TRESYS
TECHNOLOGY

SECURING SUPPLY CHAIN DATA DISTRIBUTION WITH XD AIR

SECURING SUPPLY CHAIN DATA DISTRIBUTION WITH XD AIR

INTRODUCTION

The prevalence of digital threats in modern computing environments requires separating critical networks from public Internet infrastructure. This separation is established as a best-practice in corporate, defense, and critical infrastructure environments. Facilities that enforce such separation are known as secure facilities. Despite this separation, it is still necessary to transfer some data into and out of secure facilities during the course of normal day-to-day operations. The primary question is therefore:

- How do you allow data transfer into and out of secure facilities without exposing the facilities to digital threats?

In the course of answering this question we will examine the current security threat landscape, describe methods to address those threats, and make the case that only a secure concept of operations using Tresys XD Air™ fully addresses the primary concern of securing data transfer in secure facilities.

DATA TRANSFER IN SECURE FACILITIES

Many secure facilities enforce separation through digital boundary protection at the network layer, i.e. firewalls and cross-domain solutions. The most strictly secure environments enforce true network separation by prohibiting all external network connectivity. This complete separation is known as Air Gap Separation. Tresys develops products to secure network-layer boundaries and air gap boundaries for secure facilities. This paper focuses specifically on air gap separation; for more information about network-layer boundary protection visit the Tresys website: http://www.tresys.com

Even enforcing air gap separation does not assure security for a secure facility. Normal operations require that some data must be transferred into and out of secure facilities. Inbound data includes vendor-provided software updates. Outbound data includes logging and compliance information. This data transfer process is part of Supply Chain Distribution, and this paper focuses on Securing Data Transfer in Supply Chain Distribution.

There are three primary questions faced in securing data transfer in supply chain distribution:

- How do you assure only trusted, non-malicious data gets transferred inbound?
- How do you assure only intended, non-sensitive data gets transferred outbound?
- How do you enforce this security without adversely impacting critical system operations?

Because air gap separation precludes network transfer, the data associated with supply chain distribution is commonly carried in and out of the facility on removable media such as CD/DVD ROMs and USB storage devices. The use of removable media introduces numerous threats to secure facilities, as evidenced by exploits such as Stuxnet and BadUSB. The threats from removable media fall into two main categories:

- Data-borne Threats – Viruses, Malware, Trojans, etc.
- Media-borne Threats – Hidden Partitions, Hidden Files, Malicious Firmware, etc.

The full spectrum of data-borne threats and media-borne threats on removable media can be addressed with the existing Tresys XD Air Capabilities.

SECURE SUPPLY CHAIN DISTRIBUTION

During the course of normal operations it is necessary to receive software updates from vendors and load those updates onto systems in secure facilities. Ideally those vendor-supplied updates should be signed files using keys or certificates shared with the secure facility and those files should be transferred on secure devices.

There are three main categories of files which are brought in to a secure facility as part of supply chain data distribution:

- Structured files which can be inspected to ensure contents are non-malicious.
- Files signed by the vendor during distribution.
- Untrusted files which are not signed by a vendor and cannot be verified as non-malicious.

XD Air supports transfer for these three categories of files using known good file inspection, known source file assurance, and traditional antivirus scanning. As structured file inspection capabilities improve and security best practices are adopted by more vendors it will be possible to reduce the volume of untrusted files that get transferred in to a secure facility.

CONTENT INSPECTION & SANITIZATION

Known Good (KG) File Inspection

For common file types it is possible to perform deep content inspection and assure that a file is Known Good (KG). This deep content inspection requires breaking down complex file types into sub-components and inspecting each sub-component, then removing any potentially malicious components such as hidden data or macros. XD Air currently supports known good file inspection for numerous common file types. All files that pass KG inspection are also scanned with multiple traditional anti-virus (AV) engines as an added layer of defense.

Known Source (KS) File Assurance

If the vendor follows security best practices and signs their files for supply chain data distribution it is possible to ensure that the file has come from a Known Source (KS). Establishing trusted transfer of known source files into secure facilities is straightforward. Simply add the vendor's signing verification certificate to XD Air and the files can be transferred in with no exception to the facility's security concept of operations. This is the ideal case for trusted supply chain data distribution for files such as software updates which cannot be adequately inspected with existing KG analytics. Vendors who do not already follow security best practices by providing signed files for supply chain distribution should be strongly encouraged to do so.

Unknown Source Files

Not all vendors supply signed files for supply chain data distribution. While this is not ideal, there are means to help secure this process.

Site-Specific Signing

Tresys offers a secure signing station to accompany XD Air. A secure facility operator can install this secure signing station to allow vendor representatives to sign files on-site which were not signed at the vendor facility. This can ensure that only the files designated as trusted by the vendor representative will be transferred into the secure facility, and no unintended files enter the facility. This option does not mitigate the risk of files being modified in-transit between the vendor facility and the secure facility. To mitigate that risk full KS assurance would be required.

AV-Only Scanning Option

As vendors increase the security of their software distribution methods, the management of data transfer into and out of secure facilities will become simpler. However, there will always be the need to adapt to new and changing situations. For this reason XD Air includes more traditional AV-only scanning as a fallback option for scanning digital content.

While the AV-only scanning is a limited inspection option compared to full KG inspection, the AV-only option in XD Air still provides device isolation and firmware protection, which cannot be provided by traditional software-only antivirus solutions. Therefore the AV-only scanning option on XD Air still reduces the potential attack surface for secure facilities compared to traditional AV solutions.

Problems with Anti-Virus Scanning

Antivirus software can protect against common, well-known malicious data. However, antivirus software does not provide significant protection against targeted, zero-day exploits. Secure facilities such as power plants have been identified for targeted, zero-day exploits in the past. This was proved with the well-documented Stuxnet attack.

Because the sort of targeted attacks in use against secure facilities are particularly effective despite traditional antivirus software protection, it is apparent that traditional antivirus software protection alone is insufficient to provide security against the modern digital threats facing secure facilities. For this reason, we recommend only using the AV-only scanning option of XD Air as a fallback for cases where KG or KS verification are not feasible. These cases should be documented as exceptions to the facility secure policy.

A secure facility should monitor the number of exceptions made to the security concept of operations and work to reduce that number over time. There are two approaches to reducing the number of exceptions and increasing the assurance and protection provided to the Critical Digital Assets (CDAs) in the secure facility: increasing KG capabilities, and securing supply chain data distribution.

Device Sanitization

In addition to the malicious content risk discussed above, there is additional risk from low-level device-borne threats such as hidden partitions or malicious firmware. The threat from malicious firmware has been especially well publicized with the BadUSB exploit. By using XD Air along with a secure concept of operations for secure facility border security, it is possible to mitigate any risk from BadUSB-style firmware exploits as well.

For a full discussion of device firmware threats and how those threats are mitigated using XD Air, please see the Tresys response on BadUSB here: http://www.tresys.com/products/badusb.php

Secure Process & Procedure for Removable Media

It should be apparent based on the breadth of threats posed by removable media that no single technology can address all removable media risks. It is critical that the XD Air removable media content & device sanitization tool is used as part of a broader secure process & procedure for managing the use of removable media in secure facilities.

Based on experience with basic NEI 08-09 Appendix E compliance requirements, Tresys offers suggestions for creating digital media procedures using XD Air here:
http://www.tresys.com/products/datasheets/tresys_xdair_nuc_proc_template.pdf

For site-specific recommendations Tresys can support tailoring your secure processes and procedures. If you are interested in learning more about how XD Air can address your site-specific security concerns please contact Tresys technology: sales@tresys.com

XD Air Capabilities

The XD Air solution addresses data-borne threats with content inspection & sanitization capabilities and addresses device-borne threats with device-sanitization capabilities.

- **Content Inspection & Sanitization:** There are many data-borne threat vectors present in numerous file types. XD Air provides three mechanisms to address these data content threats.

  - **Known Good Analytics:** XD Air performs deep content inspection for many common file types to ensure only trustworthy content is transferred. XD Air can sanitize many common file types to allow the safe transfer of content with any potentially malicious elements removed.

  - **Signed Known Source File Transfer:** For files from a trusted known source, such as a key vendor in a supply chain distribution network, XD Air allows the transfer of signed files for file types that are not verifiable using existing known good analytic methods. This ensures that security does not adversely impact critical system operations.

› **Known Bad Analytics:** XD Air uses multiple behavioral & heuristic anti-virus scanners for performing known bad analytics. Virus scanning can assure that files do not contain any common, well-known malicious content. However, virus scanners are not effective in detecting targeted zero-day threats. An AV-only option is provided as a fallback for files that cannot be scanned using known good analytics and which have not come from a trusted vendor source. This method should therefore be used only for exceptions to the broader security concept of operations.

- **Device Sanitization:** There are many device-borne threats, such as device firmware threats or hidden partition threats XD Air allows the transfer of data to be restricted to only fully sanitized, trustworthy devices.

For a more thorough discussion of these capabilities please see the XD Air website and corresponding data sheet:
http://www.tresys.com/products/xd-air.php
http://www.tresys.com/products/datasheets/XD-Air-Datasheet.pdf

Known-Good Supported File Types
XD Air currently supports the following file categories:

- Microsoft Office Files (97-2010)
- Portable Document Format (PDF) Files
- Compressed Archive Files
- Image Files
- ASCII Text Files

For a full and current list of supported file types see the XD Air data sheet here:
http://www.tresys.com/products/datasheets/XD-Air-Datasheet.pdf

SUMMARY

The scope of portable media threats facing secure facilities is broader than traditional security solutions can address. While these threats are significant, it is possible to address the full scope of portable media threats with a secure deployment of XD Air.

Traditional antivirus solutions provide limited data inspection capabilities, poor protection against zero-day threats, and no protection against device-borne threats. These solutions are not sufficient to address the full scope of portable media threats facing secure facilities.

The known good data inspection capabilities of XD Air provide more robust secure data inspection than is possible with current antivirus software. The device sanitization capabilities offered by XD Air along with a secure concept of operations mitigate the latest generation of device-borne firmware threats. The digital signing and validation capabilities of XD Air enable a more secure supply chain data distribution process. And, because it includes traditional antivirus scanning, XD Air allows for these security modernization efforts to occur without adverse impact to current facilities operation.

Tresys has developed XD Air to be the ideal solution for addressing modern digital threats in air gap protected secure facilities. We have described the functionality implemented in XD Air that addresses each of the primary questions faced for security boundaries in secure facilities. Please send all questions, comments, and inquiries to: sales@tresys.com