CYBER GUIDELINE DOCUMENT

NCSP Bluetooth Guideline

ABSTRACT:
This guidance provides policing and law enforcement organisations with relevant information regarding risks associated with deploying Bluetooth technology within the workplace, and to enhance the risk-based decisions required in the use of such technology.

ISSUED	April 2024
PLANNED REVIEW DATE	March 2025
DISTRIBUTION	Community Security Policy Framework Members

POLICY VALIDITY STATEMENT
This guideline is due for review on the date shown above. After this date, this document may become invalid.

Cyber guideline users should ensure that they are consulting the currently valid version of the documentation.

CONTENTS

Community Security Policy Commitment

National Policing and its community members recognise that threats to policing information assets present significant risk to policing operations. National Policing and its community members are committed to managing information security and risk and maintaining an appropriate response to current and emerging threats, as an enabling mechanism for policing to achieve its operational objectives whilst preserving life, property, and civil liberties.

This guideline, in conjunction with the National Policing Community Security Policy Framework and associated documents, sets out National Policing requirements.

Introduction

Bluetooth technology is an integral part of our lives, and a highly adaptable means to aid data transit and delivery. More and more people have access to, and use of, technology assets equipped with Bluetooth. These include (but not limited to) laptops, mobile devices, printers, keyboards, and headsets.

Today's devices tend to have fewer USB ports and, instead, rely on wireless communication technology to provide connectivity to peripherals such as a wireless mouse, keyboard, headset, or vehicular-based wireless hands-free kits.

It is important, therefore, that users are educated on the security risks posed through connecting peripheral devices and that, at an organisational level, technical controls are applied to restrict or disable access from these devices if not required.

This guidance document aims to provide important information to assist law enforcement agencies to make informed decisions about using Bluetooth technology in their operations. By taking a cautious approach and implementing appropriate security measures, organisations can ensure a secure and safe use of Bluetooth enabled devices.

Owner

National Chief Information Security Officer (NCISO).

Purpose

The purpose of this guidance document is to provide policing and law enforcement organisations with relevant information regarding risks associated with deploying Bluetooth technology within the workplace, and to enhance the risk-based decisions required in the use of such technology.

The purpose of this guidance is to:

- Provide relevant information regarding Bluetooth technology
- Empower organisations to conduct suitable risk/benefit analysis prior to deployment/use of Bluetooth technology
- Encourage organisations to take a risk-based approach to their selection, deployment and use of Bluetooth technology
- Provide relevant information that allows organisations to manage any risk associated with the deployment and use of Bluetooth technology
- Provide guidance of best practice on selecting, deploying, and managing Bluetooth enabled devices, based on industry standards and best practices.

Audience

All UK Home Office and non-Home Office police forces, including other law enforcement agencies.

This guidance is aimed at:

- Information Security Officers (ISOs), information security practitioners and any roles who plan, undertake and review penetration tests or ITHCs.
- Member Senior Information Risk Owners (SIROs), and Information Asset Owners (IAOs.)
- Third parties who act as service providers or suppliers to members.
- Auditors providing assurance services to members.

Scope

This guidance applies to any member of the Policing Community of Trust. It is also applicable to third parties to the policing community.

When

This guidance should be referred to as part of any decision-making in relation to the selection, procurement, deployment and use of any Bluetooth technology within the law enforcement arena.

Where

The guidance should be referred to for application of Bluetooth technology in any scenario, and it is not geographically restricted.

What

The guidance applies to the use of any Bluetooth technology deployed to send/receive, store, amplify or otherwise process any policing data / data consumed as part of policing and law enforcement business functions. This includes mobile / smart phones, tablets, body worn technology, cameras, recording equipment, navigation aids, in-vehicle technology, smart speakers, device remote controls, drones and any device capable of connecting using Bluetooth.

What is Bluetooth?

Bluetooth is technology that uses a band of radio frequencies to share data over a short distance. The Bluetooth frequency band is available worldwide. The current standard is Bluetooth 5.0, which has a reported typical transmission distance of 40 metres. However, whilst the signal range of this standard is greater than that of previous standards (there are reports of transmission capabilities >100m), it should still be noted that the further devices are from each other, the greater the impact of signal to noise ratio. The lower the ratio, the greater the likelihood of communication loss.

Further reading on this can be found at “Understanding Reliability in Bluetooth® Technology Bluetooth® Technology Website” [1]

Bluetooth can provide easy ways to pair devices for data sharing. This can enable attackers unauthenticated access however, which can lead to data loss or maliciously modifying devices remotely.

[1] See www.bluetooth.com – external site

How secure is Bluetooth?

Due to the short range of transmission, Bluetooth as an attack vector can be less likely, as threat actors are required to be within close proximity to their target.

Whilst the Bluetooth standard has device authentication, it does not include user authentication. This means that when communicating over Bluetooth you should verify the person handling the Bluetooth enabled device.

Bluetooth data transmissions are encrypted. The 5.0 and later standards use Advanced Encryption Standard (AES), which is the current industry standard. However, many devices still use older standards (Bluetooth 4.0 and earlier) with decreasing levels of inbuilt security the lower down the standard that you go. It is important that organisations understand what devices are being deployed (asset tracking), the Bluetooth version (standard) for each device, the application for which the device is being deployed (e.g. in-car hands-free) and the type of data being processed.

Whilst devices may claim full compliance with the Bluetooth standards, hardware or software may be present that increase risks. Official devices must be suitably configured, hardened and managed in line with Force / organisational security policies. Devices are typically backwards compatible which increases risk when using legacy equipment. Configurations should enforce the later versions (v5.0 or later.)

Common Bluetooth Attacks

Basic tools can be used to gather information about devices without any interaction by potential victims. These tools are used to undertake reconnaissance or collect geo-information about premises, people, or operations.

- Bluebugging: is a type of Bluetooth attack where an attacker gains unauthorised access to your device and takes control of it remotely. This can allow the attacker to make calls, send messages or access sensitive data on the device without the owner’s knowledge.
- BlueJacking - When a device leaves its Bluetooth enabled, it can be discovered by threat actors looking for open connections and can receive unwanted messages.
- BlueSnarfing - When a device leaves its Bluetooth enabled, it can receive unsolicited pairing where a threat actor can then retrieve data from the device.
- Denial of service – As with any wireless technology, in the presence of strong signals the reliability of connections can be disrupted or interrupted.
- Car Whisperer - allows an attacker to send to or receive audio from vehicle Bluetooth equipment. An attacker could transmit audio to the car’s speakers or receive audio (eavesdrop.)

Possible Routes to Compromise

Bluetooth is not a typical attack vector. The threat actor must be in close proximity, and the reward of connecting to a phone is fairly low, compared to other police infrastructure. However, particular care and consideration should be given in the deployment of resources to sensitive locations, including:

- Private addresses of principals/police officers & staff/military personnel/gov’t agents and their employees
- Safe havens, e.g. women’s refuges
- Any strategic or tactical location relating to covert, CT or OCG operations.

Due to Bluetooth being used with location finding services, any deployments to sensitive locations must be accompanied by messaging/protocols to ensure Bluetooth is switched off or hidden.

- For higher risk / sensitive areas RF pouches or RF lockers should be used to temporarily store devices

Typical attacks can be conducted with minimal tools and expertise which can lead to data leaks, gathering intelligence about people, devices and locations and unsolicited harmful software being delivered, affecting device integrity. Examples include:

- Identifying people operating out of discrete / covert locations,
- mapping movements of personnel,
- capturing of conversations or keystrokes (including passwords) and
- remotely installing eavesdropping software on mobile phones.

It is also worthy of note that data transfers over Bluetooth may not be visible to Data Loss Prevention / information management tools, thereby providing a route for unauthorised data sharing.

Bluetooth Best Practice

Whilst Bluetooth can provide a neat solution for connecting multiple devices, there are security risks present in the use of this technology. The points below should be considered as best practice and as part of a local risk assessment when deploying Bluetooth based solutions.

Reference	Minimum Requirement	Control Reference
Legitimacy of Use		
CSP-BLU-001	Is Bluetooth required? There are various methods to share data, is Bluetooth the best method/ is it required? If not, then devices should disable Bluetooth or consider low power modes where available.	
CSP-BLU-002	The use of Bluetooth for police issued devices must always be considered in the context of properly configured, organisation managed assets. Poorly configured or unmanaged devices will represent the most vulnerable targets to attacks or compromise.	ID.RA-01 PR.PS-01
CSP-BLU-003	Develop an 'asset tracker' for devices using Bluetooth & review every 6-12 months. Refer to *NCSP Physical Asset Management standard* for further information.	ID.AM-1
Configuration controls		
CSP-BLU-004	Technical policies should be put in place to prevent or control, as well as monitor, data transfer via Bluetooth on corporate devices. This will help to manage risks around Data Loss Prevention. This should include limiting communication to v5.0 or later only.	DE.CM-01
CSP-BLU-005	The NEP Blueprint Volume 5 on Mobility describes device configuration MEM Intune configuration policies which can	PR.PS-01

Reference	Minimum Requirement	Control Reference
	help protect devices, by controlling a multitude of settings and features. For example: • restrict use of hardware features on the device such as the camera or Bluetooth and • configuring compliant and noncompliant apps. Administrators can be alerted if a non-compliant app is installed. For further information force administrators should visit 'Apply features and settings on your devices using device profiles in Microsoft Intune'.	
CSP-BLU-006	Control the installation of applications (apps) on devices where Bluetooth is enabled. Some applications have been known to have excessive permissions which allows access to Bluetooth channels or data which might be used maliciously. Refer to the *NCSP guidance on Mobile Applications* for more information and utilise the lifecycle in **Error! Reference source not found.** in all cases.	ID.RA-09
CSP-BLU-007	Keep devices updated - Android and Apple will often include Bluetooth vulnerability updates within their wider operating system updates. Keep devices updated to mitigate the time the device is vulnerable. Minimise the permissions that applications (apps) on devices have to access Bluetooth.	ID.AM-08
CSP-BLU-008	Where possible, ensure you are using the latest Bluetooth standard (v5.0 or later). This will ensure you are using the most secure iteration (improved encryption) and fastest transmission of data. This can be achieved by purchasing devices through a trusted supply chain and keeping devices up-to-date and patched (see below) and in line with technical policies.	ID.RA-09 PR.PS-03

Reference	Minimum Requirement	Control Reference
Pairing		
CSP-BLU-009	Only pair police-issued devices. Personal devices should never be paired with police assets (this should include wireless home printers, wearable technology such as watches, fitness trackers, headphones etc.)	PR.PS-01
CSP-BLU-010	Police-issued devices should never be paired to smart devices / Internet of Things (IoT) devices e.g. Google, Alexa, Siri or wireless cameras (BWV devices being an obvious exception to this). Further guidance may be found within forthcoming **NCSP guidance documents 'Conferencing Tools Guidance' and 'IoT Guidance'.**	PR.PS-01
CSP-BLU-011	Unpair devices as needed – When Bluetooth devices are not required, or are no longer in operation, they should be unpaired from any other police tech/devices. This must always include unpairing devices from hire cars / non-police vehicles. Always remove previously paired devices from the 'Previously connected device' list. Efforts should also be made to remove personal data from paired equipment such as sat-navs and entertainment systems.	ID.AM-08
CSP-BLU-012	Verify who you are pairing with - Without technical user authentication, it is good practice to physically verify the user handling the device you are communicating with.	PR.AA-01 PR.AA-03
CSP-BLU-013	Don't pair devices in public – With the limited operating range of Bluetooth devices, pairing requests should be made away from public areas wherever possible, especially transport hubs or crowded places.	PR.AA-06 PR.IR-01 PR.IR-02

Reference	Minimum Requirement	Control Reference
CSP-BLU-014	Ensure that default pairing codes are changed before issue where practicable. • Regular pairing code changes: To complete a Bluetooth connection, devices will often request a user to input a 4-digit code. The default pairing codes are widely available and therefore make devices vulnerable to unwanted connections.	PR.PS-01
Device specific		
CSP-BLU-15	Seized devices that have Bluetooth capability should be assumed to have Bluetooth switched on. • Consider use of RF pouches or Faraday bags. • Seek advice from Force Technical Support Units (TSU's) or their equivalents. • Seek technical advice on safe storage prior to Bluetooth-equipped devices being taken to police premises.	
CSP-BLU-16	Change default settings in devices to ensure that controls are in place through choice.	PR.PS-01
CSP-BLU-017	Correct configuration - Some devices can be configured to only allow simple Bluetooth connections such as from mouse and keyboards, while blocking connections from complex devices that are more likely to cause harm.	PR.PS-01
CSP-BLU-018	Avoid choosing device names that might disclose the owner, function, business or device type. Avoid naming Bluetooth devices in a way that identifies them as police assets. Example: • Covert_Car • Control_Room_Headset_1 • Custody_Printer	PR.IR-01

Reference	Minimum Requirement	Control Reference
Geo-location		
CSP-BLU-019	Avoid use of Bluetooth at or near sensitive locations. • Implement Zones for higher risk / sensitive areas, to enforce restrictions on the use of devices which may be capable of using Bluetooth. • RF pouches or RF lockers should be used to temporarily store devices.	PR.IR-01 PR.IR-02 PR.AA-06
CSP-BLU-020	Avoid use of Bluetooth during covert, CT or OCG-related operations.	
User education & awareness		
CSP-BLU-021	Reinforce safe use of Bluetooth behaviours, through engagement with users e.g. via End User Device Agreements, Security Operating Procedures (SyOPs), regular reminders to staff, bulletin updates etc. Where the capability exists, conduct Bluetooth scanning to highlight devices that are enabled. This may be included in IT health-checks – see **NCSP ITHC & Penetration testing guideline.**	PR.AT-01

Communication approach

This document will be communicated as follows:

- Internal peer review by the members of the National Cyber Policy & Standards Working Group (NCPSWG), which includes PDS and representatives from participating forces.
- Formal publication and external distribution to PDS community, police forces and associated bodies.

Measurables generated by adopting this guideline can also form part of regular cyber management reporting.

Review Cycle

This guideline will be reviewed at least annually (from the date of publication) and following any major change to Information Assurance (IA) strategy, membership of the community, or an identified major change to the cyber threat landscape. This ensures IA requirements are reviewed and that the guideline continues to meet the objectives and strategies of the police service.

Document Compliance Requirements

(Adapt according to Force or PDS Policy needs.)

Equality Impact Assessment

(Adapt according to Force or PDS Policy needs.)

Document Information

Document Location

PDS - National Policing Policies & Standards

Revision History

Version	Author	Description	Date
1.0	Matt Roff	First Release	April 2023
1.6	Matt Roff	Annual review	March 2024

Approvals

Version	Name	Role	Date
1.0	NCPSWG	National Cyber Policy & Standards Working Group approval	05/04/23

Document References

Document Name	Version	Date
ISF - Standard of Good Practice (for Information Security)	**v2022**	**07/2022**
ISO 27002:2022 - Information security, Cybersecurity and privacy protection – Information security controls	**v2022**	**02/2022**
CIS Controls	**v8**	**05/2021**
NIST Cyber Security Framework	**v1.1**	**04/2018**
CSA Cloud Controls Matrix	**v4**	**01/2021**
10 Steps to Cyber Security - NCSC.GOV.UK	**Web Page**	**05/2021**
Bluetooth Technology Website https://www.bluetooth.com/	**Web Page**	
Secure Development Standard	**NCSP document**	**V1.0**
Physical Asset Management Standard	**NCSP document**	**V1.0**
ITHC & Pen Testing guideline	**NCSP document**	**V1.0**
Mobile Application guideline	**NCSP document**	
Internet of Things guideline	**Forthcoming NCSP document**	
Conferencing Tools guideline	**Forthcoming NCSP document**	