Federal Desktop Core Configuration

Beating the Application Compatibility Challenge

Mr. Chris Jackson
Microsoft Senior Consultant
Optimizing Application Testing

**Basic Cost Center**
- Limited or ad-hoc application testing
- Limited or ad-hoc sharing of application issues and solutions

**Standardized More Efficient Cost Center**
- Defined set of test tools and approaches
- Issues/solutions reported on multiple central systems

**Rationalized Business Enabler**
- Scripted test plans and automated tests
- Issue/solution data captured from various sources with clear escalation paths

**Dynamic Business Asset**
- Automated application tests easily used and updated
- Issue/solution data captured - tied to tools and training plans

This slide represents the views of the presenter and not the Federal Government.
Windows Application Compatibility Infrastructure

Windows components change

| New technology | Bug fixes | Strategy changes |

Changing Windows itself has issues

| May fix one application, but break another | Code branches affect servicing and performance |

We need a way to simulate the behavior of previous versions of Windows, but only for a particular application

This slide represents the views of the presenter and not the Federal Government.
How Shims Work

Application

Shim DLL

Windows

Import Function

Export Function

This slide represents the views of the presenter and not the Federal Government
Standard User Analyzer

- A tool to help IT Professionals and Developers understand issues preventing an application from running with Standard User privileges
- Based on Application Verifier

This slide represents the views of the presenter and not the Federal Government.
What Can You Fix?

Fixable
- Registry
- File
- Token (100101)
- Namespace
- Process

Not Fixable
- Privilege
- Other Objects

This slide represents the views of the presenter and not the Federal Government.
SUA Mitigations

- SUA can recommend:
  - ElevateCreateProcess
  - ForceAdminAccess
  - LocalMappedObject
  - VirtualizeDeleteFile
  - VirtualizeHKCRLite

This slide represents the views of the presenter and not the Federal Government.
ElevateCreateProcess

Symptom
- Host process calls CreateProcess, and it returns ERROR_ELEVATION_REQUIRED (740L)
  - This error code is new in Windows Vista – legacy applications will not be aware of it

Fix Description
- Handles the error code and attempts to CreateProcess a second time, this time requesting elevation
- No effect if the shimmed application has a UAC manifest – error code is returned unchanged

This slide represents the views of the presenter and not the Federal Government.
Symptom
- Application fails explicit administrator check

Fix description
- Pretends the user is a member of the administrators group, even when they aren’t, by:
  - Returning TRUE for various queries of the token
  - Returning success for various permission checks
LocalMappedObject

- **Symptom**
  - Application is trying to create an object in the Global namespace

- **Fix Description**
  - Intercepts the call to create the object, replacing the word Global with Local

This slide represents the views of the presenter and not the Federal Government.
Symptom
- Application is unable to delete files because of permissions issues

Fix description
- Returns success from calls to delete files that are in protected locations
  - If the file was successfully deleted, but it was a virtualized copy, pretends that the real one was deleted as well
  - Subsequent calls to check for the existence of the file will return that the file was not found

This slide represents the views of the presenter and not the Federal Government
Symptom

Application failing to register COM components at run-time

Fix Description

Redirects HKCR writes (HKLM) to HKCU for a per-user COM registration

Lighter weight and better performance than VirtualRegistry with VIRTUALIZEHKCR parameter

Typically, you will use in combination with VirtualizeRegisterTypeLib
SUA Mitigations
demo

This slide represents the views of the presenter and not the Federal Government
File Virtualization

Legacy Application

Vista Application

User Mode

Kernel Mode

\Users\<user>\AppData\Local\VirtualStore\Windows\App.ini

\Windows\App.ini

Luafv.sys

Access Denied

This slide represents the views of the presenter and not the Federal Government.
Registry Virtualization

Legacy Application

Vista Application

HKLM\Software\App

HKCU\Software\Classes\VirtualStore\
Machine\Software\App

User Mode

Kernel Mode

Ntoskrnl.exe

Access Denied

Registry

This slide represents the views of the presenter and not the Federal Government
VirtualRegistry

- Symptoms
  - Application is checking the registry for keys that:
    - Return a more current value than they are looking for
    - Have been deprecated
    - Deny access to standard users

- Fix description
  - Enables registry functions to allow virtual keys, redirection, and expansion values

- Command line parameters...
Virtual Registry Version Lies

- DISABLEWIN9XMODE
- DX7A
- DX8
- IE401
- IE60
- NT4SP5
- NT50
- NT51
- WIN2K
- WIN9X
- WINNT
- WinNTCurrentVersion
- WINXP
- X86ARCHLIE
- XPSP1LIE
- XPSP2LIE

This slide represents the views of the presenter and not the Federal Government.
Virtual Registry Generic Fixes

AddRedirect(HKLM\Key^HKCU\Key^HKLM\Key2^HKCU\Key2)

This slide represents the views of the presenter and not the Federal Government.
Virtual Registry demo
CorrectFilePaths

Symptoms

- Application receives access denied errors when trying to write to files
- Application received file not found or path not found errors when trying to write to files

Fix description

- Modifies path names to point to a new location on the drive
Correct File Paths Processing

1. Default Corrections Applied
2. NEW_PATH converted to short file name
3. OLD_PATH converted to short file name
4. Command line paths corrected

*This slide represents the views of the presenter and not the Federal Government.*
# CorrectFilePaths Variables

<table>
<thead>
<tr>
<th>Variable</th>
<th>Typical Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>%windir%</td>
<td>C:\windows</td>
</tr>
<tr>
<td>%systemroot%</td>
<td>C:\windows</td>
</tr>
<tr>
<td>%systemdrive%</td>
<td>C:\</td>
</tr>
<tr>
<td>%systemdir%</td>
<td>C:\windows\system32</td>
</tr>
<tr>
<td>%username%</td>
<td>bill\g</td>
</tr>
<tr>
<td>%programfiles%</td>
<td>C:\program files</td>
</tr>
<tr>
<td>%userstartmenu%</td>
<td>C:\Users\bill\AppData\Roaming\Microsoft\Windows\Start Menu</td>
</tr>
<tr>
<td>%allstartmenu%</td>
<td>C:\ProgramData\Microsoft\Windows\Start Menu</td>
</tr>
<tr>
<td>%userdesktop%</td>
<td>C:\Users\bill\Desktop</td>
</tr>
<tr>
<td>%alldesktop%</td>
<td>C:\Users\public\desktop</td>
</tr>
<tr>
<td>%userfavorites%</td>
<td>C:\Users\bill\Favorites</td>
</tr>
<tr>
<td>%allfavorites%</td>
<td>C:\Users\Public\Favorites</td>
</tr>
<tr>
<td>%profile%</td>
<td>C:\Users\Public</td>
</tr>
</tbody>
</table>

This slide represents the views of the presenter and not the Federal Government.
## CorrectFilePaths Switches

<table>
<thead>
<tr>
<th>Switch</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>-c</td>
<td>Do not shim CreateProcess routines</td>
</tr>
<tr>
<td>-f</td>
<td>Do not shim file routines</td>
</tr>
<tr>
<td>-p</td>
<td>Do not shim GetPrivateProfile routines</td>
</tr>
<tr>
<td>-s</td>
<td>Do not shim IShellLink routines</td>
</tr>
<tr>
<td>-b</td>
<td>Bare: No built-in path changes</td>
</tr>
<tr>
<td>-u</td>
<td>User: Do not force Start Menu links from <code>&lt;username&gt;</code> to All Users</td>
</tr>
<tr>
<td>+GetCommandLine</td>
<td>Shim GetCommandLine APIs</td>
</tr>
<tr>
<td>+RegSetValue</td>
<td>Shim Registry APIs</td>
</tr>
<tr>
<td>+Win9xPath</td>
<td>Apply Win9x path specific fixes</td>
</tr>
<tr>
<td>-Profiles</td>
<td>Disable user profiles (same as -u)</td>
</tr>
</tbody>
</table>

This slide represents the views of the presenter and not the Federal Government.
CorrectFilePaths Parameters

- switch1  switch2 OLD_PATH;NEW_PATH
  OLD_PATH2;NEW_PATH2

Examples:
- b setup.exe;setupapp.exe
- f -p -s -b setup.exe;setupapp.exe
- setup.exe;setupapp.exe “Bad Place;Correct Location”
- wordpad.exe;%SystemDir%\wordpad.exe
  .\%SystemDir%;%SystemDir%
When applying CorrectFilePaths to an installer, you should apply CorrectFilePathsUninstall as well.

**Symptoms**
- Files, directories, and links are left behind during uninstall.

**Fix description**
- Corrects file paths for uninstallation of the application.
  - Installers that do not remember whether they installed to user or common directories.
  - Installers shimmed using CorrectFilePaths.
CorrectFilePaths

demo

This slide represents the views of the presenter and not the Federal Government.