

Enabling Mobile and Portable Media for Use in Mission Critical Operations

Challenge

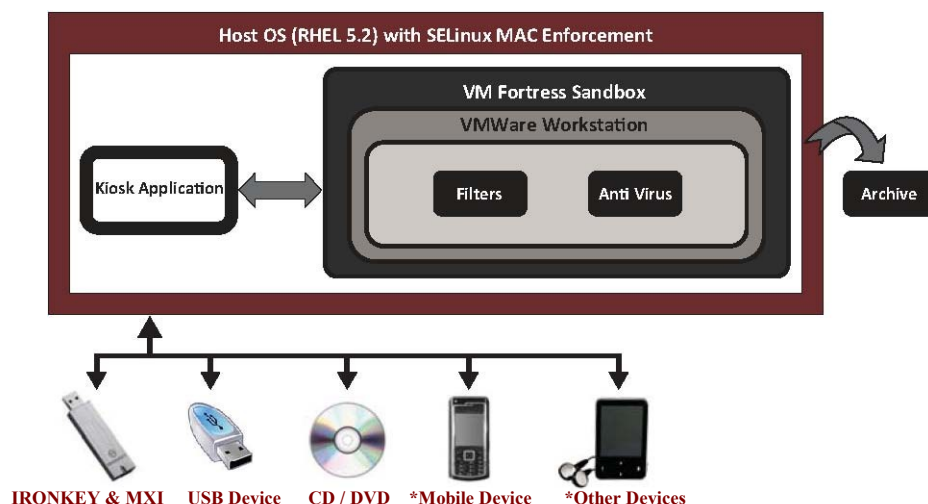
Mobile and portable media play a critical role in data sharing across systems and networks in use by the US Government and its coalition partners. Recent cyber attacks have used these devices to propagate various forms of virus software and malware across these systems and networks, and the potential exists for additional attacks via this vector. A solution was required to address these complex and dynamic challenges, maintain operational use of the device, prevent users from altering or bypassing its critical functions and be readily available with minimum support requirements to be able to deploy it globally and in forward operating locations.

The solutions needed to be able to cleanse a USB device of malicious content or files to eliminate the risk of propagating these files and to quickly enable continued operation use for mission critical applications. It had to be able to inspect a large number of file types for malware and other malicious content on a USB device, capture and archive data for later forensics analysis and cleanse the files and the device while keeping safe user data intact. The solution also needed to be able to adapt to new types of USB and peripheral device attacks as they evolve.

Solution

Tresys worked with the customer to develop the solution known as XD Air [USG program name FiST], a kiosk-based, file sanitization tool. XD Air accesses a mobile and portable media device and it's data in a virtual, controlled and isolated environment to safely handle malicious content without the risk of infecting either the kiosk itself or subsequent USB devices. XD Air conducts deep content inspection and analysis and detects, removes and stores (for forensic analysis) malicious hidden content, viruses and malware from mobile and portable media devices. In addition to the malicious content detection software, XD Air includes software for forensic capture and archival, secure erasure of M&P media devices and a simple interface. XD Air reconstructs infected files and securely cleanses the M&P media device to rapidly enable use in operational environments. The inspection engine is a combination of GOTS and COTS software that inspects and cleanses a variety of file formats, including:

- Microsoft Office 97-2007 (.doc, .xls, .ppt)
- Imagery files (.jpeg, .bmp, .tiff, .gif, .wmf, .emf, .png)
- Compressed files (.zip, .gz, .bz2, .tar)
- Presentation and text files (.txt, .pdf)



The inspection engine also includes a carefully tuned policy that balances the need to block malicious content with the operational need to pass important data.

To further enhance end-to-end protection of USB drives, Tresys XD Air supports all MXI keys and IronKey Enterprise, Personal and Basic secure flash drives. IronKey's family of encrypted USB devices deliver the most secure data at rest solutions on the market FIPS 140-2 Level 3 certification. Always-on hardware encryption combined with active malware defenses safeguard the most sensitive data on the USB device, ensuring that only authorized individuals can access the data on the device.

XD Air software is hosted on a secure platform built using several COTS products, including Red Hat Enterprise Linux 5 and Tresys VM Fortress for secure virtualization. This platform facilitated the rapid creation of XD Air by allowing secure integration with existing USG and other commercial software to create the complete solution. The underlying security of both Red Hat Enterprise Linux and VM Fortress is established and enforced by Security Enhanced Linux (SELinux). Using secure VMs enables the system to process malware and virus-infected devices without the system itself becoming infected. The solution is designed and built to be shipped as an appliance with minimal implementation and support requirements.

XD Air appliance:

- Red Hat Enterprise Linux 5
- Tresys VM Fortress
- FiST Software
- SELinux

Hardware:

- 64 bit based COTS laptop
- 7200 RPM hard drive
- Dual core Intel Pentium Processor
- 8 GB RAM

Summary and Benefits

The USB interface has become a broadly accepted standard across government and industry, and M&P media are familiar and widely used tools. They are used to share vital information in forward locations, move data between coalition partners, deliver command instructions and situation briefs and in a wide variety of other critical applications. They are also used in more routine, yet equally important roles such as providing language training via USB-connected MP3 players and the downloading of photos from digital cameras.

At the same time, the variety and sophistication of attacks on Government computer systems and networks continues to grow. The mobile and portable media device is being used as a vector for malicious software, and virus and malware scanning software tools are an inadequate defense against these emerging threats. The Government quickly recognized this critical security challenge and elected to put the XD Air appliance in place to mitigate the risks associated with this evolving threat.

About Tresys

Tresys innovates and applies advanced technologies to quickly solve the needs of customers requiring agile responsiveness to security requirements. By leveraging secure open source software, our products and services support the most sensitive security missions around the world. As a result Tresys enjoys a distinct reputation for shifting the way governments and businesses approach security. For more information, visit: www.tresys.com.

