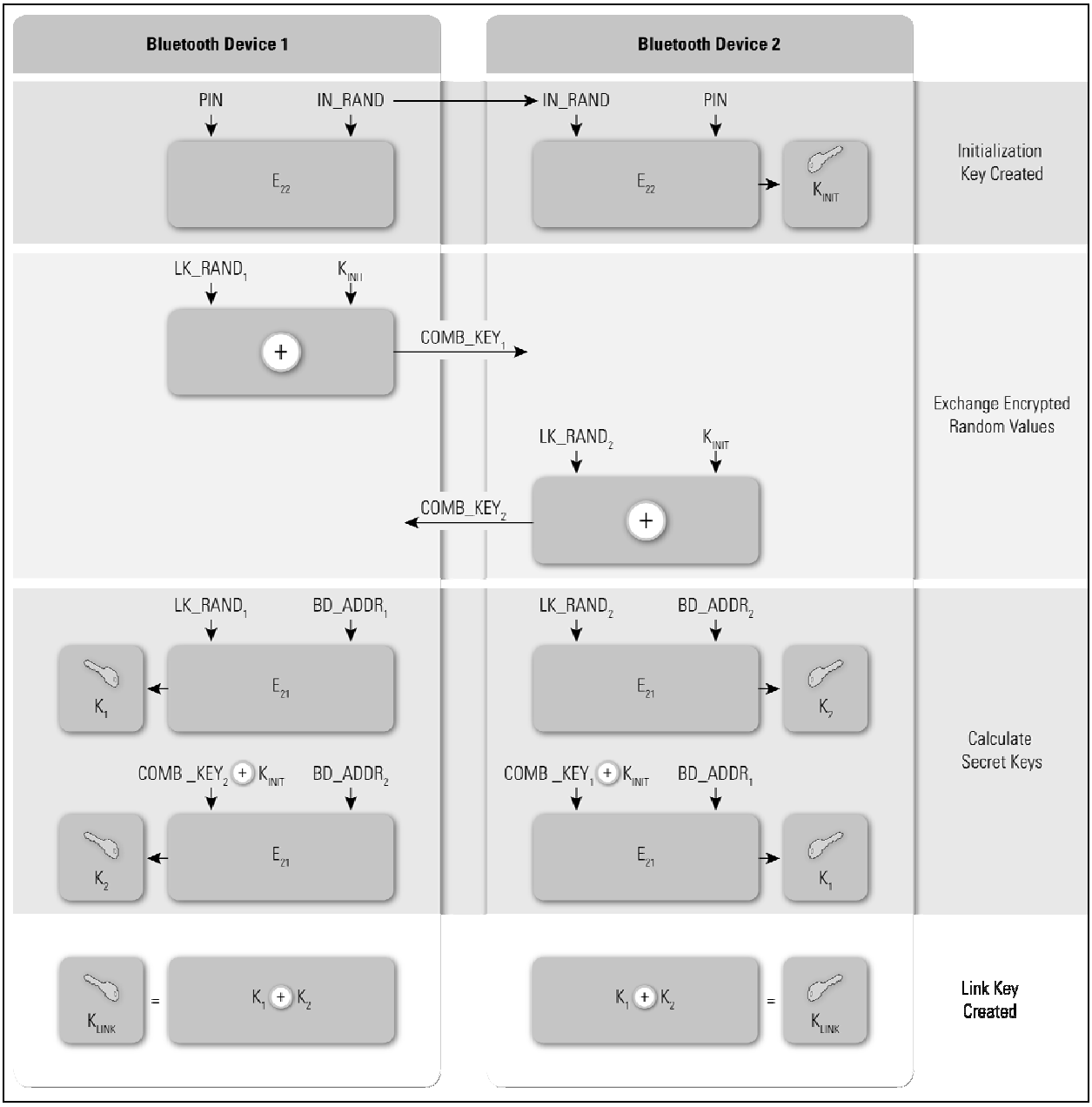

Figure 3-2. Link Key Generation from PIN (v2.0 & earlier)

After initialization is complete, devices automatically and transparently authenticate and initiate the encryption procedure to secure the wireless link, if encryption is enabled. The PIN code used in Bluetooth devices can vary between one and 16 bytes. The typical four-digit PIN may be sufficient for low-risk situations; a longer PIN should be used for devices that require a higher level of security.[7]

3.2.2 Security Mode 4

Secure Simple Pairing (SSP) was introduced in Bluetooth v2.1 + EDR for use with Security Mode 4. SSP simplifies the pairing process by providing a number of association models that are flexible in terms of device input capability. SSP also improves security through the addition of ECDH public key cryptography for protection against passive eavesdropping and man-in-the-middle attacks (MITM) during pairing.

The four association models offered in SSP are as follows:[8]

- **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 will fail. A key difference between this operation and the use of PINs in legacy pairing is that the displayed number is not used as input to subsequent link key generation. An attacker 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., Bluetooth-enabled 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 hence is of no value to an attacker.
- **Just Works** was designed for the situation where one (or both) of the pairing devices has neither a display nor a keyboard for entering digits (e.g., Bluetooth-enabled headset). It performs Authentication Stage 1 (see Figure 3-3 below) 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 MITM protection is not provided.
- **Out of Band (OOB)** was designed for devices that support a wireless technology other than Bluetooth (e.g., Near Field Communication [NFC]) 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 the chosen OOB wireless technology should be configured to mitigate eavesdropping and MITM attacks to keep the pairing process as secure as possible.

Security Mode 4 requires Bluetooth services to mandate an authenticated link key, an unauthenticated link key, or no security at all. Of the association models described above, all but the Just Works model provide authenticated link keys.

---

7 The Bluetooth Security White Paper from the Bluetooth Special Interest Group is available at http://www.bluetooth.com/NR/rdonlyres/E870794C-2788-49BF-96D3-C9578E0AE21D/0/security_whitepaper_v1.pdf.

8 This information is derived from "Simple Pairing Whitepaper", written by the Bluetooth Special Interest Group, August 2006. The paper is available at http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf.

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.

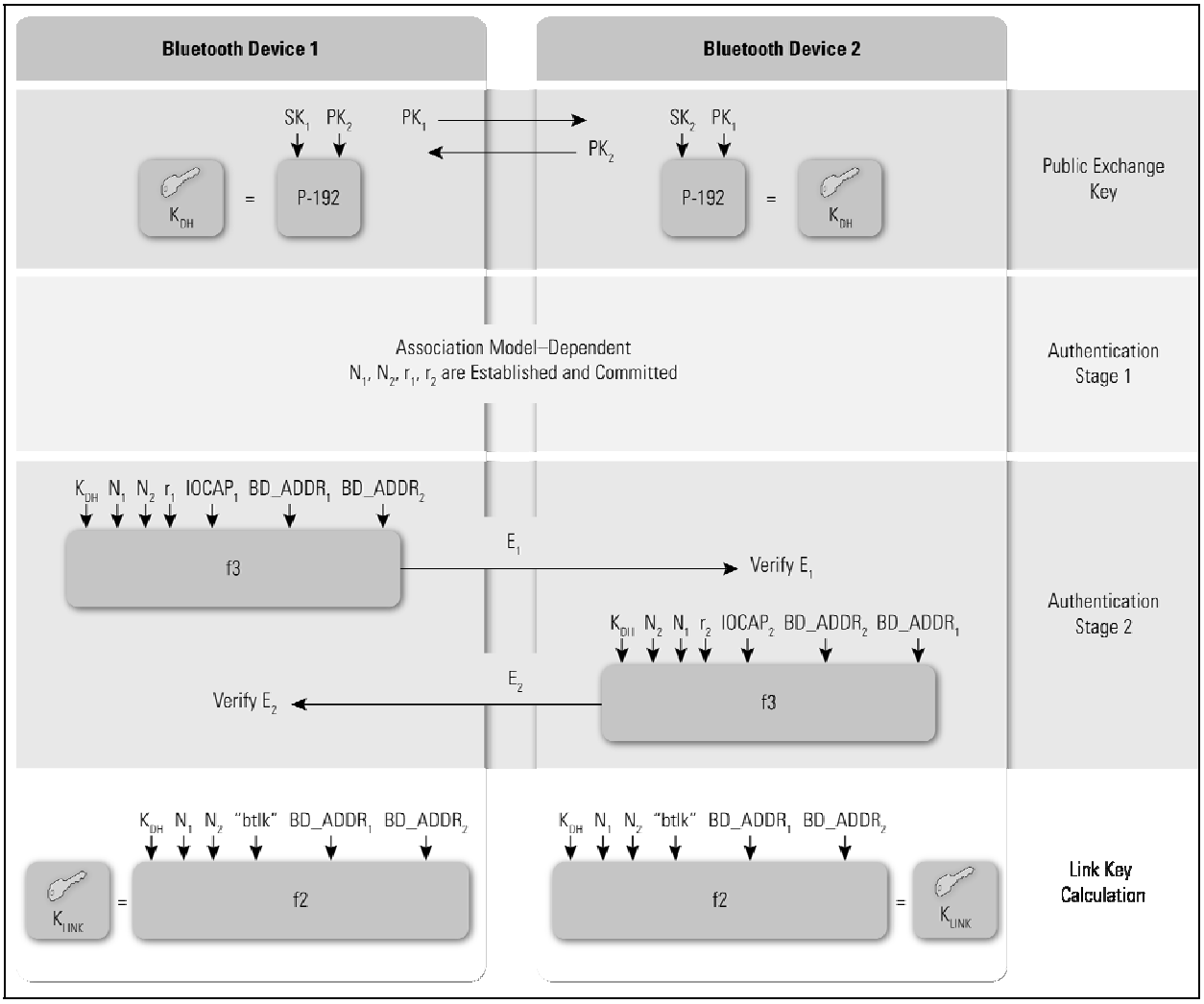

Figure 3-3. Link Key Establishment for Secure Simple Pairing

3.3 Authentication

The Bluetooth device authentication procedure is in the form of a challenge-response scheme. Each device interacting in an authentication procedure is referred to as either the claimant or the verifier. 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 challenge-response verification scheme is depicted conceptually in Figure 3-4.

APPL-1038
APPLE INC./Page 19 of 43

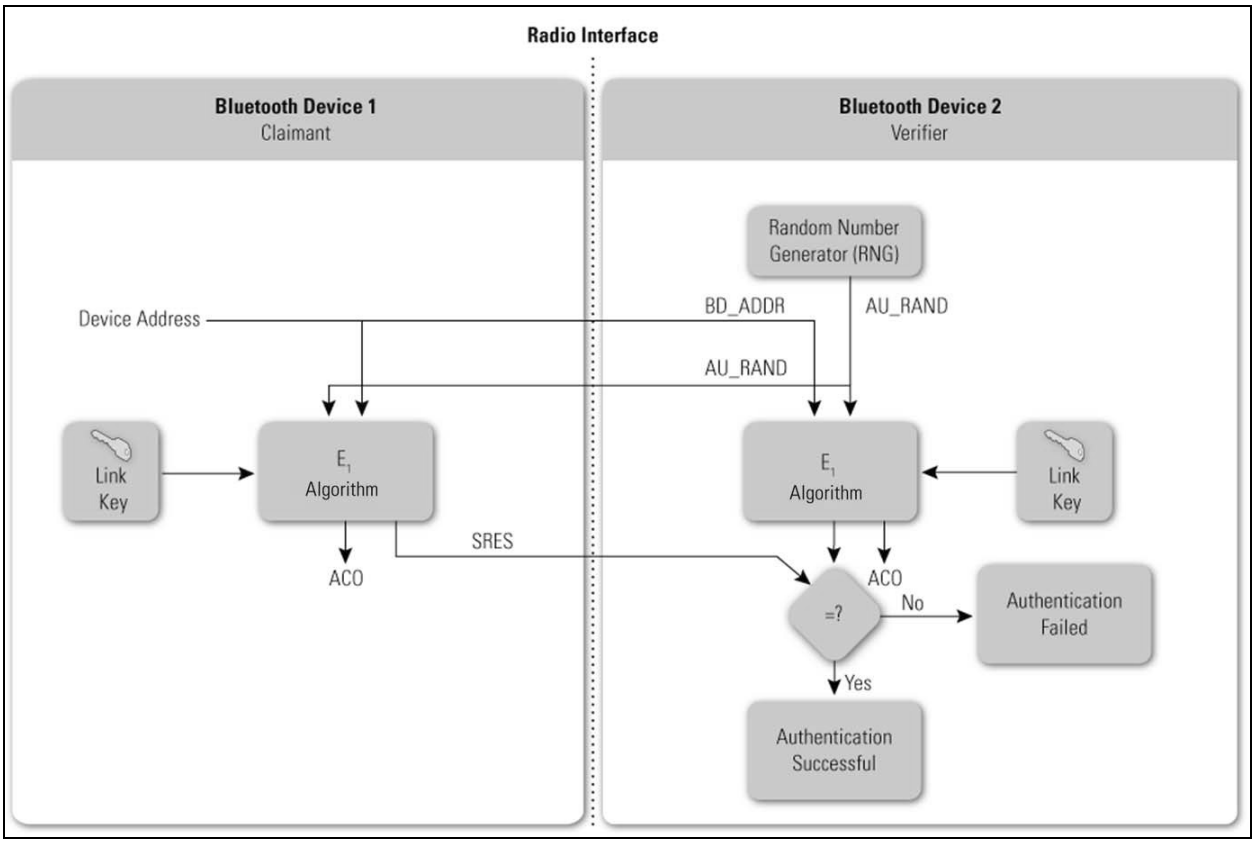

Figure 3-4. Bluetooth Authentication

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[9] to compute an authentication response using his 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 Authenticated Ciphering Offset (ACO) value, which will be used later 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, 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 has failed.

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.

[9] The E_1 authentication function is based on the SAFER+ algorithm. SAFER stands for Secure And Fast Encryption Routine. The SAFER algorithms are iterated block ciphers (IBC). In an IBC, the same cryptographic function is applied for a specified number of rounds.

If authentication fails, a Bluetooth device waits an interval of time before a new attempt is made. 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 keys. It is important to note that this *suspend* technique does not provide security against sophisticated adversaries performing offline attacks to exhaustively search 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 is never disclosed outside the Bluetooth device or transmitted over wireless links. The link key is passed in the clear from the host to the host controller (e.g., PC to USB dongle) if the host is used for key storage. The random challenge, which is a public parameter associated with the authentication process, is designed to be different for every transaction. The random number is derived from a pseudo-random process within the Bluetooth device. The cryptographic response is public as well and part of the encryption establishment process.

3.4 Confidentiality

In addition to the Security Modes, Bluetooth provides a separate confidentiality service to thwart eavesdropping attempts 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.

Encryption Modes 2 and 3 use the same encryption mechanism.

As shown in Figure 3-5, 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 3-4.

The Bluetooth 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 (LFSR).[10] The encryption function takes the following as inputs: the master identity (BD_ADDR), the 128-bit random number (EN_RAND), a slot number, 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.

[10] 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.

APPL-1038
APPLE INC./Page 21 of 43

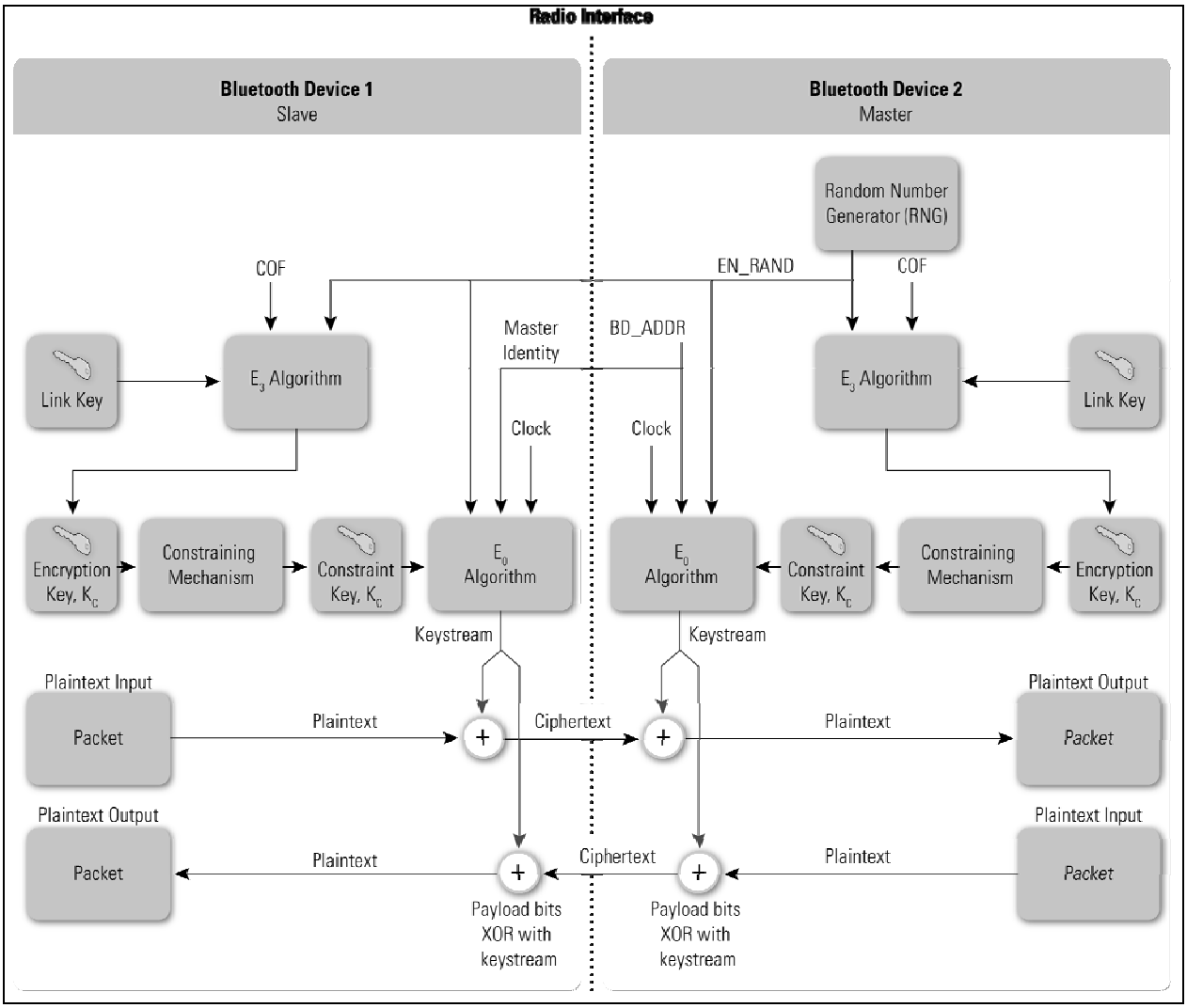

Figure 3-5. Bluetooth Encryption Procedure

The encryption key (K_C) is generated from the current link key and may vary from eight bits to 128 bits. The key size negotiation process occurs between the master and slave devices. During negotiation, a master device makes a key size suggestion for the slave. The initial key size suggested by the master is programmed into the host controller by the manufacturer and is not always 128-bit. 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 eight bits, making the link less secure.

It is important to note that E_0 is not a Federal Information Processing Standards (FIPS) approved algorithm and has come under scrutiny recently in terms of algorithmic strength.[11] A recently published theoretical known-plaintext attack has been discovered that can recover the encryption key in 2^{38} computations, as compared to a brute force attack, which would require the testing of 2^{128} possible keys. If communications require FIPS-approved cryptographic protection (e.g., sensitive information

[11] Y. Lu, W. Meier, and S. Vaudenay. "The Conditional Correlation Attack: A Practical Attack on Bluetooth Encryption". http://lasecwww.epfl.ch/pub/lasec/doc/LMV05.pdf

transmitted by Federal agencies), this can be achieved by employing application-level FIPS-approved encryption over the native Bluetooth encryption.

3.5 Trust Levels, Service Levels, and Authorization

In addition to the four security modes, Bluetooth allows two levels of trust and three levels of 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. Three levels of security have been defined for Bluetooth services. These levels allow the requirements for authorization, authentication, and encryption to be configured and altered independently. The service security levels are as follows:

- **Service Level 1—**Requires authorization and authentication. Automatic access is granted only to trusted devices; untrusted devices need manual authorization.
- **Service Level 2—**Requires authentication only; authorization is not necessary. Access to an application is allowed only after an authentication procedure.
- **Service Level 3—**Open to all devices, with no authentication required. Access is granted automatically.

The Bluetooth architecture allows for defining security policies that can set trust relationships in such a way that even trusted devices can get access only to specific services. It is important to understand that although Bluetooth core protocols can only authenticate devices and not users, it is possible to initiate user-based authentication in an alternative manner. 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, it is possible to enforce user-based authentication and fine-grained access control within the Bluetooth security framework through the application layers.

APPL-1038
APPLE INC./Page 23 of 43

4. Bluetooth Vulnerabilities, Threats, and Countermeasures

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

Organizations that are planning countermeasures for Bluetooth technologies that use the v2.1 + EDR specification should carefully consider its security implications. The specification was released in mid-2007, and as of mid-2008, few products that support the specification are yet available. As the specification becomes more widely adopted, it is likely that additional vulnerabilities will be discovered and additional recommendations needed for securing v2.1 technologies effectively. Organizations planning on deploying v2.1 technologies should monitor developments involving new vulnerabilities and threats and additional security control recommendations.

4.1 Bluetooth Vulnerabilities

Table 4-1 below provides an overview of some of the known security vulnerabilities with Bluetooth. The Bluetooth security checklist in Section 4.4 addresses these vulnerabilities.

Table 4-1. Key Problems with Existing (Native) Bluetooth Security

	Security Issue or Vulnerability	Remarks
Versions Before Bluetooth v1.2		
1	**Unit key is reusable and becomes public once used.**	A unit key should be used as input to generate a random key. A key set should be used instead of only one unit key.
2	**Unit key sharing can lead to eavesdropping.**	A corrupt user may be able to compromise the security between two other users if the corrupt user has communicated with either of the other two users. This is because the link key (unit key), derived from shared information, has been disclosed.
Versions Before Bluetooth v2.1		
3	**Short PINs are allowed.**	Weak PINs, which are used for the generation of link and encryption keys, can be easily guessed. People have a tendency to select short PINs.
4	**PIN management is lacking.**	Establishing use of adequate PINs in an enterprise setting with many users may be difficult. Scalability problems frequently yield security problems.
5	**Encryption keystream repeats after 23.3 hours of use.**	Per Figure 3-5, 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.
All Versions		
6	**Link keys are stored improperly.**	Link keys can be read or modified by an attacker if they are not securely stored and protected via access controls.

	Security Issue or Vulnerability	Remarks
7	**Attempts for authentication are repeated.**	A limiting feature needs to be incorporated in the specification to prevent unlimited requests. The Bluetooth specification currently requires a time-out period between repeated attempts that will increase exponentially.
8	**Strength of the challenge-response pseudo-random generator is not known.**	The Random Number Generator (RNG) may produce static number or periodic numbers that may reduce the effectiveness of the authentication scheme.
9	**Encryption key length is negotiable.**	The specification allows devices to negotiate encryption keys as small as one byte. A more robust encryption key generation procedure needs to be incorporated in the specification.
10	**The master key is shared.**	A better broadcast keying scheme needs to be incorporated into the specification.
11	**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.
12	**The E_0 stream cipher algorithm used for Bluetooth encryption is weak.**	More robust encryption needs to be incorporated in the specification.
13	**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 could be logged, resulting in a loss of privacy.
14	**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 users and the network are legitimate.
15	**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.
16	**Security services are limited.**	Audit, nonrepudiation, and other services are not part of the standard. If needed, these services can be incorporated in an overlay fashion by the application developer.
17	**Discoverable and/or connectable devices are prone to attack.**	Any device that must go into discoverable or connectable mode to pair should only do so for a minimal amount of time. A device should never be in discoverable or connectable mode all the time.

4.2 Bluetooth Threats

Bluetooth offers several benefits and advantages, but the benefits of Bluetooth are not provided without risk. Bluetooth technology and associated devices are susceptible to general wireless networking threats, such as denial of service attacks, eavesdropping, man-in-the-middle attacks, message modification, and resource misappropriation,[12] and are also threatened by more specific Bluetooth-related attacks, such as the following:

[12] 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* (http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf).

- **Bluesnarfing.** Bluesnarfing[13] enables attackers to gain access to a Bluetooth-enabled device by exploiting a firmware flaw in older devices. This attack forces a connection to a Bluetooth device, allowing access to data stored on the device and even 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.

- **Bluejacking.** Bluejacking is an attack conducted on Bluetooth-enabled mobile devices, such as cellular telephones, smart phones, and PDAs. Bluejacking is initiated by an attacker sending unsolicited messages to a user of a Bluetooth-enabled device. The actual messages do not cause harm to the user's device, but they are used to 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 that is sent with a harmful intent.

- **Bluebugging.** Bluebugging[14] exploits a security flaw in the firmware of some older 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 telephone calls, eavesdrop on telephone calls, send messages, and exploit other services or features offered by the device.

- **Car Whisperer.** Car Whisperer[15] is a software tool developed by European security researchers that exploits a key implementation issue 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.** Bluetooth is susceptible to DoS attacks. Impacts include making a device's Bluetooth interface unusable and draining the mobile device's battery. These types of attacks are not significant and, due to the proximity required for Bluetooth use, can usually be easily averted by simply walking away.

- **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. When a device's response is slowed or stopped by these attacks, this indicates that a serious vulnerability potentially exists in the protocol stack.

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 checklists in Section 4.4 do not guarantee a secure Bluetooth environment and cannot prevent all adversary penetrations. Also, security comes at a cost—financial expenses related to security equipment, inconvenience, maintenance, and operation. Each organization needs to 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 life cycle of Bluetooth solutions.[16]

---

13 http://trifinite.org/trifinite_stuff_bluesnarf.html
14 http://trifinite.org/trifinite_stuff_bluebug.html
15 http://trifinite.org/trifinite_stuff_carwhisperer.html
16 For more information about technology life cycles, see NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle* (http://csrc.nist.gov/publications/PubsSPs.html).

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 management, operational, and technical security controls for information systems based on the FIPS PUB 199 impact categories.[17] The recommendations in NIST SP 800-53 should be helpful to organizations in identifying controls that are 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 technology 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 enforced.

The general nature and mobility of Bluetooth-enabled devices increases the difficulty of employing traditional security measures. 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 checklists in Section 4.4.

4.4 Bluetooth Security Checklists

This section provides Bluetooth security checklists. For each recommendation or guideline in a 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 and justification, a checklist with three columns is provided. 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 provides a Bluetooth security checklist with guidelines and recommendations for creating and maintaining secure Bluetooth piconets. Additional checklists for Bluetooth headsets and smart card readers are located later in this section.

[17] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, is available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf. NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*, is available at http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf.

APPL-1038
APPLE INC./Page 27 of 43

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 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 security practices that help prevent security incidents.	✓		
3	Perform comprehensive security assessments at regular intervals to fully understand the organization's Bluetooth security posture.	Bluetooth products should support upgrade and patching of firmware to be able to take advantage of Bluetooth security enhancements and fixes.	✓		
4	Ensure that wireless devices and networks involving Bluetooth technology 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 must 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.	✓		
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 should be responsible for its wireless technology components because theft of those components could lead to malicious activities against the organization's information system resource.	✓		
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 company security policy.	✓		

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
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 should be avoided due to their extended range (approximately 100 meters).	✓		
9	Choose PIN codes that are sufficiently random and long. Avoid static and weak PINs, such as all zeroes.	PIN codes should be random so that they cannot be easily guessed by malicious users. Longer PIN codes are more resistant to brute force attacks. For Bluetooth v2.0 (or earlier) devices, an eight-character alphanumeric PIN should be used, if possible. The use of a fixed PIN is not acceptable for sensitive Bluetooth connections.	✓		
10	Ensure that link keys are based on combination keys rather than unit keys.	The use of shared unit keys can lead to successful MITM attacks. The use of unit keys for security was deprecated in Bluetooth v1.2.	✓		
11	For v2.1 devices using Secure Simple Pairing, avoid using the "Just Works" model.	The "Just Works" association model does not provide MITM protection. Devices that only support Just Works should not be procured if similarly qualified devices that support one of the other association models (i.e., Numeric Comparison, Out Of Band, or Passkey Entry) are available.	✓		
12	Service and profile lockdown of device Bluetooth stacks should be performed.[18]	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 approved profiles and services are available for use.	✓		
13	Bluetooth devices should be configured by default as, and remain, undiscoverable except as needed for pairing.	Bluetooth interfaces should be configured as non-discoverable, which prevents visibility to other Bluetooth devices except when discovery is specifically needed. Also, the default self-identifying or discoverable names provided on Bluetooth devices should be changed to anonymous, unidentifiable names.	✓		

[18] Derived from requirement 6.0 in DoD's Bluetooth Smart Card Reader Security Requirements Matrix (01 June 2007), available at http://iase.disa.mil/stigs/checklist/DoD-Bluetooth-Smart-Card-Reader-Security-Requirements-Matrix.pdf

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
14	Invoke link encryption for all Bluetooth connections regardless of how needless encryption may seem (i.e., no Security Mode 1).	Link encryption should be used to secure all data transmissions during a Bluetooth connection, otherwise transmitted data is vulnerable to eavesdropping.	✓		
15	If multi-hop wireless communication is being utilized, ensure that encryption is enabled on every link in the communication chain.	Every link should be secured because one unsecured link results in compromising the entire communication chain.	✓		
16	Ensure device mutual authentication is performed for all accesses.	Mutual authentication is required to provide verification that all devices on the network are legitimate.	✓		
17	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.	✓		
18	Configure encryption key sizes to the maximum allowable.	Using maximum allowable key sizes provides protection from brute force attacks.	✓		
19	Establish a “minimum key size” for any key negotiation process.	Establishing minimum key sizes ensures that all keys are long enough to be resistant to brute force attacks. Preferably, keys should be at least 128 bits long.	✓		
20	Use application-level (on top of the Bluetooth stack) authentication and encryption 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 140-2 validated) over the native encryption will further protect the data in transit.		✓	
21	Deploy user authentication 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.		✓	

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
Operational Recommendations					
22	Ensure that Bluetooth devices are turned off when they are not used.	Bluetooth capabilities should be disabled on all Bluetooth devices, except when the user explicitly enables Bluetooth to establish a connection. Shutting down Bluetooth devices when not in use minimizes exposure to potential malicious activities.	✓		
23	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.[19]	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-v.2.1 devices (security is solely dependent on PIN entropy and length). This is also recommended for v2.1 devices, although similar attacks against Secure Simple Pairing have not yet been documented.	✓		
24	A 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. It is highly recommended that devices use Security Mode 3. (However, note that v2.1 devices cannot use Security Mode 3.)	✓		
25	Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.	Authenticating users to a portable Bluetooth device is a good security practice in the event the device is lost or stolen, which provides a layer of protection for an organization's Bluetooth network.	✓		
26	In the event a Bluetooth device is lost or stolen, users should immediately unpair the missing device from all other Bluetooth devices with which it was previously paired.	This will prevent an attacker from using the lost or stolen device to access another Bluetooth device owned by the user(s).	✓		

[19] Derived from requirement 2.2 in DoD's Bluetooth Smart Card Reader Security Requirements Matrix (01 June 2007), available at http://iase.disa.mil/stigs/checklist/DoD-Bluetooth-Smart-Card-Reader-Security-Requirements-Matrix.pdf

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
27	Install antivirus software on Bluetooth-enabled hosts that are frequently targeted by malware.	Antivirus software should be installed on frequently targeted Bluetooth-enabled hosts to ensure that known malware is not introduced to the Bluetooth network. Organizations may also choose to deploy antivirus software on less-often targeted Bluetooth-enabled hosts.	✓		
28	Fully test and deploy Bluetooth software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should be fully tested before implementation to ensure that they work.	✓		
29	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	✓		
30	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.	✓		
31	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 appointed 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 provides guidelines and recommendations on Bluetooth headsets based on the Department of Defense's (DoD) Bluetooth Headset Security Requirements Matrix (Version 2.0, 07 April 2008)[20]. These recommendations are only intended for situations where the organization is concerned about threats within physical range of the Bluetooth headset usage. Note that most commercially available Bluetooth headsets, handsets, and hands-free devices cannot be configured to meet the recommendations in Table 4-3. Most of those devices do not provide encryption and often use a four-digit PIN with a default value like "0000" that cannot be changed.

[20] http://iase.disa.mil/stigs/checklist/dod_bluetooth_headset_security_requirements_matrix_v2-0_7april2008.pdf

Table 4-3. Bluetooth Headset Security Checklist

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
1	Bluetooth v1.2 or later should be used.	The Bluetooth 1.2 specification deprecated the use of unit keys for link key generation. It also included enhancements such as adaptive frequency hopping (AFH) which improved resistance to radio frequency interference in the crowded 2.4 GHz band (which is used by IEEE 802.11b/g and other protocols).	✓		
2	Bluetooth radios should be Class 2 or Class 3.	Bluetooth Class 1 radios provide 100mW of power with an approximate range of 100 meters, which facilitates discovery and eavesdropping by attackers.	✓		
3	Bluetooth pairing passkeys should be at least eight decimal digits in length and generated randomly for each pairing.	For pre-v2.1 devices, this is essential to prevent link key cracking if pairing messages have been successfully eavesdropped by an attacker. Note that v2.1 devices using the Numerical Comparison or Passkey Entry association models will always use a 6-digit passkey per the Bluetooth specification. This is currently deemed adequate since v2.1 passkeys used during Secure Simple Pairing—by design—cannot be used to derive the associated link key.	✓		
4	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.)	Key establishment 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-v.2.1 devices (security is solely dependent on PIN entropy and length). This is also recommended for v2.1 devices, although similar attacks against Secure Simple Pairing have not yet been documented.	✓		

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
5	The Bluetooth headset/audio gateway device should remain undiscoverable to other Bluetooth devices at all times other than the initial pairing process. It should only support the minimal amount of Bluetooth services required for use as a headset for a handheld device.	While a Bluetooth device is in discoverable mode, any inquiring device within range can capture important connection information including device address and clock, which is the first stage of any Bluetooth attack.	✓		
6	Bluetooth Security Mode 3 (link level security) should be used by both the headset and the audio gateway device along with 128-bit Bluetooth encryption.	Security Mode 3 provides link-level security, which requires authentication and encryption prior to link establishment. (However, note that v2.1 devices cannot use Security Mode 3.) 128-bit encryption is the maximum provided by the Bluetooth specification, so it should be used to mitigate potential attacks against lower entropy (weak) cryptographic keys.	✓		
7	Devices should support only a single headset connection between one headset and one handheld device or audio gateway device.	Bluetooth headset support for multiple simultaneous connections would provide an additional attack vector.	✓		
8	The user should be able to authorize all initial incoming connection requests, and there should be an indication of any active Bluetooth link on both the handheld device and the Bluetooth headset.	The user should be made aware of, and explicitly authorize, all connections associated with the headset to preclude potential attacks.	✓		
9	Bluetooth stack lockdown techniques should be used on the handheld device to disable unauthorized Bluetooth connections (headset profile and serial port profile are authorized). Unnecessary Bluetooth services, user controls, and applications should be either removed from the handheld device or reliably disabled permanently so that users cannot enable them. Note: This feature may already be included with the handheld device security policy manager.	The Bluetooth stack on the handheld device should only support the minimal services/profiles approved for use. Supporting unauthorized services/profiles could introduce vulnerabilities.	✓		

Table 4-4 provides recommendations on Bluetooth smart card readers based on DoD's Bluetooth Smart Card Reader Security Requirements Matrix (01 June 2007)[21]. Note that FIPS-140 validated encryption is recommended in addition to native Bluetooth authentication and encryption.

Table 4-4. Bluetooth Smart Card Reader Security Checklist

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
1	Bluetooth mutual authentication, 128-bit Bluetooth encryption, and FIPS 140-validated cryptography should all be used for all communications between the smart card reader and the host device.	Strong authentication and encryption is essential to network security, especially wireless connections. Mutual authentication confirms both devices have the appropriate link key, and 128-bit encryption is the maximum key length provided by the Bluetooth specification. FIPS 140-validated cryptography should also be used to compensate for weaknesses in the native Bluetooth encryption.	✓		
2	Bluetooth pairing passkeys should be at least eight decimal digits in length and generated randomly for each pairing.	For pre-v2.1 devices, this is essential to prevent link key cracking if pairing messages have been successfully eavesdropped by an attacker. Note that v2.1 devices using the Numerical Comparison or Passkey Entry association models will always use a 6-digit passkey per the Bluetooth specification. This is currently deemed adequate since v2.1 passkeys used during Secure Simple Pairing—by design—cannot be used to derive the associated link key.	✓		
3	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.)	Key establishment 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-v.2.1 devices (security is solely dependent on PIN entropy and length). This is also recommended for v2.1 devices, although similar attacks against Secure Simple Pairing have not yet been documented.	✓		
4	Bluetooth mutual authentication should occur immediately after the initial establishment of any Bluetooth connection.	Devices should authenticate each other as soon as possible and certainly before providing access to any offered services.	✓		

[21] http://iase.disa.mil/stigs/checklist/DoD-Bluetooth-Smart-Card-Reader-Security-Requirements-Matrix.pdf

	Security Recommendation	Security Need, Requirement, or Justification	Checklist		
			Recom-mended Practice	Should Consider	Status
5	The Bluetooth smart card reader should remain undiscoverable to other Bluetooth devices at all times other than the initial pairing process and cannot initiate Bluetooth connections on its own. It should only support the minimal amount of Bluetooth services required for use as a smart card reader for a single host device.	While a Bluetooth device is in discoverable mode, any inquiring device within range can capture important connection information including device address and clock, which is the first stage of any Bluetooth attack.	✓		
6	Unnecessary Bluetooth services, user controls, and applications should be either removed from the host device or reliably disabled permanently.	The Bluetooth stack on the host device should only support the minimal features approved for use. Supporting other features could introduce vulnerabilities unnecessarily.	✓		
7	All Bluetooth profiles except for Serial Port Profile should be disabled at all times, and the user should not be able to enable them.	Additional profiles could introduce vulnerabilities unnecessarily. The Serial Port Profile is the only profile needed for smart card readers.	✓		

Appendix A—Glossary of Terms

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 dynamically connects wireless client devices to each other 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.

Flooding: An attack in which an attacker sends large numbers of wireless messages at a high rate to prevent the wireless network from processing legitimate traffic.

Infrared (IR): An invisible band of radiation at the lower end of the electromagnetic spectrum. It starts at the middle of the microwave spectrum and extends to the beginning of visible light. Infrared transmission requires an unobstructed line of sight between transmitter and receiver.

Infrastructure Network: A wireless network that requires the use of an infrastructure device, such as an access point or a base station, to facilitate communication between client devices.

Jamming: A device emitting electromagnetic energy on a wireless network's frequency to make it unusable.

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 Bridge: A device that links two wired networks, generally operating at two different physical locations, through wireless communications.

Wireless Local Area Network (WLAN): A group of wireless AP 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.

APPL-1038
APPLE INC./Page 37 of 43

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.

ACO	Authenticated Cipher Offset
AFH	Adaptive Frequency Hopping
AP	Access Point
dBm	Decibels referenced to one milliwatt
DISA	Defense Information Systems Agency
DoD	Department of Defense
ECDH	Elliptic Curve Diffie Hellman
EDR	Enhanced Data Rate
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
GHz	Gigahertz
HCI	Host Controller Interface
IBC	Iterated Block Ciphers
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Infrared
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
LFSR	Linear Feedback Shift Register
LMP	Link Manager Protocol
MAC	Medium Access Control
Mbps	Megabits per second
MITM	Man-in-the-Middle
mW	Milliwatt
NFC	Near Field Communication
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OOB	Out of Band

P2P	Peer to Peer
PC	Personal Computer
PDA	Personal Digital Assistant
PHY	Physical Layer
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RF	Radio Frequency
RNG	Random Number Generator
RSSI	Received Signal Strength Indication
SAFER	Secure And Fast Encryption Routine
SDP	Service Discovery Protocol
SIG	Special Interest Group
SP	Special Publication
SRES	Signed Response
SSP	Secure Simple Pairing
TDM	Time Division Multiplexing
USB	Universal Serial Bus
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Networks

APPL-1038
APPLE INC./Page 40 of 43

Appendix C—References

The list below provides references for the publication.

Bluetooth Special Interest Group, Bluetooth 2.0 and 2.1 specifications, http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/

Bluetooth Special Interest Group, "Bluetooth Security White Paper", May 2002, http://www.bluetooth.com/NR/rdonlyres/E870794C-2788-49BF-96D3-C9578E0AE21D/0/security_whitepaper_v1.pdf

Bluetooth Special Interest Group, "Simple Pairing Whitepaper", August 2006, http://bluetooth.com/NR/rdonlyres/0A0B3F36-D15F-4470-85A6-F2CCFA26F70F/0/SimplePairing_WP_V10r00.pdf

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

Defense Information Systems Agency (DISA), "DoD Bluetooth Headset Security Requirements Matrix", Version 2.0, 07 April 2008, http://iase.disa.mil/stigs/checklist/dod_bluetooth_headset_security_requirements_matrix_v2-0_7april2008.pdf

Defense Information Systems Agency (DISA), "DoD Bluetooth Smart Card Reader Security Requirements Matrix", Version 2.0, 01 June 2007, http://iase.disa.mil/stigs/checklist/DoD-Bluetooth-Smart-Card-Reader-Security-Requirements-Matrix.pdf

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

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

APPL-1038
APPLE INC./Page 41 of 43

Appendix D—Online Resources

The lists below provide examples of online resources related to Bluetooth technologies and wireless network security that may be helpful to readers.

Documents

Name	URL
Bluetooth SIG Specifications	http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/
DoD Bluetooth Headset Security Requirements Matrix (Version 2.0, 07 April 2008)	http://iase.disa.mil/stigs/checklist/dod_bluetooth_headset_security_requirements_matrix_v2-0_7april2008.pdf
DoD Bluetooth Smart Card Reader Security Requirements Matrix (Version 2.0, 01 June 2007)	http://iase.disa.mil/stigs/checklist/DoD-Bluetooth-Smart-Card-Reader-Security-Requirements-Matrix.pdf
FIPS 140-2, *Security Requirements for Cryptographic Modules*	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
FIPS 180-2, *Secure Hash Standard (SHS)*	http://csrc.nist.gov/publications/fips/fips180-2/fips180-2withchangenotice.pdf
FIPS 197, *Advanced Encryption Standard*	http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
GAO-05-383, *Information Security: Federal Agencies Need to Improve Controls over Wireless Networks*	http://www.gao.gov/new.items/d05383.pdf
GRS 24, *Information Technology Operations and Management Records*	http://www.archives.gov/records-mgmt/ardor/grs24.html
NIST SP 800-30, *Risk Management Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
NIST SP 800-32, *Introduction to Public Key Technology and the Federal PKI Infrastructure*	http://csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf
NIST SP 800-48 Revision 1, *Guide to Securing Legacy IEEE 802.11 Wireless Networks*	http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf
NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
NIST SP 800-53 Revision 2, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf
NIST SP 800-63, *Electronic Authentication Guideline*	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
NIST SP 800-63-1 (Draft), *Electronic Authentication Guideline*	http://csrc.nist.gov/publications/PubsSPs.html
NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle*	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf
NIST SP 800-70, *Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers*	http://checklists.nist.gov/docs/SP_800-70_20050526.pdf
NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*	http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf
NIST SP 800-114, *User's Guide to Securing External Devices for Telework and Remote Access*	http://csrc.nist.gov/publications/nistpubs/800-114/SP800-114.pdf

Resource Sites

Name	URL
Bluetooth Special Interest Group	http://www.bluetooth.com/ http://www.bluetooth.org/
Cellular Telecommunications and Internet Association (CTIA)	http://www.ctia.org/
Federal Communications Commission	http://www.fcc.gov/
FIPS-Validated Cryptographic Modules	http://csrc.nist.gov/groups/STM/index.html
IEEE 802.15 Working Group for Wireless Personal Area Networks	http://www.ieee802.org/15/
NIST National Vulnerability Database (NVD)	http://nvd.nist.gov/
NIST's National Checklist Program	http://checklists.nist.gov/
Trifinite Group (Bluetooth Security Research)	http://www.trifinite.org/
Wireless Vulnerabilities and Exploits	http://www.wirelessve.org/