Windows Embedded Standard 7 Whitepaper

Securing Your Custom Operating System Image with Windows Embedded Standard 7

As with standard desktops and laptops, protection from viruses, malicious users and general malware is of paramount importance for embedded devices. Additionally, you many need to preserve the runtime images of embedded systems by protecting them against write operations; because Windows Embedded Standard 7 is based on Windows 7, depending on your configuration, many of the same security vulnerabilities will apply.

To address these issues, Windows Embedded Standard 7 has a variety of tools - both in Windows 7 and through Windows Embedded Enabling features - that help secure your device at the hardware, network and applications levels.

Windows 7 Security Features for Windows Embedded Standard 7

Because Windows Embedded Standard 7 is based on Windows 7, you can use many different Windows 7 security features to lock down your device. In this whitepaper, we highlight some of the features that can be used to achieve common scenarios for locking down Windows Embedded devices.

Application Lockdown with AppLocker

For Windows Embedded Standard 7 devices, it is essential to be able to control the applications that run on the system. If a device runs only on your own custom application, such as a kiosk or set-top box, it may be advisable to block all other applications that might take the user out of the custom experience. If the device runs on a more open shell, however, you may want to merely restrict a set of applications that are allowed to run.

AppLocker is a Windows 7 standard technology that prevents the execution of unknown and unwanted applications within your network or on an individual device. It builds and improves on Software Restriction Policies (SRPs) to allow for easy and flexible application lockdown.

In addition to blocking certain applications, AppLocker can block certain scripts (.ps1, .bat, .cmd, .vbs and.js), installer files (.msi, .msp) and even libraries (.dll, .ocx). AppLocker can also be configured to audit prohibited activities and track their history in Event Viewer. This is particularly useful during testing, but can also be used to monitor undesirable activity remotely.

In addition, AppLocker rules can be pushed down by Group Policy in a domain environment or be applied to individual devices through Local Group Policy, even if the device is not in a domain environment or connected to a network.

Depending on the configuration method you decide to employ, to get AppLocker to work on your embedded device, you must include the Security/Application Security, System

Services/Windows Installer and Management/System Management/Group Policy Management (with its optional dependencies for configuration) packages, at a minimum. For specific instruction on how to use AppLocker to block an application from running on your embedded device, please see http://blogs.msdn.com/embedded/archive/2010/03/16/application-lockdown-with-applocker-on-standard-7.aspx.

Hardware Lockdown

With hardware lockdown, Windows 7 features can help you control device installation and usage on the computers that you manage, through the configuration of Group Policy settings. These features allow you to:

- Prevent users from installing any device
- Allow users to install only devices that are on an "approved" list.
- Prevent users from installing devices that are on a "prohibited" list.
- Deny read or write access to users for devices that are themselves removable, or that use removable media (e.g. CD and DVD burners, floppy disk drives, external hard drives and portable devices such as smart phone and Pocket PC devices).

Restricting the devices that users can install helps reduce the risk of data theft by eliminating the most convenient methods for misappropriating data, such as CD burning. You can also reduce the risk of data theft by using Group Policy to deny write access to users for certain devices that are removable or that use removable media.

The Group Policy settings can be configured in Local Group Policy Editor by navigating to Local Computer Policy\Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions.

Windows 7 uses two types of identifiers to control device installation and configuration: (1) device identification settings; and (2) device setup classes.

Device identification strings are contained on the individual hardware devices and assigned by the device manufacturer. The same identification strings are included in the .inf file contained in the device driver package. Windows 7 chooses which device driver package to install by matching the number to the identification string. If there is no exact hardware match, Windows will search for, and employ a compatible ID, based on the best possible match. The strings range from the very specific – matching a single make and model of a device – to the very general, possibly applying to an entire class of devices.

Device setup classes are another type of identification string, that are used to encompass an entire class of devices (e.g. all CD drives). These identification strings are also assigned by the manufacturer and are grouped around devices that are installed and configured in the same way.

You can use the Group Policy settings to allow or block users from installing device drivers that are an exact match to an identification string or fit into the device setup class. Additional Group Policy settings allowing administrators to override the device installation policy for the purpose of adding or updating the drivers for any device are also available.

To allow these solutions to work on your embedded devices, you must include the Devices and Printers/Driver Foundation and Management/System Management/Group Policy (with its optional dependencies for configuration) packages.

Network Lockdown
For network lockdown, Windows Embedded Standard 7 contains the traditional firewall security and all of the Windows 7 updates to Windows Firewall with Advanced Security.

Windows Firewall with Advanced Security provides host-based, two-way networking traffic filtering for your devices. This allows you to block unauthorized network traffic flowing in and out of each device. It also works with Network Awareness so that it can apply security settings appropriate to the types of networks to which the device is connected.

Windows Firewall with Advanced Security for Windows Embedded Standard 7 can, among other things:

- Allow for multiple active profiles
- Allow for certificates issued by an intermediate certification authority
- Specify port numbers, protocols or port ranges
- Co-exist with third party firewalls
- Specify groups of devices or users authorized to establish a tunnel to the local computer
- Manage outbound and inbound filtering
- Configure bypass rules for specific devices
- Create firewall rules that filter connections by user, computer, or groups in the Active Directory.

To employ Windows Firewall and Advanced Security on your devices, you must include the Networking\Windows Firewall (with its optional dependencies for configuration) Package.

Windows Embedded Standard 7 Enabling Features for Embedded Devices

For security scenarios that are important for certain embedded devices, but not necessarily traditional PCs, Windows Embedded Standard 7 includes new features, called Embedded Enabling Features (EEFs) to help enable embedded-specific solutions.

Write Filters
Write filters enable building more secure and reliable embedded systems by protecting disks against write operations. They intercept writes and redirect them to a different storage location, called an overlay. Windows Embedded Standard 7 offers three write filters, which protect the system at partition and file levels.

Enhanced Write Filter
The Enhanced Write Filter provides the ability to write protect a run-time image. Specifically, it secures the system at the partition level by preventing writes to disk and redirecting them to an overlay cache in RAM. These writes can be discarded at reboot, thereby restoring the system to a known state.

In addition to the Enhanced Write Filter overlay, an Enhanced Write Filter volume is created on the media in unpartitioned disk space. This volume stores configuration information about all of the Enhanced Writer Filter-protected volumes on the device, including the number and sizes of protected volumes. Only one Enhanced Write Filter volume is created on your device, regardless of how many disks are in the system. If your media does not support multiple partitions, you can save the Enhanced Write Filter configuration information in the system's registry.

File Based Write Filter

In certain embedded devices, writing to storage media may be undesirable or impossible. As an alternative, the File Based Write Filter protects at the file level and redirects writes to a RAM overlay cache, but allows for exceptions. In this sense, the overlay is similar to a transparency overlay on an overhead projector. Any change made to the overlay affects the picture as seen in the aggregate, but if the overlay is removed, the underlying picture remains unchanged. Explicitly defined folders and files will continue writes to disk but all other writes will be redirected to RAM and can be discarded at reboot.

FUNCTIONALITY	EWF	FBWF
Overlay	RAM	RAM
Write Through Capability	None	File and Folder Write Through
Commit	Commit whole overlay	File Commit Only
HORM	Yes	No
NTFS Support	Full, plus FAT	Subset
Relative Protection	Higher Protection (Lower in I/O stack)	Less Protection (Higher in I/O stack)
Memory Utilization Optimization	No	Yes (can free memory when files are deleted)
Configuration	Limited Runtime Config	Full Runtime Config

Registry Filter

The Registry Filter works with both the Enhanced and File Based Write Filters to allow the persistence of certain registry keys even when the write filters are turned on. It officially supports only two registry keys – TSCAL licenses and Machine Domain Account Secret.

Antivirus Software

As noted, devices operating on Windows Embedded Standard 7 are not self-secured. Therefore, antivirus software is a necessary component of device security. Although write filters provide significant levels of protection, they are not a substitute for an antivirus solution. Worms and viruses can spread quickly throughout a network and even if a run-time image is protected with an Enhanced Write Filter, a virus can still infect it.

Because the virus is stored in the EWF overlay, the virus will continue to propagate to other systems. Even if the overlay is discarded when the system reboots, other systems on the network can continue to infect your run-time image. If a EWF overlay is committed to the protected volume, the system will become infected.

Microsoft's Forefront, Microsoft's antivirus client, is a suggested solution, but third party solutions work on the Windows Embedded Standard 7 platform as well.

Conclusion

The combination of Windows 7 and embedded-specific enabling features can help secure your devices and lock down your operating system image for Windows Embedded Standard 7.