XD Air

Position Paper

Secure File Transfer of Portable Media

31 July 2014

1 Portable Media Security

The primary purpose of portable media security efforts is to protect the operation and maintenance of critical digital assets (CDA) – secure supply chain distribution.

This position paper describes XD Air's layered protective measures in the context of support for secure supply chain distribution and maintenance activities:

1. *Known Good Analytics*: DoD-developed deep content inspection of data and proven data validation tools.
2. *Known Bad Analytics*: *Multiple* behavioral/heuristic anti-virus scanners.
3. *Secure Digital Signing*: Site, media, and file authentication and validation.
4. *Media Hardware/Firmware Sanitization*: Media brought to *known good* state.
5. *Secure Platform*: A safe workstation to digitally sign objects, process unknown data, and isolate attack objects.

Collectively, these functions provide more than "sanitized portable media". Their purpose is to provide a secure process for supply chain distributions and this process centers on the goal of providing the tool to *managing the flow* of files/objects entering and exiting controlled areas and loaded on CDA.

2 Product Goal – Use All Available Technologies

Our goal is to provide a tool that can provide a transition from less secure behavioral scans to more complete and trustworthy management and control practices that govern the flow of file objects entering and exiting controlled areas.

XD Air has anti-virus scanners but focuses on providing a 'clean' signing platform and advanced *known good* sanitization capabilities for those files that can be scanned this way.

Simply, the operating procedures are:

- Use *Known-Good* sanitization on the objects you can.
- Digitally sign media and file objects for external transfers (vendor-operator, intra/inter site)
- Use anti-virus scans *Known Bad* as an analysis tool for the exceptions

The AV systems used by XD Air are no better or worse than other products when used for files that inherently cannot be brought to a known-good state, but XD Air does provide far better assurance for those file types that do have known good profiles.

The combination of *known good* and *known bad* sanitization technologies, plus digital object signing, operated from a secure platform, provides a the most complete product available to address software transfer needs in the existing operating environment.

3 Background

Software and configuration updates on portable media enter facilities daily to operate and maintain critical digital assets. This includes software revisions and bug fixes from vendors, data collected from remote equipment and configuration changes for control and monitoring systems. These transfers have historically been a major attack vector of process and business systems in air-gapped sensitive or controlled access areas.

In 2008, a foreign intelligence agency launched a cyber-attack against the United States via USB flash drives[i] with malicious code embedded in the USB firmware. Infected USB drives were inadvertently placed into classified mission critical systems and the malicious code spread. The National Security Agency (NSA), tasked with preventing future attacks, began an operation codenamed *Buckshot Yankee*[ii] and contracted Tresys to build a solution, which became XD Air.

4 Solution: Whitelisting and "Known Good"

XD Air employs a Nuclear Regulatory Commission (NRC) accepted approach for scanning complex files against a "known good" baseline for each file type. Where possible, XD Air will cleanse the questionable content; if not, the file is quarantined for further human or forensic review. Hundreds of filter settings are configured to scan for potentially dangerous content.

In this way, XD Air protects against ***unknown*** malware attacks by permitting transfer of only those resources ***known to be good***. While XD Air also virus scans each file, conventional virus software rejects only "known bad" objects, a process inherently exposed to new, highly targeted, single instance attack schemes.

XD Air additionally provides a protected audit archive to ensure the organization knows what files transferred through the device, when and by whom. This information provides insight into the insider threat and tracks the movement and flow of all data into the controlled area.

Custom filter configurations can be created to support scanning of additional file types. However, not all file types have a "known good" state. For these, multiple antivirus engines scan the media.

XD Air supports all types of portable media including USB flash drives, SD Cards, CDs, DVDs and removable hard drives and other USB-connected devices. XD Air requires no special training for operation and updates to the virus definition files is the only on-going administrative requirement.

5 Clean Media

As demonstrated by *Buckshot Yankee* and BadUSB[iii], USB devices themselves can harbor malicious content to infect a system. Some USB flash drives include a special area called a "U3 partition".[iv] When a U3 smart drive attaches to a Windows computer, the

contents of the partition are automatically launched. The intention of this mechanism is to allow loading any special device drivers or other software necessary to access the device. Malicious users of this mechanism are easy to imagine and several attacks have propagated this way[v].

To protect confidentiality and provide integrity, XD Air offers multiple mechanisms for sanitizing destination USB devices, both formatting and overwriting. Before XD Air writes filtered data to any destination device, the media is reformatted. This process deletes the file pointers but does not attempt to overwrite the memory locations. If the device contains a U3 partition, that partition is removed. XD Air also provides an option to overwrite all of the storage locations on the device, providing a more secure data transfer. Software based on NSA's own tool is used to perform this operation. Once the process overwrites the drive multiple times, it is deemed to be clean and safe for reuse - the integrity of the device is assured. Some facilities have already established a process to ensure that the USB drives they use to input data to their systems have been sanitized, using the Tresys overwriting process. The drives are then coded and segregated so that only clean devices are written to, and previously used devices again undergo cleansing before they are reintroduced into the process.

6 Pre-validated Files

Many files types, by their nature, are potentially malicious, such as executables and binary files and can have no known good basis. XD Air offers the option to sign and pre-validate these files, so that the originator vouches that the content is safe. At the customer site, XD Air verifies the digital signature and "unwraps" the file for loading to the appropriate systems, along with a signed file manifest. This assures that the data was not modified in transit and allows the facility to log the origin of the data and have strong attribution of ownership. This is a valuable tool for securing the supply chain. Tresys is working with suppliers to insert this security step into their process. XD Air creates an auditable event when this type of data is transferred, ensuring a method to track this type of data transfer.

7 A Process Template for the Supply Chain

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

As vendors increase the security of their software distributions and better security tools and processes become more available and familiar the management of the 'flow' of software and data files to CDA will improve. This section presents a concept for better management and organization of the flow of objects into controlled areas (e.g. Levels 3 and 4).

Use *Known Good* Sanitization function where possible

Files from unknown sources are scanned to extremely high levels of assurance using the XD Air. See Section 10 *Known Good* File Types for those files that are scanned automatically. Note that many custom 'flat' file types can be added to known good processing at the discretion of the administrator. (Other file types might also be added to known good file types: inquire with Tresys.)

Files received from vendors and other external sources

Ideally, all files received from vendors should be digitally signed to preserve the integrity and origin ID of the files/objects. This establishes a trusted relationship between vendor and operator and extends the measures taken by the vendor to develop and safely distribute programs to their customers.

While compiled programs and binaries (e.g. .exe, .dll, etc) cannot be made known-good, XD Air has filename 'whitelist' policies that can be modified to suit requirements.

Use Known Bad (AV) scanning for exceptions

For files that cannot be scanned by the known good process and those files that are digitally signed (pre-validated), XD Air will scan the files with multiple AV engines, conforming to older industry policy.

If only AV scanning is applicable, the operation should be performed by an administrator, who also evaluates the circumstances of the transfer, such as the origin and transport of the media.

8 Summary

XD Air is a valuable tool to support compliance with cyber intrusion detection and prevention needs and regulations. Uniquely combining whitelisting with known good analytics, XD Air provides the most effective means to eliminate malicious content on portable media, greatly enhancing the integrity of file transfers and the advanced digital signing and validation capabilities allow for simple integration into a more secure advanced supply chain distribution processes.

9 *Known Good* File Types

Microsoft® Office (97-2010)

- Word (.doc,.docx, .docm)
- Excel (.xls, .xlsx, .xlsm)
- PowerPoint® (.ppt, pptx, .pptm)

Portable Document Format (.pdf)

Compressed Files

- BWT zip (.bz2)
- UNIX tar (.tar)
- Pkzip (.zip)
- GNU zip (.gz)

Image Files

- Joint Photographic Experts Group (.jpg, .jpeg)
- Windows® Bitmap (.bmp)
- Tagged Image Format (.tif, .tiff)
- Windows® Metafile (.wmf)
- Windows® Enhanced Metafile (.emf)
- Graphics Interchange Format (.gif)
- Portable Network Graphics (.png)

ASCII text files (.txt)

10 Supported Media Types

- USB flash drives
- Floppy disks
- Solid state drives
- SD cards
- DVD
- CD
- Portable hard drives
- Compact flash
- Hardware-encrypted USB flash drives (Imation Ironkey/MXI)

For more detail, see: http://www.tresys.com/products/xd-air.php

---

References

[i] http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain

[ii] http://www.washingtonpost.com/national/national-security/cyber-intruder-sparks-response-debate/2011/12/06/gIQAxLuFgO_story.html

[iii] http://www.wired.com/2014/07/usb-security/

[iv] http://en.wikipedia.org/wiki/U3

[v] http://www.irongeek.com/i.php?page=security/plug-and-prey-malicious-usb-devices