11.1. Bluetooth Communications

Objective

11.1.1. Bluetooth is used securely and Bluetooth communications are protected.

Context

11.1.2. Bluetooth radios are commonly found in end user devices, including laptops, mobile phones, and peripherals such as speakers, headphones, keyboards, and mice. More recently Bluetooth has been integrated into medical devices and personal devices.

11.1.3. It is important to be aware of all risks associated with Bluetooth technology. The specific threats to Bluetooth communications, that the controls in this section address, relate to are:

- eavesdropping on the Bluetooth communications between paired devices, and
- connection interception attacks that leverage the network communications channel (including during establishment) of Bluetooth devices.

Background

11.1.4. The Bluetooth specification has evolved over time and is regularly updated. Version 4.0 of the specification introduced Bluetooth Low Energy (LE) which offers a different feature set than the original Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) standard. Version 4.1 and 4.2 of the specification introduced enhanced security features for Bluetooth BR/EDR and LE respectively.

11.1.5. Determining the security level being provided depends on several factors, including the capabilities and Bluetooth version supported by the devices being paired together. The actual security provided between devices is a combination of:

a. the version of the Bluetooth specification supported by each device,

b. the capabilities of the devices to accept user input (eg, through a keyboard, or camera) and to display output (eg, through a screen or character display), and

c. whether the devices are using Bluetooth BR/EDR or Bluetooth LE.

11.1.6. The following table summarises the security protections expected based on the pairing Bluetooth device capabilities where devices are Bluetooth BR/EDR using Secure Connections (version 4.1 or later) or Bluetooth LE using Secure Connections (version 4.2 or later) – refer to NIST SP 800-121 REV.2 Guide to Bluetooth.

Display or input capabilities of the devices	Association mode used	Protected against connection interception	Protected against eavesdropping
Both devices can display and accept input	Numeric Comparison	Yes	Yes
One device has input, one has display	Passkey Entry	Yes	Yes
At least one device has no display or input	Just Works	No	Yes
External channel for matching devices (eg, QR codes or NFC)	Out of Band	Yes	Yes

11.1.7. Particular care is required when associating Bluetooth devices using the Just Works association mode (eg, with headsets) due to the risk of the pairing connection being intercepted, and encryption keys being discovered.

11.1.8. Since Bluetooth LE v4.2, released in 2014, versions of the Bluetooth protocol have included more advanced security features including authentication, authorisation, and encryption through the Secure Connections functionality. Encryption protocols are used to protect data from interception and authentication protocols ensure that only authorised devices can connect.

11.1.9. The table below displays the key differences between Bluetooth Basic Rate/Enhanced Data Rate (BR/EDR) and Bluetooth Low Energy (LE).

Characteristic	Bluetooth BR/EDR		Bluetooth Low Energy	
	Prior to 4.1	4.1 onwards	Prior to 4.2	4.2 onwards
RF Physical Channels	79 channels with 1 MHz channel spacing		40 channels with 2 MHz channel spacing	
Discovery / Connect	Inquiry / Paging		Advertising	
Number of Piconet Slaves	7 (active) / 3255 (total)		Unlimited	
Device Address Privacy	None		Private device addressing available	
Max Data Rate	1-3 Mbps		1 Mbps via GFSK modulation	
Pairing Algorithm	Prior to 2.1: E21/E22/SAFER+	P-256 Elliptic Curve, HMAC-SHA-256	AES-128	P-256 Elliptic Curve, AES-CMAC
	2.1-4.0:P-192 Elliptic Curve[9] HMAC-SHA-256			
Device Authentication Algorithm	E1/SAFER	HMAC-SHA-256	AES-CCM[10]	
Encryption Algorithm	E0/SAFER+	AES-CCM	AES-CCM	
Typical Range	30m		50m	
Max Output Power	100mW (20 dBm)		10mW (10 dBm)[11]	

Reference: NIST SP 800-121 REV.2 Guide to Bluetooth Table2-2

11.1.10. 5.x Bluetooth versions have introduced faster data transfers, larger data capacity, greater range and optimised power consumption.

Threats

General wireless networking threats

11.1.11. Bluetooth is susceptible to general wireless networking threats such as:

- **denial-of-service (DoS) attacks:** is a malicious attempt to overwhelm an online service or network and render it unusable
- **eavesdropping;** occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices.
- **adversary in the middle attacks:** a threat actor puts themselves in the middle of two parties to intercept data & use it for malicious purposes
- **message modification:** an intruder alters packet header addresses to direct a message to a different destination or to modify the data on a target machine.
- **resource misappropriation:** is an attack in which the attacker steals or makes unauthorised use of a service.

Bluetooth specific threats

11.1.12. **Connection Interception Attacks**

Bluetooth connections can be intercepted by a hacker who poses as a legitimate device to gain access to sensitive information.

- **Bluesnarfing:** is a hacking technique in which a hacker accesses a wireless device through a Bluetooth connection. It happens without the device user's permission and often results in the theft of information or some other kind of damage to the device (and user).
- **Bluebugging:** is a hacking technique that lets someone get into your device through your discoverable Bluetooth connection.
- **Bluejacking:** is a Bluetooth attack in which a hacker spams your device with unsolicited phishing messages.
- **Car Whisperer:** is a hacking technique that can be used by attackers to hack a hands-free Bluetooth in-car system.
- **Fuzzing Attacks:** consist of sending malformed or otherwise non-standard data to a device's Bluetooth radio and observing how the device reacts.

11.1.13. **Eavesdropping attacks**

When eavesdropping takes place on the Bluetooth communications between paired devices

- **Pairing Eavesdropping:** is an attack where Bluetooth devices are forced to re-pair in the open and this allow the pairing process to be eavesdropped.
- **Secure Simple Pairing Attacks:** During the Bluetooth pairing process, an attacker with physical proximity can gain unauthorised access via an adjacent network, and intercept traffic and send forged pairing messages between two vulnerable Bluetooth devices.

References

11.1.14. References are available at the following source:

Reference	Publisher	Title
NIST 800-121, Rev.2, May 2017 **(INCLUDES UPDATES AS OF 1-19-2022)**	NIST	Guide to Bluetooth Security (nist.gov)

Rationale & Controls

Bluetooth within agency environments

11.1.15.R.01. **Rationale**

Bluetooth provides a convenient method of wirelessly connecting devices and includes support for a wide variety of usage scenarios.

11.1.15.R.02. **Rationale**

Bluetooth is commonly found in low powered consumer devices, medical devices, and peripherals. Bluetooth operates in the same 2.4GHz wireless band as other non-licenced spectrum services such as Wi-Fi.

11.1.15.R.03. **Rationale**

Bluetooth is generally suitable for connectivity between devices in lower classification settings, and where adequate consideration is given to the purpose of the connection, the type of information being transmitted, the security capabilities of the devices, and the environment the devices are operating in.

11.1.15.R.04. **Rationale**

Given the large number of potential situations Bluetooth could be used in, it is essential that agencies develop a considered position on where and where not to permit the use of Bluetooth connections.

11.1.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7524]

Agencies wishing to permit the use of Bluetooth MUST develop a policy that details the circumstances under which Bluetooth usage is permitted, and situations where it is not to be used.

11.1.15.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7525]

The policy position MUST include information about Bluetooth security controls that are to be used, and methods for verifying that the controls are in place and are effective.

Bluetooth connections

11.1.16.R.01. **Rationale**

Bluetooth connections between devices of different security protocol levels will result in a degradation of the security level.

11.1.16.R.02. **Rationale**

Bluetooth connections between devices that can revert to weaker protocol options, and that do not support effective security features will increase risk of compromise.

11.1.16.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7526]

Agencies MUST ensure that Bluetooth pairing is only established between authorised devices. (Unless a gateway is being used, paired devices are considered to operate at the same security classification level).

11.1.16.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7527]

Agencies SHOULD ensure that Bluetooth discovery of devices is disabled unless a new pairing connection is being established.

11.1.16.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7528]

Agencies SHOULD ensure that Bluetooth device pairing only occurs at a location where only authorised persons have access.

11.1.16.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7529]

Agencies SHOULD ensure that Bluetooth pairings are removed when they are no longer required.

Bluetooth versions

11.1.17.R.01. **Rationale**

It is difficult to determine what Bluetooth security features are being used for a connection between devices without capturing and decoding the connection establishment packets.

Since Bluetooth LE v4.2, versions of the Bluetooth protocol have included more advanced security features including authentication, authorisation, and encryption through the Secure Connections functionality.

11.1.17.R.02. **Rationale**

Ensuring some end-user visible features are being used during the device pairing process can provide a level of understanding of the security between Bluetooth connected devices.

11.1.17.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:7530]

Agencies using Bluetooth MUST use the most secure configuration supported by the paired devices.

11.1.17.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7531]

Agencies SHOULD identify the:

- Bluetooth type (BR/EDR or LE),
- version, and
- security capabilities;

for devices used to form Bluetooth connections, and ensure they are used to inform risk decisions on the use of Bluetooth.

11.1.17.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:7532]

Agencies SHOULD ensure that new Bluetooth connections between devices are authenticated using explicit user actions, such as entry of a numeric code, confirmation of a matching PIN, or other affirming action, such as challenge-response process.

Encryption and authentication protocols

11.1.18.R.01. **Rationale**

When transferring information between Bluetooth devices, encryption protocols are used to protect data from interception and authentication protocols ensure that only authorised devices can connect.

11.1.18.R.02. **Rationale**

Chapter 17 of the NZISM provides approved encryption algorithms. Even in the most secure operating model, Bluetooth specifications are currently unable to support these approved encryption methods. Whilst Bluetooth cannot meet these requirements, there may be organisational requirements to use Bluetooth to transfer Restricted or Sensitive information between devices.

11.1.18.C.01. **Control System Classifications(s): Unclassified/In-Confidence; Compliance: Should** [CID:7533]

Agencies using Bluetooth between devices to transfer UNCLASSIFIED or IN-CONFIDENCE information SHOULD ensure that connections meet NZISM standards for authentication and use Approved Cryptographic Algorithms for encryption and message integrity.

11.1.18.C.02. **Control System Classifications(s): Restricted/Sensitive; Compliance: Must** [CID:7534]

Agencies using Bluetooth between devices to transfer RESTRICTED or SENSITIVE information MUST ensure that connections meet NZISM standards for authentication and use Approved Cryptographic Algorithms for encryption and message integrity.

11.1.18.C.03. **Control System Classifications(s): Restricted/Sensitive; Compliance: Must** [CID:7535]

If Bluetooth specifications do not support these approved encryption methods, organisations MUST do a risk assessment and use the exception or waiver process to accept this risk.

Bluetooth in secure areas

11.1.19.R.01. **Rationale**

As with other wireless protocols, the level of security offered by Bluetooth can vary widely depending on the capabilities of the devices being connected.

11.1.19.R.02. **Rationale**

Bluetooth devices will revert to older, less secure versions of the protocol to maintain compatibility, so careful consideration needs to be undertaken before approving the use of the Bluetooth protocol.

11.1.19.C.01. **Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must** [CID:2492]

Agencies MUST complete a technical evaluation of the secure area, consult the relevant technical authority and seek approval from the Accreditation Authority before permitting the use of Bluetooth devices.

11.1.19.C.02.

Control System Classifications(s): Confidential, Top Secret, Secret; Compliance: Must Not [CID:2494]

Agencies using Bluetooth devices MUST NOT allow:

- line of sight and reflected communications travelling into an unsecure area.
- multiple Bluetooth devices at different classifications in the same area.

11.1.19.C.03. **Control System Classifications(s): Top Secret, Confidential, Secret; Compliance: Must Not [CID:2495]**

Agencies MUST NOT allow Bluetooth devices into secure areas unless authorised by the Accreditation Authority.