OFFICE OF THE BIOMETRICS
AND SURVEILLANCE
CAMERA COMMISSIONER

Biometrics and Surveillance Camera Commissioner

Secure by Design, Secure by Default

Video Surveillance Products

Introduction

This guidance is for any organisation manufacturing Video Surveillance Systems (VSS), or manufacturing or assembling components intended to be utilised as part of a VSS.

It is intended to layout the Biometrics and Surveillance Camera Commissioners (BSCC) minimum requirements to ensure such systems are designed and manufactured in a manner that assures they are Secure by Design.

It also contains certain component requirements that will ensure a configuration that is Secure by Default when the component is shipped, thereby making it more likely that the system will be installed and left in a secure state.

This guidance forms part of a wider suite of documentation being developed as part of the SCC Strategy, in support of the SCC Code of Practice.

Background and Context

The nature of the Internet means that connected devices can be subjected to a cyber attack from anywhere in the world. Widespread attacks on connected products is a current and real threat, and a number of highly publicised attacks have already occurred.

The Mirai malware targeted devices such as internet-enabled cameras (IP cameras). Mirai was successful because it exploited the use of common default credentials (such as a username and password being set by the manufacturer as ‘admin’) and poor security configuration of devices. Ultimately, this facilitated attacks on a range of commercial and social media services and included an outage of streaming services such as Netflix.

An evolution of Mirai, called Reaper, has also been discovered. Reaper used publicly and easily available exploits that remained unfixed (patched) and highlighted the problem around non patching of known security vulnerabilities, allowing attackers to utilise them to cause harm.

In order to reduce the risk of harm and damage to organisations utilising VSS, it is vital that component and system manufacturers are able to demonstrate that their products meet the minimum requirement to be deemed Secure by Design. This will provide confidence to the end user that systems, if installed in the recommended configuration, can be used in a connected environment without introducing any undue, additional vulnerabilities.

In putting together this guidance, consideration has been given to existing International and National Standards and a range of Industry Guidance and Best Practice.

Secure by Design

Secure by Design ensures that a product has been designed from the foundation with security in mind. Manufacturers following a Secure by Design process are generally well aware of the current threat landscape and are committed to developing products that are resistant, at the point of manufacture, to such threats. Through life Secure by Design also requires an ongoing vulnerability management programme that ensures vulnerabilities identified are mitigated in a timely manner. This often includes a vulnerability disclosure process and the development and distribution of software patches to correct the vulnerability.

Secure by Default

Security by Default ensures that the default configuration settings of a product are the most secure settings possible. It is important to appreciate that these will not necessarily be the most user-friendly settings, and the balance between security and user friendliness often needs consideration.

In putting together this guidance, consideration has been given to creating a set of minimum requirements that will provide a baseline level of Secure by Default, whilst still balancing the needs for a user-friendly experience for the installer and system integrator.

Secure by Default has an added benefit of removing the burden of knowledge away from the installer or system integrator on how to lock a system down, providing them with an already secure product.

Demonstrating Compliance

Manufacturers seeking to display the Secure by Default logo will need to self-certify their products using the appropriate documentation, available for download from the same site as this document.
Changes to products claiming compliance must be appropriately validated against the self assessment process for continuing display of the logo.

Security Requirements

The following tables provide guidance on the SCC requirements for securing VSS products by design (Secure by Design), and ensuring that these products are Secure by Default, rather than relying on security installers to instigate such procedures. All of the below elements are considered to be mandatory requirements.

Element	Notes
Default Passwords	• Force the installer to change the password on boot up. • In addition, include a strength indicator or 'weak password not accepted' facility.
Hardcoded Engineer Reset Passwords	• The device must not have hidden user accounts. • The device must not have hardcoded account passwords. • Vendors must not be able to assist users recovering lost/forgotten device passwords.
Protocols and Ports	• All ports and communication protocols must be disabled by default unless vital to the functioning of the component. • Commonly accepted vulnerable or obsolete communication protocols must not be present on the device. • Where a newer version of a communication protocol has been developed and released, this must be incorporated into the development lifecycle and rolled out within a reasonable timeframe.
Encryption	• HTTPS must be used for communication with any web interfaces. It must not be possible to connect to an out-of-the-box device without HTTPS (using self-signed certificates). • Where encryption is used for protecting network communications across untrusted networks, facilitating remote access etc. then up to date Transport Layer Security must be used. • Where encryption is to be used for securing data at rest then it must utilise the current industry accepted standards.

Element	Notes
Open Network Video Interface Forum Protocol (ONVIF Protocol)	• ONVIF protocol must be disabled at boot up, although products can still be discovered by VMS/NVRs. • Video stream(s) must be disabled until a new user/password is set up.
Remote Access	• Remote access must be fully disabled as default, and must be explicitly enabled before use, or permissions granted for device to 'call home'. The device may need to use DHCP, DNS etc. in line with best practice cyber security principles to achieve this. • The device must never attempt to access external vendor-controlled network services without system owner consent. • Remote access into a VSS must not, by default, enable access onto other connected network services. • Where servers and workstations are to be provided as part of the VSS, these must be configured to be locked down in line with industry best practice, this should include no remote access in the baseline configuration.
Software Patching and Firmware Upgrades	• Manufacturers must have a portal policy/resource centre for handling upgrades/patches with transparency/community sign up programmes. • For critical updates whereby a product is vulnerable, an appropriate notification is essential at base level and must be issued to those who have signed up to the portal resource centre. • A non-critical and functional advisory service must also be made available to subscribers.
Penetration/Fuzz Testing (Vulnerability Scanning)	• The device must have a documented procedure and be self - tested at manufacturing source to comply with SCC/BS conformity.
Use of IEEE 802.1x	• Devices must be IEEE 802.1x capable.

RATIONALE

Default Passwords

In the past VSS devices have been manufactured to contain a default username and password, often ‘admin’ and ‘password’. The installer or end user is then expected to know how to change this and to actually make the change. The reality is that many devices have been left with the defaults enabled, resulting in numerous security and privacy breaches. It is therefore vital that all default usernames and passwords are changed as part of the device deployment.

In order to minimise the opportunity for a default password to be replaced with an equally insecure, easily guessable or easily crackable password, devices need to provide a visual indicator as to the password strength. Password strength indicators are a simple tool to help individuals understand how strong or weak the password chosen is, measured against common industry good practice, the intention being to steer users away from the weakest passwords.

Also acceptable are devices that have built-in password checking and will not permit the individual to select an insecure password. In these instances, onscreen prompting should aide the individual by stating the commonly accepted standard for a good/strong password.

Guidance on best practice password management and security is available from the National Cyber Security Centre (NCSC) (https://www.ncsc.gov.uk). Information on the most hacked passwords is also available from NCSC https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Hardcoded Passwords

The practice of hardcoding passwords into software has long been discouraged by The Open Web Application Security Project (OWASP) for several reasons.

Using hardcoded passwords increases the chances of a password being guessed enormously, and, where those passwords are used for authentication purposes significantly increases the likelihood that a device will be compromised by an attacker. This situation is further exacerbated where there is a single default administration account that is allocated a (often) simple default password hardcoded into the program or device. This password is then the same across all similar devices, making the compromise and harvesting of large numbers of devices highly likely.

In most cases, where usernames and passwords are hardcoded in, it is not possible for these settings to be changed or disabled by either installers or end users and in some cases, installers and end users may not even be aware that such hardcoded credentials exist, further increasing the device or system vulnerability and likelihood to attack.

In order to mitigate this risk, a compliant product must not utilise any hardcoded usernames and passwords. Instead products must implement a mode which requires the user to enter a unique strong password at first logon, to the standard referred to in the section on Default Passwords.

Protocols and Ports

Having an approach to identify baseline technology builds and processes for ensuring configuration management can greatly improve the security of systems. Only those protocols that are necessary for the functioning of the component are to be enabled on devices and all unnecessary ports disabled by default.
Manufacturers must have an effective strategy to quickly fix identified vulnerabilities in protocols.
Where a new version of a protocol, or a replacement to it, has been published, then this must be implemented into the live environment in a timely manner. Failure to do so is likely to result in increased risk of compromise of systems and information.

Encryption

Encryption is a mathematical function that encodes data in such a way that only authorised users can access it. Encryption technology has enabled much greater privacy and security for organisations that use the internet to communicate and transact business online. Mobile, cloud and web applications rely on well-implemented encryption mechanisms, using keys and certificates to ensure security and trust.

HTTPS (the lock icon in the address bar on a web browser) demonstrates an encrypted website connection. The ‘S’ in HTTPS stands for ‘Secure’. Without the ‘S’, data is sent over a connection in clear text and an eavesdropper on a Wi-Fi network, an Internet Service Provider (ISP) or any other interested party can effectively see the data you are transferring. When you transmit data over a HTTPS connection, no-one can eavesdrop while your data is in transit.

Transport Layer Security (TLS) is an encryption protocol that protects data when it moves between computers. When two computers send data, they agree to encrypt the information in a way they both understand. One or both of the computers may refuse to connect if they cannot agree on a suitable encryption method, depending on the rules in place.

It is therefore an integral part of the development of a Secure by Design approach that appropriate encryption should be considered alongside other technical and organisational measures, taking into account the benefits and risks it can offer. Advice on appropriate encryption solutions is available from the NCSC (https://www.ncsc.gov.uk).

In order to mitigate security vulnerabilities associated with unencrypted communications and data storage, a compliant product must use HTTPS for all communications with a web based interface, TLS for all communication across untrusted networks and an appropriate level of baseline encryption for all data being stored at rest.

Open Network Video Interface Forum Protocol (ONVIF Protocol)

ONVIF Protocol is now a widely used open industry protocol for the interface of physical IP-based security products including VSS. ONVIF creates a standard for how IP products within video surveillance and other physical security areas can communicate with each other, reducing interoperability issues with Video Management Systems and associated devices.

This comes with a number of benefits. For manufacturers and their development teams, it means that devices can communicate by using a common protocol while maintaining a system’s compatibility in the security industry. For the systems’ installers and integrators, it reduces

complexity and improves the efficiency of the overall implementation phase. For the end user, it opens up a range of vendors whose products can be selected based on their various merits.

These benefits do not come without their security vulnerabilities though. Often in the past ONVIF streams are left open as default, without changing the default user/password admin/admin. With software being widely available on the internet that can search and find these enabled cameras, there is increased potential for easy access, and for the streamed video to be used for malicious reasons.

In order to mitigate this risk, a compliant product must have ONVIF disabled on bootup by default and video streaming disabled until a new username and password has been created.

Remote Access

An organisation's remote access services (technologies constructed to provide authorised employees and partners with managed, secure remote access to networks and data via the internet from remote locations) have become one of the most exploited IT resources in use today. Insecure or insecurely used remote access technologies or mechanisms, that most security teams assume pose little risk, in reality offer an abundance of options for attackers to infiltrate enterprises.

The remote environment in which these devices are used may also pose risks. For example, security concerns may exist around:

- Lack of physical security controls - creating a risk of device loss or theft.
- Eavesdropping - as information travels over the public internet.
- Unauthorised access to systems or data - potentially overlooking the screen.
- Monitoring and manipulation of data - if a non-authorised user gains access to the device.

Software Patching and Firmware Upgrades

A lot of the security measures that organisations take to keep their data safe happen behind the scenes, like firmware updates and patch management. You may not be aware of them, but they are a critical element of network security and can mean the difference between a secure device and an unsecure one.

Firmware is added during the manufacturing process and provides the low-level control necessary to operate the device. When changes need to be made to a device's firmware, manufacturers will issue an update. What is included in these updates varies, but it is typically a combination of fixes for known issues, new features (limited to the capabilities of the hardware itself) and improved security.

Patches are the equivalent of firmware in the software space. Patch management is the process of applying patches or upgrades for software applications. Sometimes referred to as bug fixes, patches typically improve the usability and performance of an application and address any issues or security vulnerabilities.

Attackers will attempt to exploit unpatched systems to provide them with unauthorised access to system resources and information. Many successful attacks exploit vulnerabilities for which patches have been issued but not applied.

Penetration/Fuzz Testing (Vulnerability Scanning)

Penetration testing (also referred to as pen testing or pentesting) is a form of in-house or paid “ethical hacking”. With permission from the host organisation, members of its own IT staff or specialists from a trusted third party are given the mandate to use any means necessary to gain access to protected systems and networks; this is for the sole purpose of identifying and exploiting software and hardware for any vulnerabilities, or to perform any other activity usually engaged in by malicious intruders, insider threat actors and cyber-criminals.

Fuzz Testing is a type of testing where automated or semi-automated testing techniques are used to discover coding errors and security loopholes in software, operating systems or networks by inputting invalid or random data called ‘fuzz’ to the system. After which the system is monitored for various exceptions, such as crashing down of the system or failing built-in code.

Both types of testing are designed to expose vulnerabilities in either network infrastructure or security-critical programs that might be exploited with malicious intent.

Manufacturers must therefore have an effective process in place for appropriate security testing of components or devices, and, where vulnerabilities are identified, subject the component or device to further development before it may be put into the live environment.

Use of IEEE 802.1x

IEEE 802.1X is an IEEE Standard for Port-based Network Access Control (PNAC). Part of the IEEE 802.1 group of networking protocols, it provides an authentication mechanism to devices wishing to attach to a Local Area Network (LAN) or Wide Area Network (WAN).

When a device is connected to a LAN port on the router with 802.1X authentication enabled, no traffic can pass through that port initially. It is challenged to send authentication details that are passed by the router on to the authentication server for validation, which can then either give a "success" or "failure" response.

A compliant product must therefore be IEEE 802.1x capable.