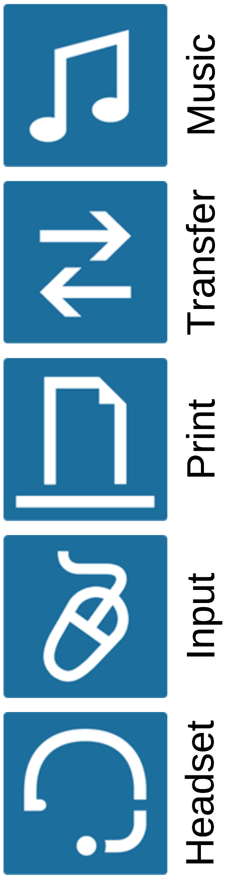
Systems and Network Analysis Center
Information Assurance Directorate

Bluetooth Security



Bluetooth is a short-range, low-power wireless technology commonly integrated into portable computing and communication devices and peripherals. Like any wireless technology, Bluetooth introduces a number of potentially serious security vulnerabilities. These vulnerabilities may lead to the compromise of the device and those networks to which it connects. Proper use of standard Bluetooth security features, however, should provide adequate security for many unclassified applications. Detailed recommendations for using Bluetooth safely are provided at the end of this document.

Bluetooth Security Mechanisms

Bluetooth links use optional pre-shared key authentication and encryption algorithms that are widely considered acceptably strong when both implemented and used correctly. The strength of Bluetooth security relies primarily on the length and randomness of the passkey used for Bluetooth pairing, during which devices mutually authenticate each other for the first time and set up a link key for later authentication and encryption. Also important for overall Bluetooth security are discoverability and connectability settings. These settings control whether remote Bluetooth devices are able to find and connect to a local Bluetooth device. Optional user authorization for incoming connection requests provides additional security.

Bluetooth Vulnerabilities

Bluetooth is by design a peer-to-peer network technology and typically lacks centralized administration and security enforcement infrastructure. The Bluetooth specification is very complex and includes support for over two dozen diverse voice and data “profiles” or services. Some of these include headset, cordless telephony, file transfer, dial-up networking, printing, and serial port profiles. In addition, designers have implemented Bluetooth using a wide variety of chipsets, devices, and operating systems. This variety in foundational elements results in user interfaces, security programming interfaces, and default settings that also vary widely. Because of these complexities, Bluetooth is particularly susceptible to a diverse set of security vulnerabilities. Publicly documented Bluetooth attacks involve identity detection, location tracking, denial of service, unintended control and access of data and voice channels, and unauthorized device control and data access. As an example, researchers have shown that Bluetooth headset use can compromise devices in multiple ways. This compromise is due to the headset profiles' support for powerful telephony signaling commands and the all too common use of weak fixed passkeys (typically “0000”).

The website http://www.bluetooth.com/Bluetooth/Learn/Security contains a general discussion of Bluetooth security and vulnerabilities, and http://www.trifinite.org contains detailed descriptions of Bluetooth attacks along with downloadable audit and demonstration software. While the proper use of existing Bluetooth security mechanisms can reduce Bluetooth security risks to a level acceptable for unclassified use, SNAC research will continue into Bluetooth vulnerabilities and secure Bluetooth design for use in sensitive and classified security domains.

Bluetooth Use in the Department of Defense

As a result of comprehensive security evaluations conducted by the SNAC, and in close partnership with vendors, the Defense Information Systems Agency (DISA) has begun approving the unclassified use of Bluetooth Common Access Card (CAC) readers with BlackBerry, Windows Mobile, and Windows XP Service Pack 2 devices. The SNAC develops stringent security requirements for DoD Bluetooth use and verifies the secure implementation of each approved solution. DISA then publishes security requirements and recommended configuration guidance in matrices and checklists at http://iase.disa.mil/stigs/checklist. Standard commercial Bluetooth headsets remain prohibited in the DoD for the reasons listed above.

Bluetooth Security Recommendations & Precautions

Both users and Bluetooth application developers have responsibilities and opportunities to minimize the risk of compromise via Bluetooth. Users should follow these best practice security guidelines:

- Never use standard commercial Bluetooth headsets.
- Enable Bluetooth functionality only when necessary.
- Require and use only devices with low-power Class 2 or 3 Bluetooth transceivers.
- Keep devices as close together as possible when Bluetooth links are active.
- Independently monitor devices and links for unauthorized Bluetooth activity.
- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.
- Use device firewalls, regularly patch Bluetooth devices, and keep device anti-virus software up to date.
- Comply with all applicable directives, policies, regulations, and guidance.
- Subject Bluetooth solutions and deployments to independent security audits by qualified evaluators.

Bluetooth application developers should consider designing to the following guidelines:

- Eliminate or disable support for the Headset and Hands-Free Profiles unless such links are adequately secured using the techniques described.
- Passkeys should be at least eight digits long. Passkeys must not be valid indefinitely.
- Use configuration and link activity indicators like LEDs or desktop icons.
- Use non-descriptive Bluetooth device names on each device and identify all paired and connected Bluetooth devices by hardware (MAC) address.
- Require user authorization for all incoming connection requests, and don’t accept connections, files, or other objects from unknown, untrusted sources.
- Program each device to initiate Bluetooth authentication immediately after the initial establishment of the Bluetooth connection (also known as Security Mode 3, Link Level security).
- Program each device to initiate 128-bit Bluetooth encryption immediately after mutual authentication. Layer FIPS-certified cryptography atop Bluetooth cryptography for defense in depth.
- Store link keys securely and regularly change link keys under encryption.
- Remove the user's ability to control Bluetooth settings that could possibly circumvent security features.
- Enable each Bluetooth service only when needed. Permanently remove, or disable, all unnecessary Bluetooth services.
- Digitally sign all Bluetooth firmware, driver, and application software. Verify that no unauthorized software applications use Bluetooth application programming interfaces.
- Prohibit the user from changing or controlling Bluetooth security features.