DHS 4300A Sensitive Systems Handbook

Attachment Q6

To Handbook v11.0

Bluetooth Security

Version 11.0

December 22, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
11.0	December 15, 2014	Initial version.

CONTENTS

1.0 INTRODUCTION

This document provides techniques and procedures for securely implementing Bluetooth enabled devices and peripherals in the Department of Homeland Security (DHS). The intent is to assure a minimum-security baseline when installing, configuring, using, and managing Bluetooth-capable devices. In mitigating risks posed by the use of Bluetooth enabled devices, the approach should be holistic; security controls for the host environment and Bluetooth device work together to reduce the risk of loss of confidentiality, availability, integrity, and non-repudiation.

1.1 Authority

This document is issued as implementation guidance under the authority of the DHS Chief Information Officer (CIO) through the DHS Office of the Chief Information Security Officer (OCISO).

1.2 Purpose and Scope

This document addresses the security specifics of sensitive wireless systems only and does not cover the use of classified wireless systems. DHS Sensitive Systems Policy Directive 4300A prohibits use of wireless communications technologies throughout DHS unless the appropriate Authorizing Official (AO) specifically approves the technology and the application. AOs must also approve the implementation and use of wireless systems at a specified risk level during the security authorization process and ensure appropriate and effective security measures are included in the Security Plan. This document sets forth acceptably secure configurations and applications of Bluetooth wireless communications that offer mechanisms and conditions under which AOs can approve limited Bluetooth use, and associated risk level specifications.

1.3 Background

Bluetooth is a wireless open standard technology used for exchanging voice or data over short distances between devices without interconnecting cables. Effective range varies and depends on propagation conditions, material coverage, antenna configuration, battery condition, etc., but most Bluetooth devices have an effective range of 10m (33 ft.) or less. The technology has been integrated into many types of devices including cell phones, laptops, printers, keyboards, mice, and headsets, and is used primarily to establish ad hoc wireless personal area networks (WPANs) – also known as *piconets* – between devices (for example, a connection between a cell phone and a headset), as shown in Figure 1.

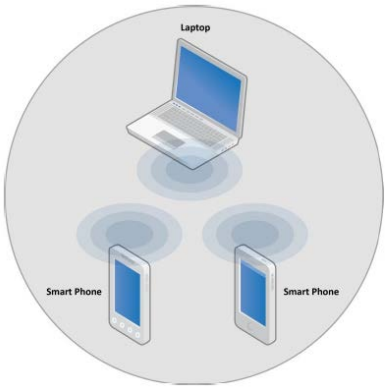

Figure 1: Ad hoc *Bluetooth network*

Bluetooth versions 1.1 and 1.2 only support transmission speeds up to 1 megabit per second (Mbps), known as Basic Rate (BR), and can achieve payload throughput of approximately 720 kilobits per second (kbps). Enhanced Data Rate (EDR), introduced in version 2.0, specifies data rates up to 3 Mbps and throughput of approximately 2.1 Mbps.

Devices connect under a master-slave structure, a model of communication where the master device or process has unidirectional control over one or more other devices. A master Bluetooth device, such as a smartphone or tablet, may communicate with up to seven (7) devices in a piconet, (e.g. other smartphones, headsets, keyboards, printers, etc.), although not all devices reach this maximum. In some cases the devices may switch roles, and a slave become the master (for example, a headset initiating a connection to a phone may initially serve as master, as initiator of the connection; but may later prefer to be slave once the connection is established).

The Bluetooth Core Specification provides for connection of two or more piconets to form a *scatternet* in which certain devices simultaneously function as master in one piconet and as slave in another.

Except in the seldom used broadcast mode, data is being transferred between two devices. The master selects which slave to address, typically switching rapidly from one device to another in a round-robin fashion.

1.4 Homeland Security Mission-Driven Use Cases

The following are examples in which use of Bluetooth technology could enhance the ability of Department personnel to fulfill their mission and business requirements. Examples are based on mission-driven use cases; the list is not exhaustive.

- Bluetooth keyboard for tablets in office environments (data)
- Officer earpieces enabling hands free inspections, protective details, border security missions (voice)
- Bluetooth headset for office workers (voice)
- Bluetooth PIV card readers (data)
- Hands free mobile phone use in a vehicle (voice)
- Field operations in degraded or failed communications infrastructure (voice and data)

- Transfer of data between a mobile device and a base unit at an inspection point (data)
- Collection of fingerprints from suspects or persons of interest encountered in the field during law enforcement encounters or investigations (data – PII)

2.0 REQUIREMENTS OF DHS POLICY DIRECTIVE 4300A

Wireless systems include wireless local area networks (WLAN), wireless wide area networks (WWAN), wireless personal area networks (WPAN) such as Bluetooth, peer-to-peer wireless networks (i.e., ad hoc wireless networks), and systems that leverage commercial wireless services. Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols. *DHS Sensitive Systems Policy Directive 4300A* establishes the Department's wireless systems policies. System owners should submit the documentation required by policy to the appropriate AO.

3.0 BLUETOOTH THREATS AND VULNERABILITIES

Bluetooth has clear ease of use advantages compared to cabled devices and peripherals, but like any wireless technology, Bluetooth communications are susceptible to a variety of threats. The technology has been fielded using a wide variety of chipsets, operating systems, and physical device configurations resulting in a large number of differing security programming interfaces and default settings. These complexities, added to those of wireless communications in general, mean that Bluetooth is susceptible to general wireless threats as well as having its own inherent vulnerabilities. Bluetooth is a peer-to-peer network technology that lacks a centralized security enforcement infrastructure. The Bluetooth specification is very complex and includes support for many voice and data services such as headset, data transfer, printing, and others. Common attacks include:

- Bluebugging – Attacker takes control of phone; can make and take calls, listen to phone conversations, read contacts and calendars
- Bluejacking – Sends anonymous, unsolicited messages to phones with Bluetooth set to discoverable
- Blueprinting – A method to remotely fingerprint Bluetooth-enabled devices
- BlueSmack – Performs a denial of service attack over the Bluetooth connection making the device unavailable
- Bluesnarfing– Gives attacker full access to calendar, contacts, e-mail and text messages
- BlueStumbling – Allows an adversary to locate and identify users based on their Bluetooth device addresses

4.0 BLUETOOTH SECURITY MODES

The Bluetooth specification includes four security modes; this section provides an overview and application for each. Security Mode 3 provides the best security.

4.1 Security Mode 1

Security Mode 1 devices are not considered to be secure. Security functionality (authentication and encryption) is never initiated; therefore the device and connections are susceptible to attack. In effect,

Bluetooth devices in this mode are "indiscriminate" and do not employ any mechanisms to prevent other Bluetooth-enabled devices from establishing connections. If a remote device initiates pairing, authentication, or encryption request, a Security Mode 1 device will accept without authenticating the request. Per their respective Bluetooth specification versions, all v2.0 and earlier devices can support Security Mode 1, and v2.1 and later devices can use Security Mode 1 for backward compatibility with older devices. Because of its high vulnerability, Security Mode 1 shall not be used by DHS.

4.2 Security Mode 2

Security Mode 2 is service level enforced in which security procedures may be initiated after link establishment but before logical channel establishment. In this security mode, a local security manager (specified in the Bluetooth architecture) controls access to specific services. Access control, and interfaces with other protocols and device users, are maintained by a separate centralized security manager. 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). All other Bluetooth services, however, 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 in the following section. All v2.0 and earlier devices can support Security Mode 2, but v2.1 and later devices can only support backward compatibility with v2.0 or earlier devices.

4.3 Security Mode 3

Security Mode 3 provides the best security. It is the link level enforced security mode, in which a Bluetooth device initiates security procedures before the link is fully established. Bluetooth devices operating in Security Mode 3 mandate authentication and encryption for all connections to and from the device. Therefore, not even service discovery can be performed before authentication, encryption, and authorization have been performed. A service level authorization is not typically performed by a Security Mode 3 device once the device has been authenticated. Service-level authorization should be performed to prevent "authentication abuse," where an authenticated remote device uses a Bluetooth service without the local device owner's knowledge. All v2.0 and earlier devices can support Security Mode 3, but v2.1 and later devices can only backward compatibility with v2.0 and later devices.

4.4 Security Mode 4

Security Mode 4 uses Secure Simple Pairing (SSP), in which Elliptic Curve Diffie-Hellman (ECDH) key agreement replaces legacy key agreement for link key generation. Device authentication and encryption algorithms, however, 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
- No security required

Whether or not a link key is authenticated depends on the SSP association model used. Security Mode 4 requires encryption for all services except Service Discovery and is mandatory for communication between v2.1 and later BR/EDR devices. However, for backward compatibility, a Security Mode 4 device can fall back to any of the other three Security Modes when communicating with Bluetooth v2.0 and earlier devices that do not support Security Mode 4. In order to minimize risks, Security Mode 4 devices shall be configured so as not to allow paring with Security Mode 1 or Security Mode 2 devices.

5.0 BLUETOOTH DEVICE COMMUNICATION RISKS AND RECOMMENDATIONS

During and after Bluetooth device pairing, critical information is passed between devices. If captured, this critical information could allow an attacker to gain full remote access to the WPAN device. For more information on Bluetooth security see NIST SP 800-121, *Guide for Bluetooth Security*.

As technology advances, so do attack vectors and methodologies. In order to reduce the risk of data compromise, the following are best practices to employ:

5.1 Management Best Practices

- Ensure that Bluetooth users are made aware of their security-related responsibilities regarding Bluetooth use and provide them with a list of precautionary measures to better protect handheld Bluetooth devices from theft.
- Enable Bluetooth only when necessary (e.g. turn off Bluetooth on the mobile device and turn off the headset when not in use).
- Minimize distance between Bluetooth linked devices when Bluetooth links are active.
- Minimize the duration of voice calls
- Minimize opportunity for signal interception. Maximize the distance from other Bluetooth devices, other people, and untrusted areas.
- When pairing, the mobile device will attempt to find other Bluetooth-enabled devices. Always verify and confirm the device being paired. Never enter passkeys when unexpectedly prompted for them.
- Remove lost, stolen or unused devices from paired device list.
- Perform comprehensive security assessments at regular intervals to fully understand the Bluetooth security posture.
- Ensure that wireless devices and networks involving Bluetooth technology are fully understood from an architecture perspective and documented accordingly.
- Maintain a complete inventory of all Bluetooth-enabled devices and addresses.
- Designate an individual to track the progress of Bluetooth security products and standards and the threats and vulnerabilities with the technology.

5.2 Technical Best Practices

- Change the default settings of the Bluetooth device.
- Set Bluetooth power to the lowest available setting in order to reduce signal range whenever practicable. The lowest Bluetooth power should be employed that is sufficient to maintain communications between authorized users.
- 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.
- Ensure that link keys are not based on unit keys. The use of shared unit keys can lead to successful spoofing, "Man in the Middle" (MITM), and eavesdropping attacks.
- 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.
- Use random and unique passkeys 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.
- A Bluetooth device using Security Mode 4 must fall back to Security Mode 3 for backward compatibility with v2.0 and earlier devices (i.e., for devices that do not support Security Mode 4). The Bluetooth specifications allow a v2.1 device to fall back to any Security Mode for backward compatibility. This allows the option of falling back to Security Modes 1- 3. Security Mode 3 provides the best security.
- Lock down the Bluetooth stack on every device to ensure that only required and approved profiles and services are available for use. Many Bluetooth stacks are designed to support multiple profiles and associated services. Disable unneeded and unapproved services.
- Configure Bluetooth devices by default as undiscoverable and to remain undiscoverable except as needed for pairing. This prevents visibility to other Bluetooth devices except when discovery is absolutely required. The default Bluetooth device names sent during discovery should be changed to non-identifying values.
- Invoke link encryption for all Bluetooth connections, and use it to secure all data transmissions during Bluetooth connections; otherwise, transmitted data is vulnerable to eavesdropping.
- 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 compromise of the entire communication chain.
- Ensure that mutual device authentication is performed for all connections. Mutual authentication is required to provide verification that all devices on the network are legitimate.
- 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 interception for malicious purposes.

- Configure encryption key sizes to the maximum allowable (128-bit). Using maximum allowable key sizes provides protection from brute force attacks.
- Use additional 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. Employing higher layer encryption (particularly FIPS 140 validated) over the native encryption will further protect the data in transit.

5.3 Operational and Deployment Best Practices

- Ensure that Bluetooth capabilities are disabled when they are not in use. Bluetooth capabilities should be disabled on all 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 turned off when not in use.
- Perform pairing as infrequently as possible, ideally in a secure area where attackers cannot realistically observe the passkey entry or intercept Bluetooth pairing messages. 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.
- A Basic Rate/Enhanced Data Rate (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 the best security.
- Ensure that portable devices with Bluetooth interfaces are configured with a password or access PIN enabled. This helps prevent unauthorized access if the device is lost or stolen.
- If a Bluetooth device is lost or stolen, users should immediately delete the missing device from the paired device lists of all other Bluetooth devices.
- Install antivirus software on Bluetooth-enabled hosts that support such host-based security software.
- Fully test and regularly deploy Bluetooth software and firmware patches and upgrades.
- Do not accept transmissions of any kind from unknown or suspicious devices. These types of transmissions often include messages, files, and images.
- Fully understand the impacts of deploying any security feature or product prior to deployment.

6.0 COMPLIANT BLUETOOTH PRODUCT LISTS

GSA operates and maintains the Federal Information Processing Standard 201 [FIPS 201] Evaluation Program (EP) and its Approved Products List [APL], as well as services for Federal Identity, Credentialing and Access Management (FICAM) segment architecture conformance and compliance. As part of the FICAM Testing Program, GSA manages the Approved Products List (APL). This list provides Federal agencies with the products and services related to ICAM implementation that have

been approved based on testing done by the FICAM Testing Program. This list includes Bluetooth Fingerprint Scanner, Bluetooth Smart Card Reader.