INDUSTRIAL CONTROL SYSTEMS
Community of Interest

GUIDANCE: THE MANAGEMENT OF REMOVABLE MEDIA WITHIN INDUSTRIAL CONTROL SYSTEMS/OPERATIONAL TECHNOLOGY ENVIRONMENTS.

Introduction

This guidance is intended to enable organisations to implement appropriate controls to ensure appropriate management of removeable media used within Industrial Control Systems (ICS) /Operational Technology (OT environments and is designed to compliment the NCSC's existing generic use of peripherals guidance. Removable media is used for many different purposes within an ICS/OT Environment, including:

- Installing software patches on ICS/OT systems
- Importing anti-virus signatures onto an ICS/OT system
- Installing new PLC/SCADA programs on ICS/OT systems
- Exporting reports and other data
- Provision of off-site backups

A key aspect of the design of any ICS/OT system is to understand all such scenarios where media is to be used, ensuring that all maintenance activities are considered, such that appropriate management of these interfaces can be implemented.

Removable media within an ICS/OT system refers to but is not limited to, media such as USB, CD, DVD, SD Cards, Floppy disks, and portable HDDs.

Differences between IT and ICS/OT

There are a number of differences between ICS/OT and IT environments in respect of the use of removeable media.

In many instances organisations are constrained by the legacy nature of the ICS/OT equipment, and associated engineering tools. This often requires the use of media considered as obsolete by IT such as 3.5" floppy disks.

It also needs to be recognised that many ICS/OT devices, e.g. PLCs, allow the connection of USB devices (e.g. for firmware upgrades) however, given the OS on which they're based, they do not allow the use of conventional port control software.

A further difference relates to the relative priorities of the Confidentiality, Integrity and Availability (CIA) attributes within the IT and ICS/OT environments. While, in an IT environment, Confidentiality of data tends to be a key driver in relation to the management of media, in an ICS/OT environment it can be the Integrity of the data being transferred by media that's the key driver, Confidentiality of some data though is actually critical within ICS/OT environments, especially when it comes to its transfer over removable media. A copy of a PLC program for instance could be extremely useful to an adversary to allow them to craft an attack against PLC systems by knowing what registers within the PLC to write data to that operate outputs. PLC data is often backed up to removable media, so can also be a conduit for data exfiltration for an adversary.

Security Principles

The primary principles required to ensure the secure management of media require that:

- Corporate policies are developed and implemented with solutions to control the use of removable media.
- Where the use of removable media is required to support your business needs, it should be limited to the minimum media types and users needed.
- All removable media should be formally issued to individual users who will be accountable for its use and safe keeping. Users should not use unofficial media.
- Media is checked to confirm that it does not contain any known malware
- The integrity of all files being transferred into the ICS/OT environment is checked to confirm files only contain the expected, authorised, content.
- A register should be kept of all media used to import/export data, and that only authorised media should be permitted for use within the ICS/OT environment.
- Records should be kept of all files/data transferred into, or out of, the ICS/OT environment.
- Any sensitive data shall be appropriately secured/encrypted to ensure its confidentiality.
- All Media should be appropriately sanitised either between use or at end of use/disposal, as per NCSC's Secure sanitisation of storage media guidance.

These principles support objective B3 (Data Security) of the Cyber Assessment Framework (CAF), in particular B3.e (Media/Equipment Sanitisation).

Removable media will be by its very nature, plugged into various devices and the physical interfaces available on them and therefore it is important not to forget both the removable media and the physical interfaces need to be securely managed within a Defence in Depth (DiD) approach. NCSC have developed separate guidance to secure physical interfaces which is also relevant within the ICS/OT Environment. In addition vendors such as Microsoft also have guidance on how logging and monitoring of removable media can be conducted within their operating systems. NIST 800-82r3 also provides guidance on how to handle removable media within ICS/OT environments, and also links to wider NIST related guidance.

There are a number of different methods by which these principles can be implemented, as outlined below.

Standalone scanning stations

Standalone scanning stations use of dedicated standalone PCs, with multiple anti-virus engines and a method of checking file integrity (e.g. confirming software hashes), to scan all media prior to use, relying on procedural controls to ensure such devices are used with any media being used within the ICS/OT environment.

Improved controls can be provided by restricting the types of USB devices that can be used with the PC, effectively standardising on a specific model of USB drive to be used within the ICS/OT environment.

While such devices may seem cost effective, there is a significant overhead in providing appropriate levels of assurance that they are being used correctly, and that all media is being scanned before use in the ICS/OT environment. This can be provided through the use of manual activity logs, which record all required details at each usage, and the regular auditing of these logs. Consideration must be given to ensuring the integrity of the scanning PC itself between uses, such as by booting from a trusted image for each scanning session.

Opportunities should be considered to securely integrate logs from these devices as part of any wider logging and monitoring efforts.

Standalone media validation stations

An alternative to scanning stations would be the deployment of stations which have the capability to install signatures on the media being used, controlling where, and for how long, the media can be used. As this requires the installation of an agent on the target device, there are a number of ICS/OT related scenarios in which they're not appropriate including:

- Use with legacy operating systems, for which compatible agents are not available
- Use with 'non-PC' assets, e.g. PLCs, where the underlying OS doesn't allow installation of the required agent

There are also challenges with the scalability of such solutions as there's a requirement to maintain compatibility between the scanning station, and all agents, to allow the correct operation of the solution. Care should be taken to validate the effectiveness of any software based agents (e.g. do they enforce write blocking until media is validated as authorised).

When considering this option, consideration must be given as to how any integrity checking is to be undertaken as not all stations include the capability to check hashes or provide other means of confirming file integrity. They do though have the benefit of ensuring that only validated media can be used in the ICS/OT environment, and can also define time periods (which can be aligned to approved maintenance windows) for which the media is authorised.

Opportunities should be considered to securely integrate logs from these devices as part of any wider logging and monitoring efforts.

Dedicated Import/Export stations

Where there's a need to be able to import data onto multiple devices within an ICS/OT environment (e.g. a suite of SCADA workstations), an alternative approach is to use a dedicated import/export kiosk with a secure file transfer mechanism to a host (which may be integral to the kiosk) from which multiple devices (which are configured to prevent the use of local media) can draw down the required files.

These devices have the capability to be used with many different types of media, including CD, 3.5" floppy disk, should that be required.

Where multiple devices are networked within an ICS/OT environment, then the NCSC principal based guidance pattern on safely importing data should also be followed.

Opportunities should be considered to securely integrate logs from the dedicated Import/Export stations as part of any wider logging and monitoring efforts.

USB Media

To simplify management of USB media, it's an advantage if the same device type/range can be utilised. Selection of an appropriate device needs to consider the file sizes required to be transferred, whether that be signature updates, WSUS updates, modified PLC programs, firmware etc.

Where there's a need to protect the confidentiality of data on the media, consideration should be given to devices that allow for hardware based encryption, if necessary certified to an appropriate standard (e.g. FIPS 140-2, NCSC CPA).

In all cases, a register of the devices shall be maintained, and their usage recorded. The devices should also be stored securely when not in use.

Physical Controls

A layer of protection can be implemented through physical access controls both to the ICS/OT devices, and the stations described in the earlier sections to provide layers of protection of the environment against the unauthorised use of media. As well as ensuring devices (e.g. PLCs, desktop PCs) are installed in locked cabinets, physical media/USB locks can also be implemented.

Meet Admin Corp

With the principles above it can be difficult sometimes to see exactly how a principle should be applied in any given case. In this "Admin Corp" example, we're going to walk through the selection and usage of a solution to securely manage media in an element of their ICS/OT environment.

For this example, we will re-use fictional case study "Admin Corp" previously used by the NCSC to explore the application of the Secure Design Principles.

Admin Corp runs a plant that produces Adminox, a highly volatile, refined form of administrative paperwork that is essential to every organisation in the country. It is created from volatile raw products using a continuous chemical process.

As an essential service, Admin Corp must comply with the EU NIS Directive. This means that Admin Corp's network, information systems and technology needed for the production of Adminox must be protected from cyber attack. Also, because Admin Corp are regulated for safety by the UK Health and Safety Executive, they must take steps to ensure the continued safety of the Adminox production process.

The process for producing Adminox involves a number of steps, with the final product stored under pressure in a tank. Clearly, no one would benefit from the unconstrained release of this Adminox, with the potential for additional red-tape clogging up local services for years.

Admin Corp's Approach to securing removable media

Due to the potential impact of compromised media being used with dedicated laptops used to support the maintenance and configuration of an isolated Safety System, AdminCorp determined it was necessary to introduce a policy detailing strict controls around the media used with the laptops, that all staff members operating in the environment were required to read and sign that they understood the processes that they needed to follow. This policy covered the media that would be used to transfer new/updated source code from the isolated development environment, and tested patches onto the safety system.

The laptops were running a current operating system and utilised a modern endpoint security product that was frequently updated. The laptops had modern USB ports, with no other media interfaces. In use the laptops would be connected directly to the programming port of the Safety system, and would not be connected to any other element of the ICS/OT environment, or the corporate IT network (following NCSC's Privilege Access Workstation guidance). Their capabilities were also restricted with no access to emails or the internet, with only the applications necessary for the maintenance and configuration of the specific safety system installed.

Given the potential impact of a compromise of the safety system, it was decided that any solution must provide technical controls over the use of the USB media, so the use of a standalone scanning station was discounted. Given the limited nature of the environment to be protected (laptops and associated USB devices), it was determined that a validation station would be the most appropriate solution. A specific device was chosen on the basis that it:

- Allowed the use of different malware scanning engines to those deployed on the laptop, with them being frequently updated
- Allowed the generation of time bound signatures to control the use of the scanned media to a specific timeframe
- Could be integrated with the monitoring and logging procedures that AdminCorp have implemented.

The necessary agent, together with an application allowing the checking of file hashes, were installed on the laptop.

In order to protect the sensitive data as it was being transferred using the USB media, it was decided to enforce the use of USB media with hardware based encryption. A storage device with capacity to host the largest files being transferred to the laptop, with 256-bit hardware encryption was selected and devices purchased and recorded on the organisations asset register.

An approved process for transferring files to these laptops was prepared, with the key steps of the process (each of which was logged) being:

- Integrity of the files to be transferred verified in the source environment with hashes of the files generated and recorded.
- USB media signed out from its secure storage
- Required files copied to the USB drive, and encryption applied.
    - It was necessary to check the integrity of these files (e.g. through code comparison tools) manually
- USB drive taken to the validation station, where its encryption is removed and it is scanned to confirm it to be free from known malware.
    - Once scanned with no issues, a timeframe in which the media could be used was identified (as defined in the approved works order for the activity) and a signature written to the media confirming it to be clean for use.
- Once confirmed for use, the USB media is removed from the validation station, and the hardware-based encryption re-applied.
- As part of the preparation for the work, a laptop was signed out from its secure storage, and the IDs of both the laptop and USB drive recorded on the works order.
- When the start time of the approved works order was reached, the hardware encryption was manually removed from the scanned media, such that it could be inserted into the laptop and the required files transferred onto the laptop, and a record made of the files transferred.
- Once the files were transferred and removed from the USB drive, the USB drive was removed from the laptop which was then connected to the target system to allow the appropriate maintenance/configuration activity to be undertaken in accordance with the approved works order.
- The USB drive was appropriately wiped/sanitised using software on the validation station to remove all the files, and logs recorded automatically of the time/date/method of sanitisation.
- On completion of the activity, both laptop and USB media were returned to their secure storage.

While the validation station had the capability to be integrated with a monitoring and logging solution, in the initial implementation phase this connection was not installed. As such, periodic assurance of the use of the station was undertaken to confirm:

- The correct operation of the validation station, through the use of ‘test malware’
- Confirmation, using the logs on the station, and the details recorded on the works order, that files transferred to the laptop had all been scanned and verified as clean.

CAF IGP Summary

This case study discusses measures that contribute to the following CAF IGPs:

- **B3.A:** You have identified all mobile devices and media that may hold data important to the operation of the essential function.
- **B3.E:** You catalogue and track all devices that contain data important to the operation of the essential function (whether a specific storage device or one with integral storage).

- **B3.E:** All data important to the operation of the essential function is sanitised from all devices, equipment or removable media before disposal.

Statement of Support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS), with support from the National Cyber Security Centre (NCSC). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

This document is provided on an information basis only, ICS-COI members and NCSC have used all reasonable care in verifying the guidance contained within using the data sources available to it, they provide no warranty as to its accuracy or completeness. To the fullest extent permitted by law, the NCSC and the ICS-COI accept no liability whatsoever for any expense, liability, loss, damage, claim or proceedings incurred or arising as a result of any error or omission in the report or arising from any person acting, refraining from acting, relying upon or otherwise using this document. You should make your own judgment as regards use of this document and seek independent professional advice on your particular circumstances.

Reference to any specific commercial product, process or service by trade name, trademark, manufacturer or otherwise, does not constitute or imply its endorsement, recommendation or favour by the ICS-COI or NCSC. The views and opinions of authors expressed within this document shall not be used for advertising or product endorsement purposes.