User Account Control in Windows Vista

UAC Under the Covers

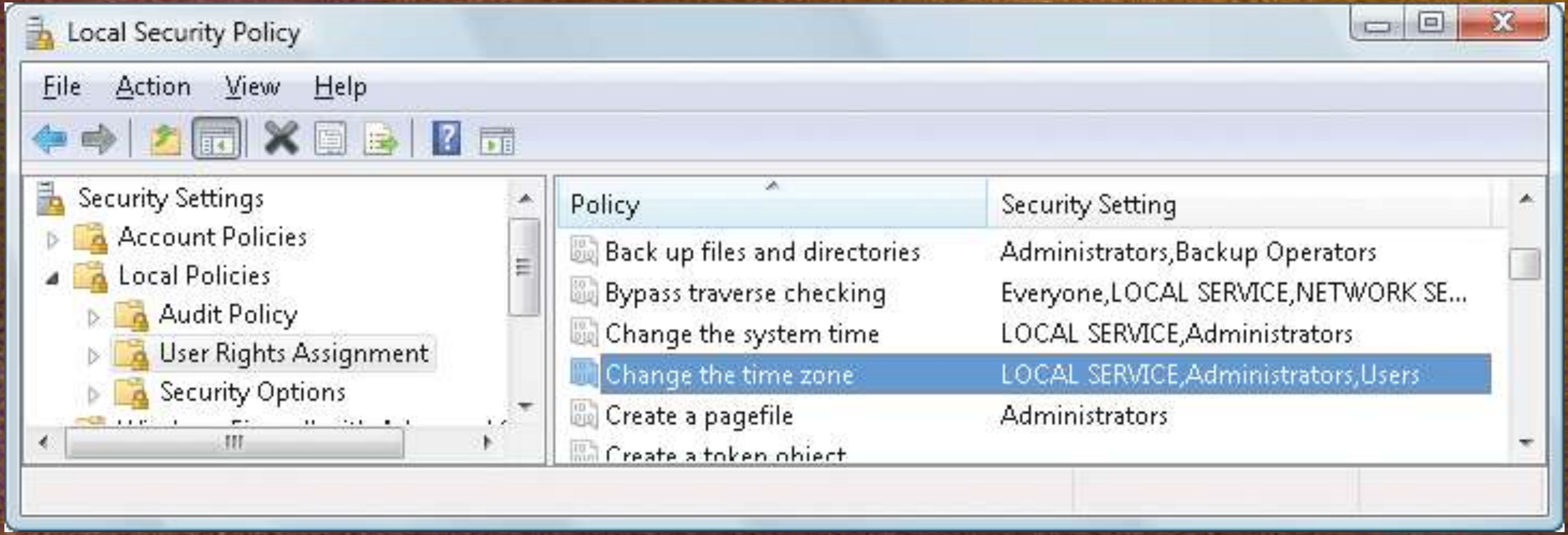
Bob McCoy, CISSP/ISSAP
Technical Account Manager
Microsoft Corporation

UAC Goal

Make running as non-admin possible and practical

Addressing the Issues

- Assumed admin rights
- Occasional need for admin rights



Policy	Security Setting
Back up files and directories	Administrators,Backup Operators
Bypass traverse checking	Everyone,LOCAL SERVICE,NETWORK SE...
Change the system time	LOCAL SERVICE,Administrators
Change the time zone	LOCAL SERVICE,Administrators,Users
Create a pagefile	Administrators
Create a token object	

Additional *User* Settings

- WEP
- Create VPN connections
- Change power management settings
- Install critical Windows updates
- Group Policy settings may enable standard users to:
  - Install IT-approved printers or devices
  - Install ActiveX controls from administrator-approved sites

Virtualization

- Been around since Windows 2000
- Configured manually via Application Compatibility Toolkit
- Happens automatically for “legacy” apps on Windows Vista

Legacy Apps

- ✓ 32-bit app
- ✓ Not running with admin rights
- ✓ No Vista manifest
  - ○ Embedded
  - ○ Separate *.manifest file

Legacy Apps

The legacy process believes that the operation succeeds when it really created the file in a location fully accessible by the user, but default permissions on the Windows directory deny access to the application written for Windows Vista.

Manifest

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<!-- Copyright (c) Microsoft Corporation -->
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
    version="5.1.0.0"
    processorArchitecture="x86"
    name="Microsoft.Windows.FileSystem.CMD"
    type="win32"
/>
<description>Windows Command Processor</description>

<trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
        <requestedPrivileges>
            <requestedExecutionLevel
                level="asInvoker"
                uiAccess="false"
            />
        </requestedPrivileges>
    </security>
</trustInfo>
</assembly>
```

```
level="requireAdministrator"
```

```
level=“highestAvailable"
```

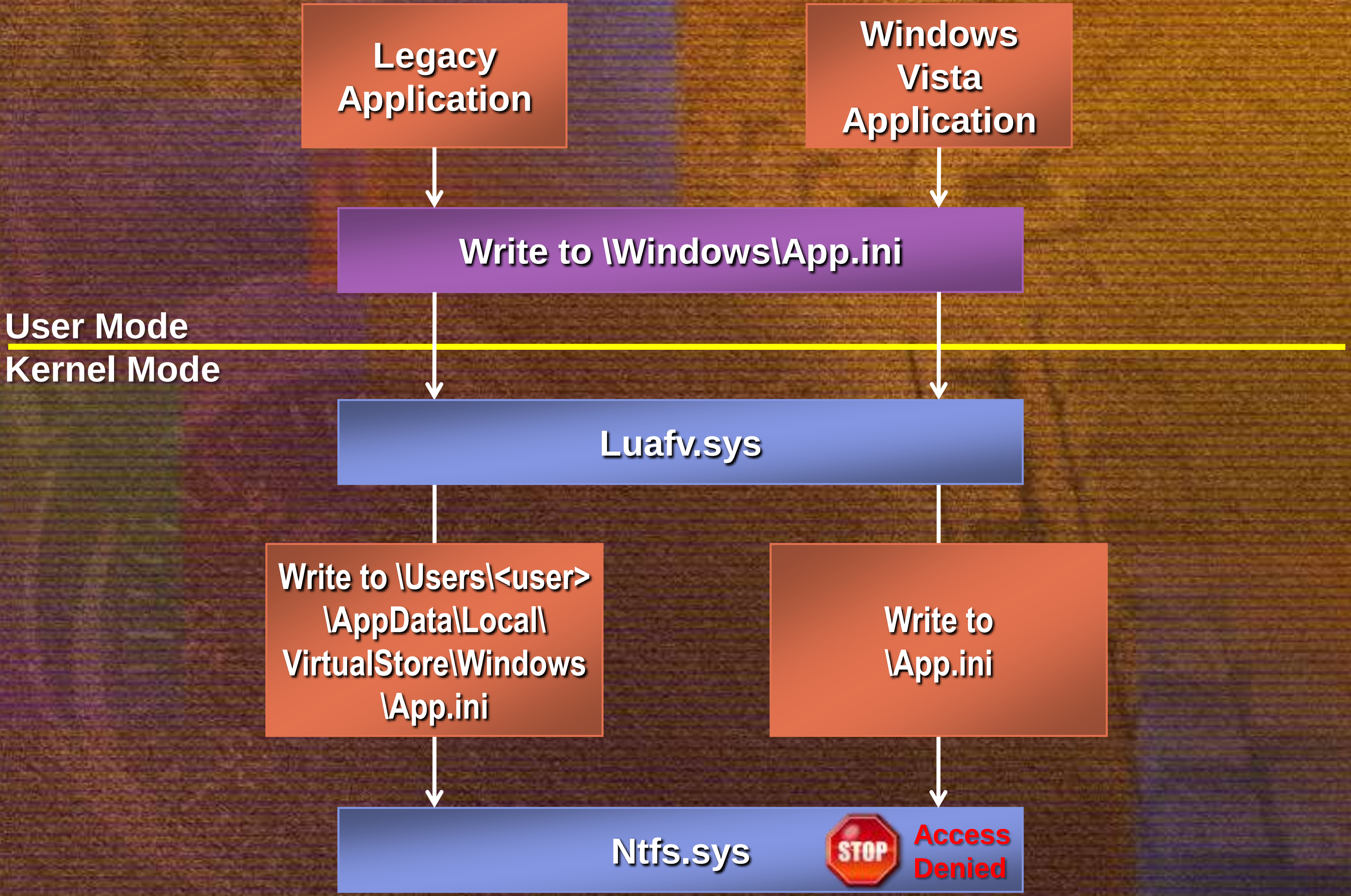
mt.exe

sigcheck –m filename

File Virtualization

- %ProgramFiles%
- %ProgramData%
- %SystemRoot%
- NOT virtualized: exe bat scr vbs
- Add additional extensions
  HKLM\System\CurrentControlSet\Services\Luafv\Parameters\ExcludeExtensionsAdd
- \Users\<user>\AppData\Local\VirtualStore

File Virtualization



Legacy Application

Windows Vista Application

Write to \Windows\App.ini

User Mode

Kernel Mode

Luafv.sys

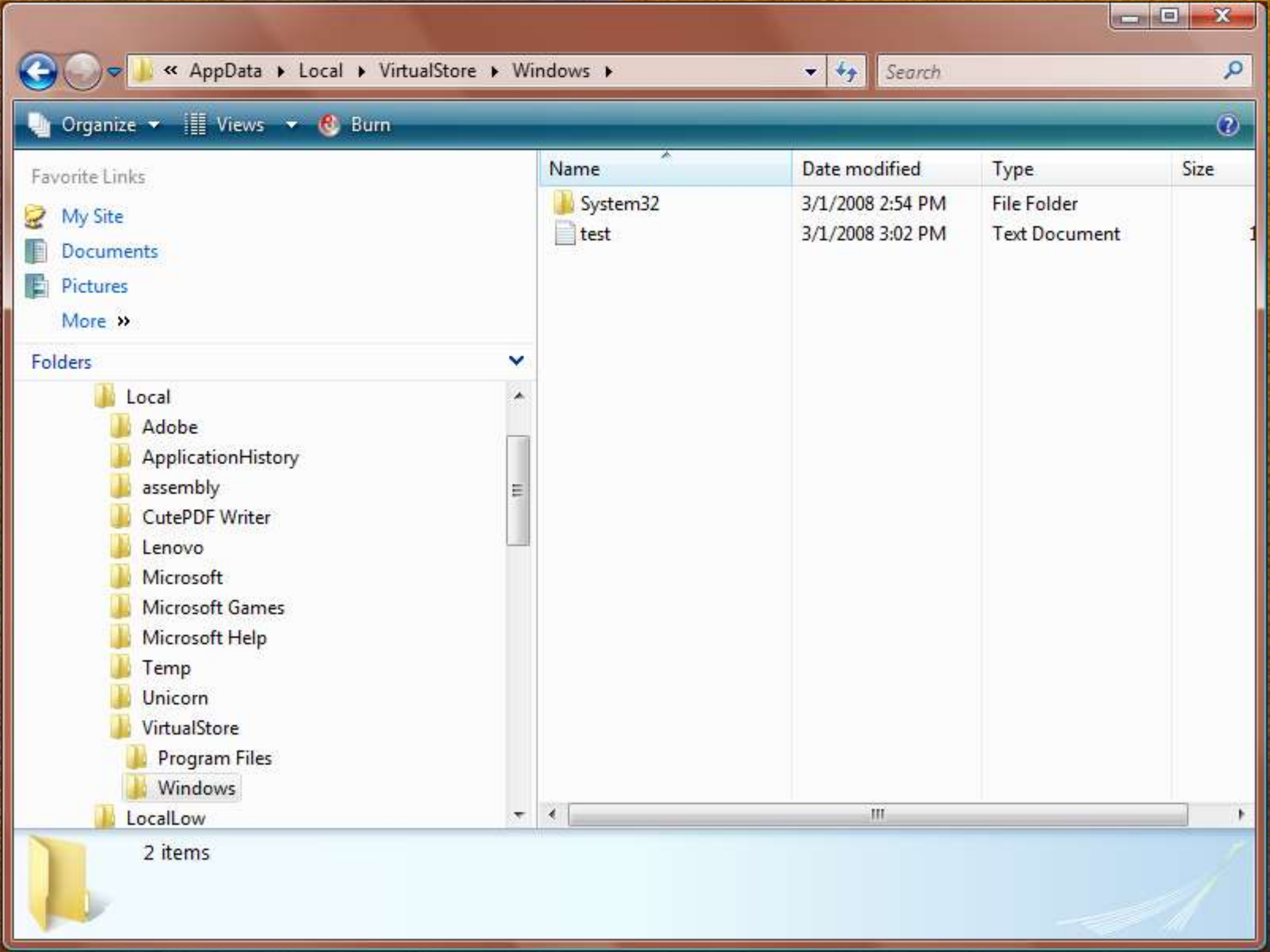
Write to \Users\<user>\AppData\Local\VirtualStore\Windows\App.ini

Write to \App.ini

Ntfs.sys

Access Denied

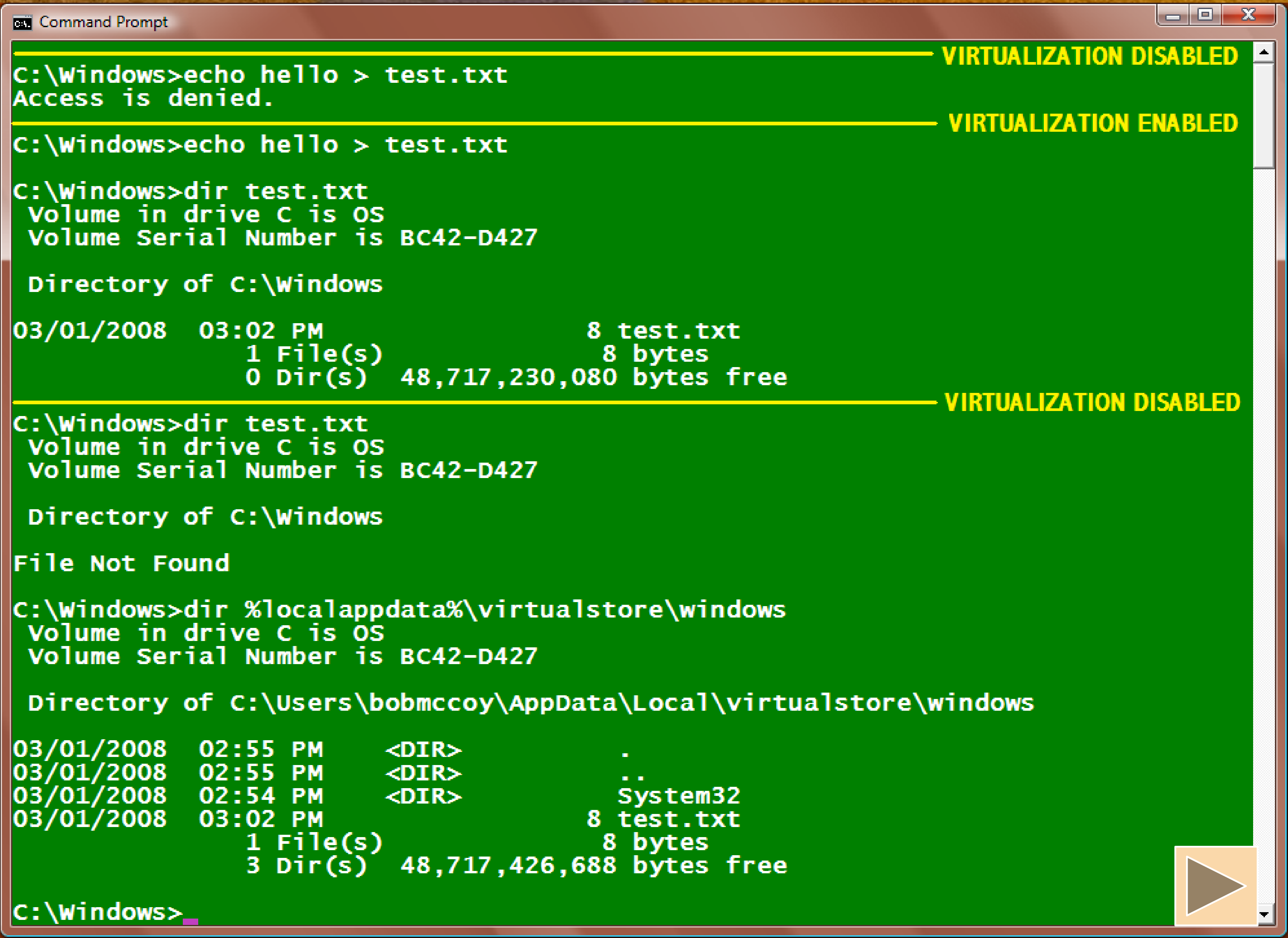
File Virtualization



« AppData ▸ Local ▸ VirtualStore ▸ Windows ▸

Name	Date modified	Type	Size
System32	3/1/2008 2:54 PM	File Folder	
test	3/1/2008 3:02 PM	Text Document	1

2 items



VIRTUALIZATION DISABLED

```
C:\Windows>echo hello > test.txt
Access is denied.
```

VIRTUALIZATION ENABLED

```
C:\Windows>echo hello > test.txt

C:\Windows>dir test.txt
 Volume in drive C is OS
 Volume Serial Number is BC42-D427

 Directory of C:\Windows

03/01/2008  03:02 PM                 8 test.txt
               1 File(s)              8 bytes
               0 Dir(s)  48,717,230,080 bytes free
```

VIRTUALIZATION DISABLED

```
C:\Windows>dir test.txt
 Volume in drive C is OS
 Volume Serial Number is BC42-D427

 Directory of C:\Windows

File Not Found

C:\Windows>dir %localappdata%\virtualstore\windows
 Volume in drive C is OS
 Volume Serial Number is BC42-D427

 Directory of C:\Users\bobmccoy\AppData\Local\virtualstore\windows

03/01/2008  02:55 PM    <DIR>          .
03/01/2008  02:55 PM    <DIR>          ..
03/01/2008  02:54 PM    <DIR>          System32
03/01/2008  03:02 PM                 8 test.txt
               1 File(s)              8 bytes
               3 Dir(s)  48,717,426,688 bytes free

C:\Windows>
```

Registry Virtualization

- Virtualize most of the HKLM\Software branch
- Exceptions:
  - HKLM\Software\Microsoft\Windows
  - HKLM\Software\Microsoft\Windows NT
  - HKLM\Software\Classes
- HKCU\Software\Classes\VirtualStore

Elevation

- Granting a process admin rights
- Admin Approval Mode (AAM)
    - Administrators run as standard users
    - Two identities at login – standard and admin
    - Simple “Continue” – consent elevation
- Over the Shoulder (OTS)
    - Enter alternative admin credentials
- whoami /groups

Vista Admin Groups

- Built-In Administrators
- Certificate Administrators
- Domain Administrators
- Enterprise Administrators
- Policy Administrators
- Schema Administrators
- Domain Controllers
- Enterprise Read-Only Domain Controllers
- Read-Only Domain Controllers
- Account Operators
- Backup Operators
- Cryptographic Operators
- Network Configuration Operators
- Print Operators
- System Operators
- RAS Servers
- Power Users
- Pre-Windows 2000 Compatible Access

Resources

- Inside Windows Vista User Account Control *(by markruss)* http://technet.microsoft.com/en-us/magazine/cc138019.aspx
- Mt.exe *(Windows SDK)* http://msdn.microsoft.com/en-us/library/aa375649.aspx
- Whoami.exe *(Windows 2000 Resource Kit)* http://www.microsoft.com/downloads/details.aspx?familyid=3E89879D-6C0B-4F92-96C4-1016C187D429&displaylang=en
- Application Compatibility Toolkit http://technet.microsoft.com/windowsvista/aa905066.aspx
- LUA Buglight http://blogs.msdn.com/aaron_margosis/archive/2006/08/07/LuaBuglight.aspx
- Process Explorer http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

Resources

- Sigcheck
  http://technet.microsoft.com/en-us/sysinternals/bb897441.aspx
- Understanding and Configuring User Account Control in Windows Vista
  http://technet.microsoft.com/en-us/library/cc709628.aspx
- Windows Client Security and Encryption
  http://technet.microsoft.com/en-us/windows/aa905062.aspx
- User Account Control Step-by-Step Guide
  http://technet.microsoft.com/en-us/library/cc709691.aspx

"The reason we put UAC into the platform was to annoy users. I'm serious," said Cross.

"We needed to change the ecosystem, and we needed a heavy hammer to do it," Cross said.

“Microsoft Exec: UAC Designed To 'Annoy Users‘”

By Kevin McLaughlin, ChannelWeb
April 10, 2008

Microsoft®

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.