User Account Control Overview

Windows Application Quality Team
Microsoft Corporation

Windows 7

User Account Control Goals

- Enable users to run with standard user rights
  - Defend against system changes
  - Reduce impact of malware
  - Defend against compromise if information
- Keep applications working

The Standard User Problem

I am a developer, not a STANDARD user!

Too many apps break as standard user. It's not worth the trouble.

Windows 7

The UAC Solution

- Make it possible for most apps to run
- Remove excuses for running as administrator
- Encourage ISVs to develop for non-admins

UAC for Standard Users

- We fix things
- We allow you to elevate to admin

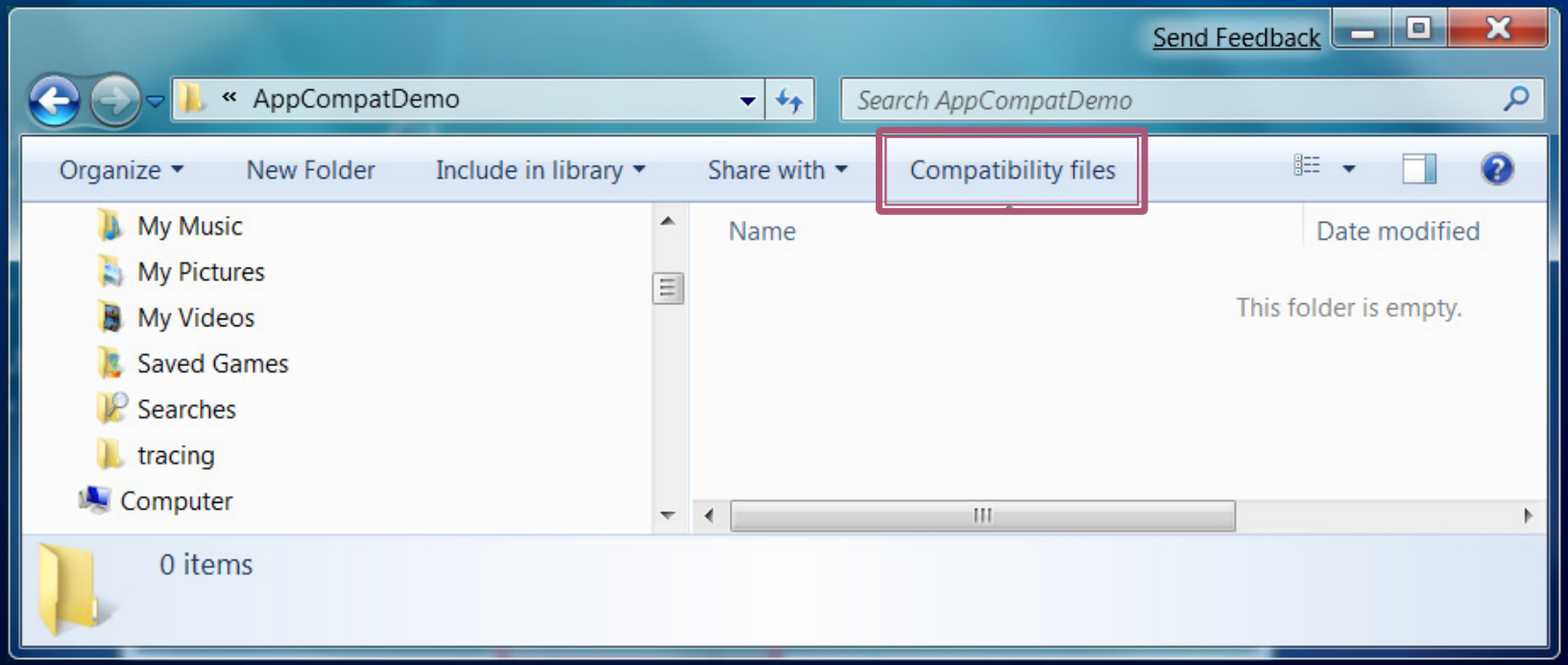
Windows 7

File and Registry Virtualization

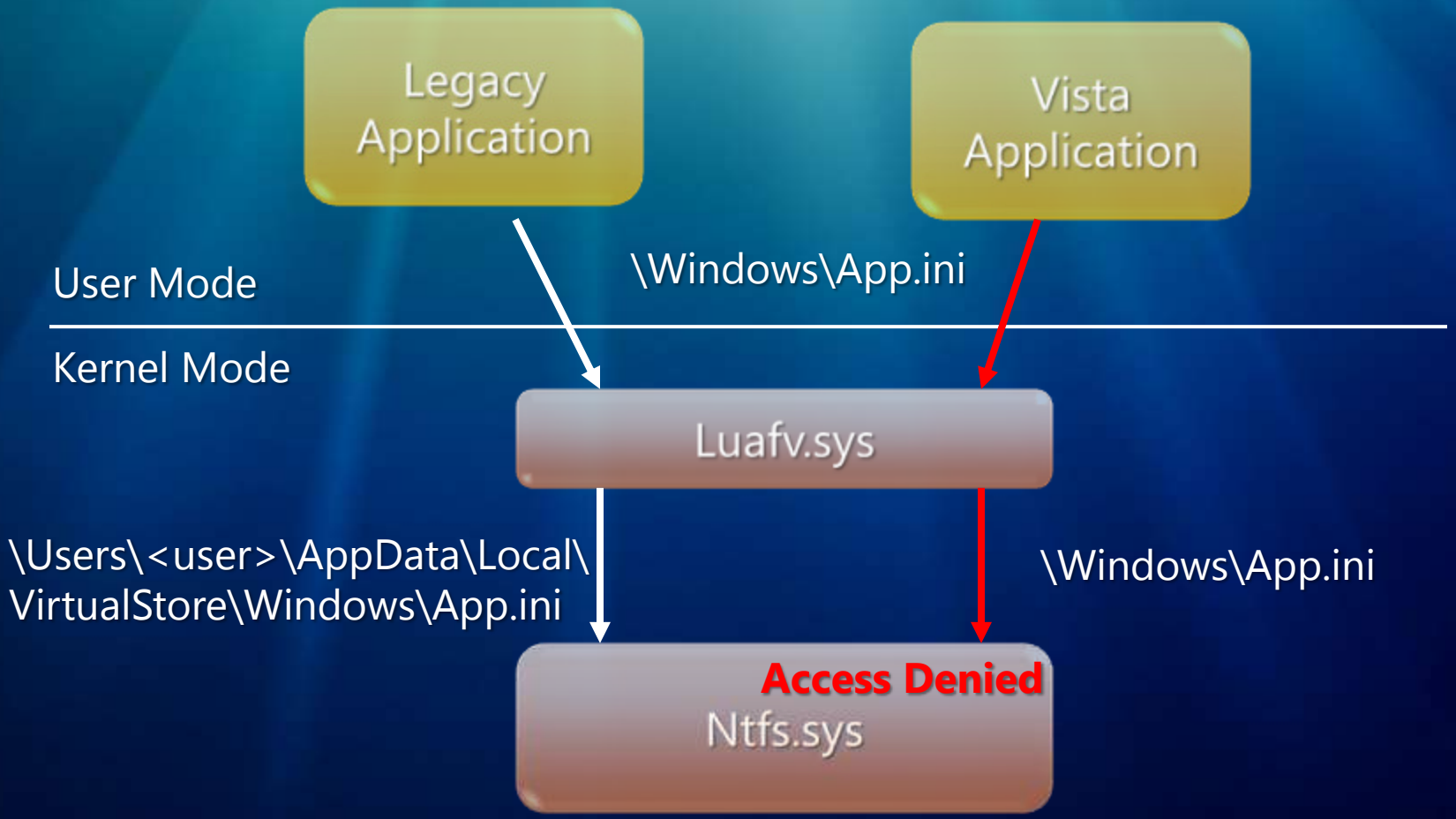
- Client only
- Legacy applications only
- 32-bit applications only
- “Sticky”
- Non-elevated apps only
- Multiple copies of files
- Doesn’t apply to executable files

File Virtualization

- c:\program files
- c:\programdata
- c:\windows



File Virtualization

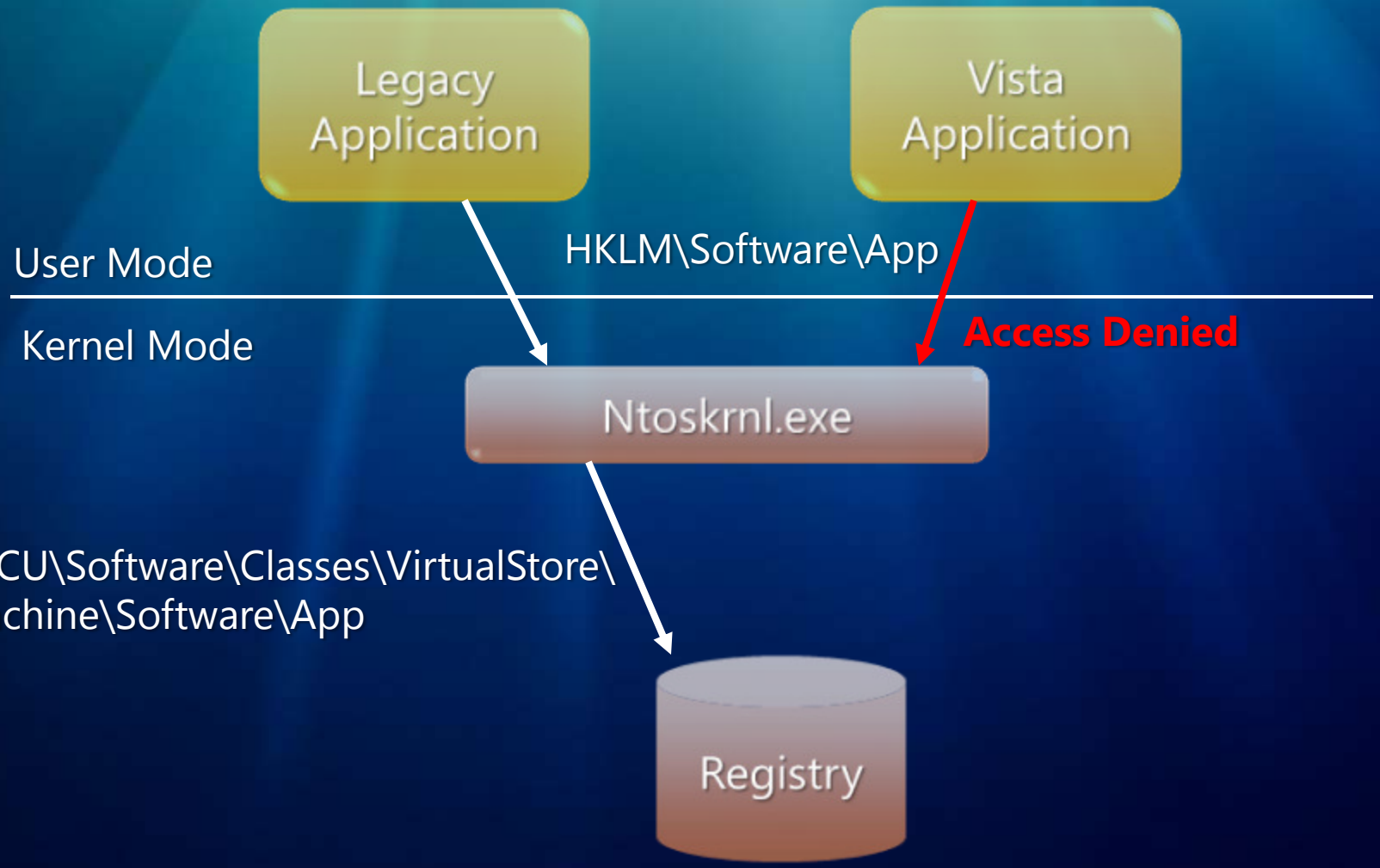


Windows 7

Registry Virtualization

- HKEY_LOCAL_MACHINE\Software

Registry Virtualization



Windows 7

File Virtualization

demo

Windows 7

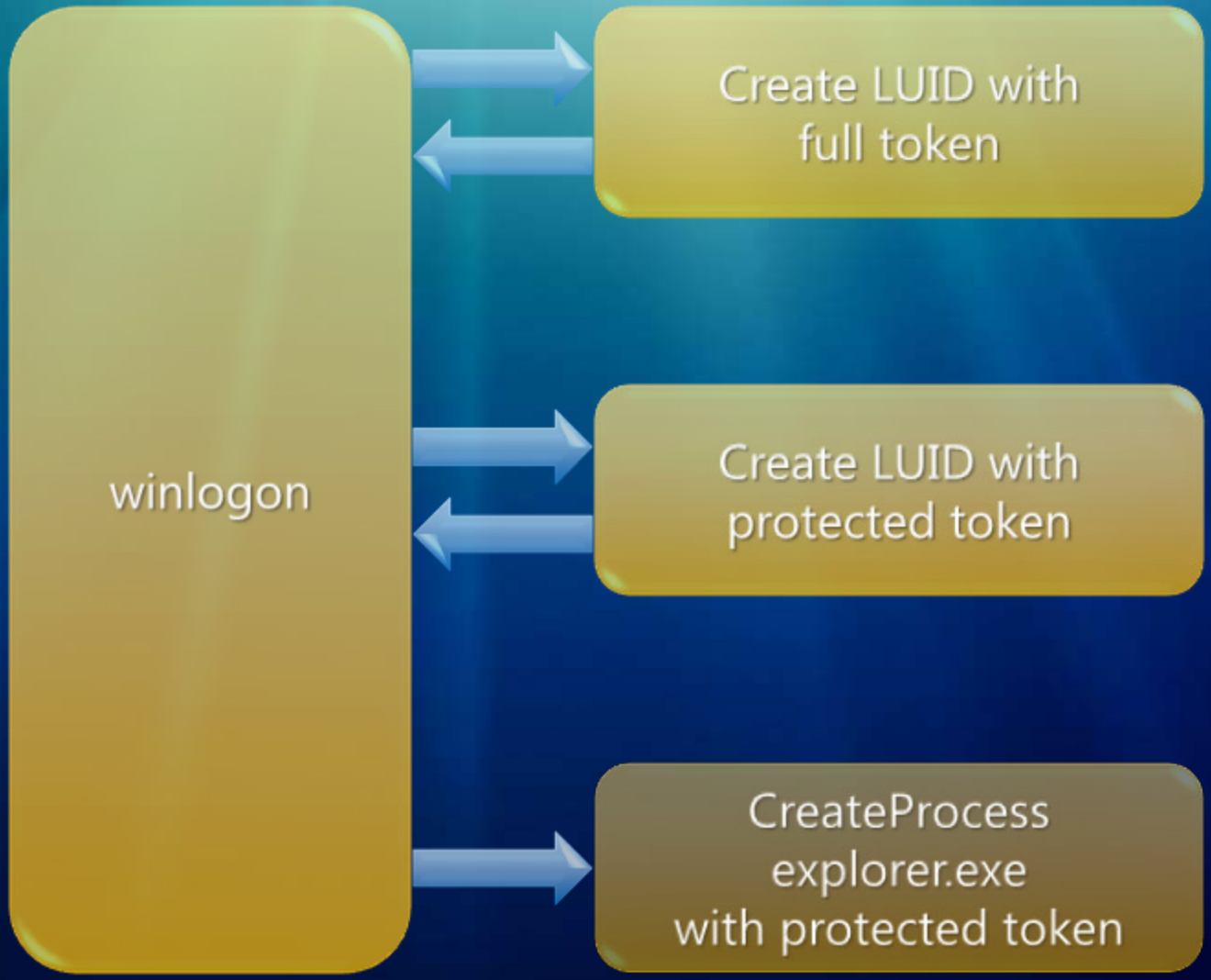
UAC for Administrators

- We fix things
- We let you run with fewer rights
- We let you elevate to full rights

The Split Token

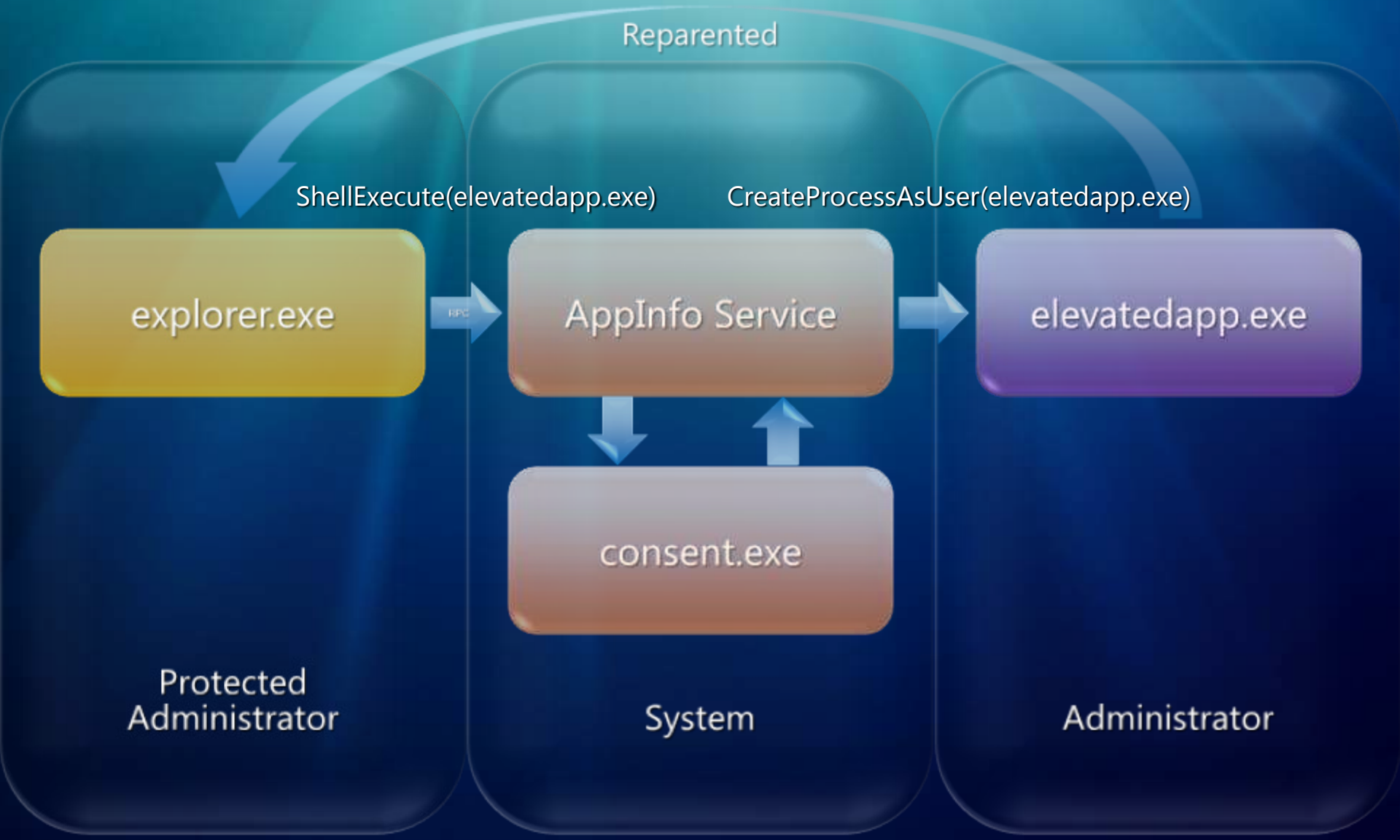
- Run with fewer rights most of the time
- Conveniently elevate when you need rights
- Applies to interactive logons only

Creating the Split Token



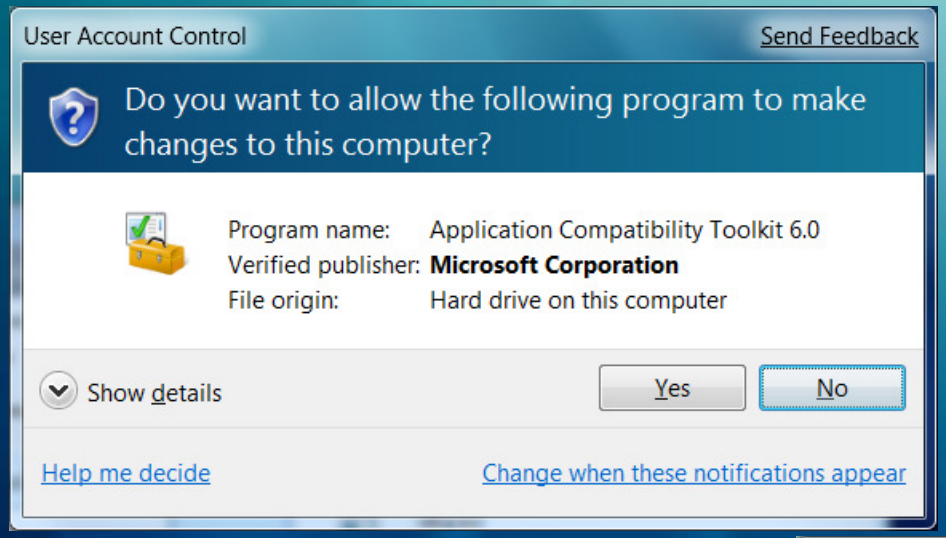
Windows 7

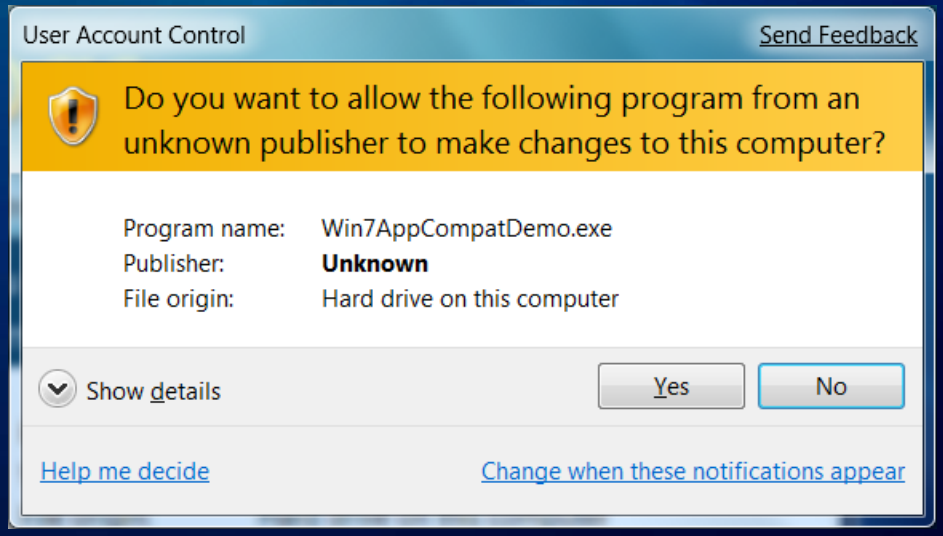
UAC OTS Elevation



Windows 7

UAC: OTS Dialogs





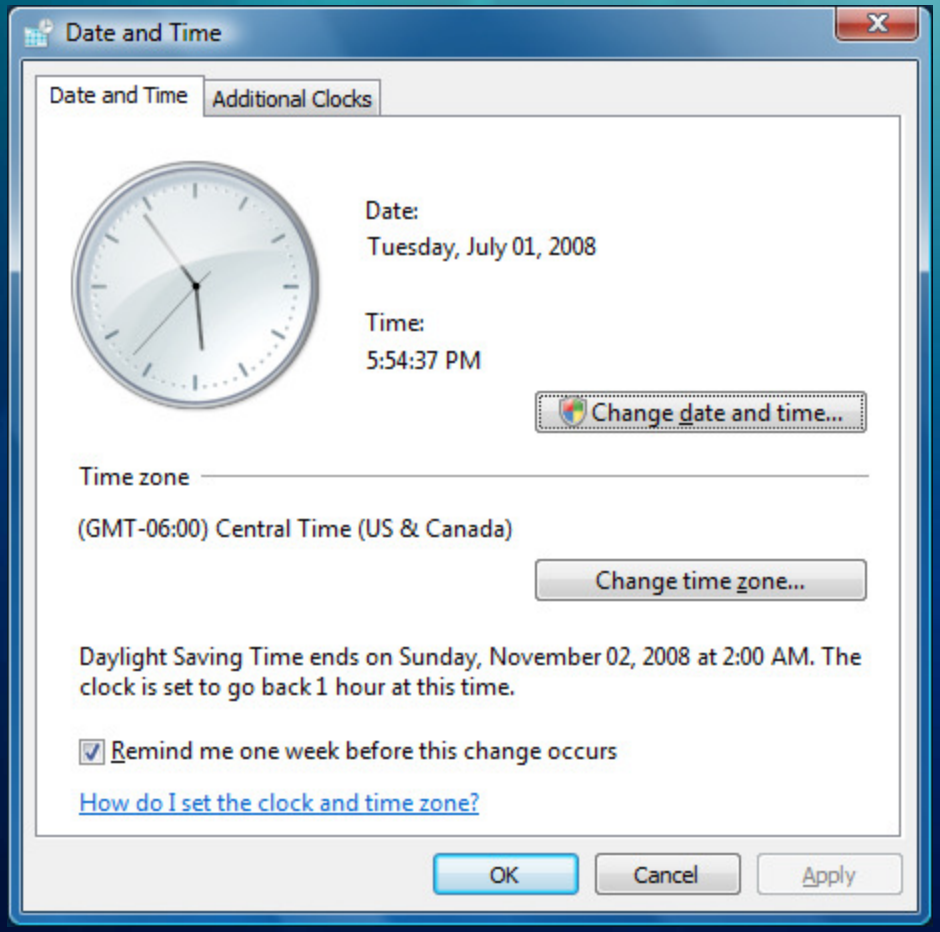
Windows 7

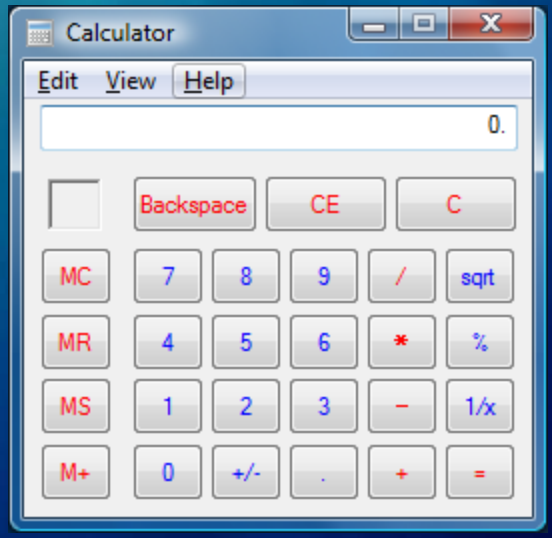
UAC Split Tokens

demo

Windows 7

Standard User Platform Fixes





Windows 7

Setup Detection

- Why is my app running elevated?
  - We think it's an installer!
- Specific Installer
- Generic Installer
- Specific Noninstaller

Windows 7

Setup Detection

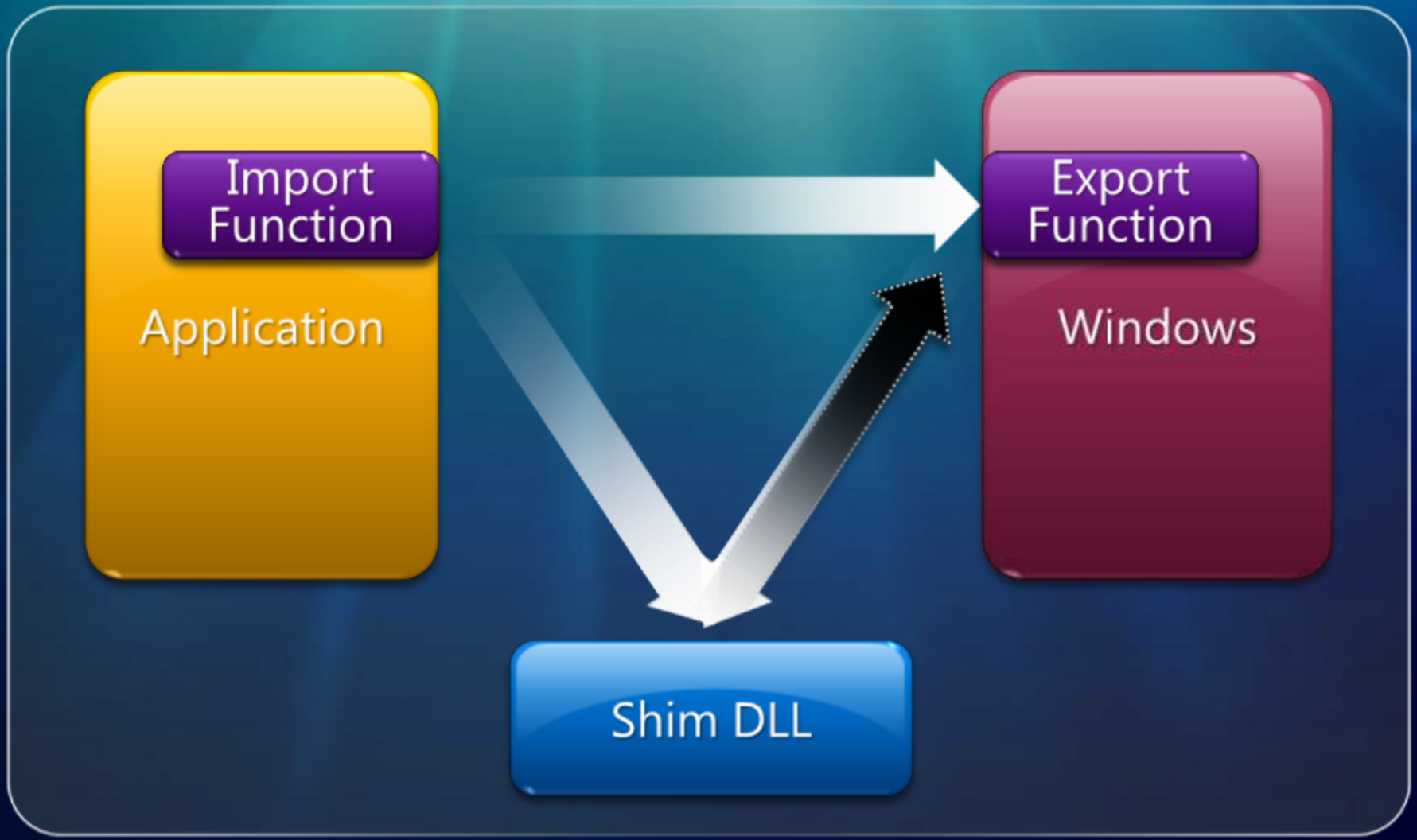
demo

Windows 7

The "Standard User Quick Test"

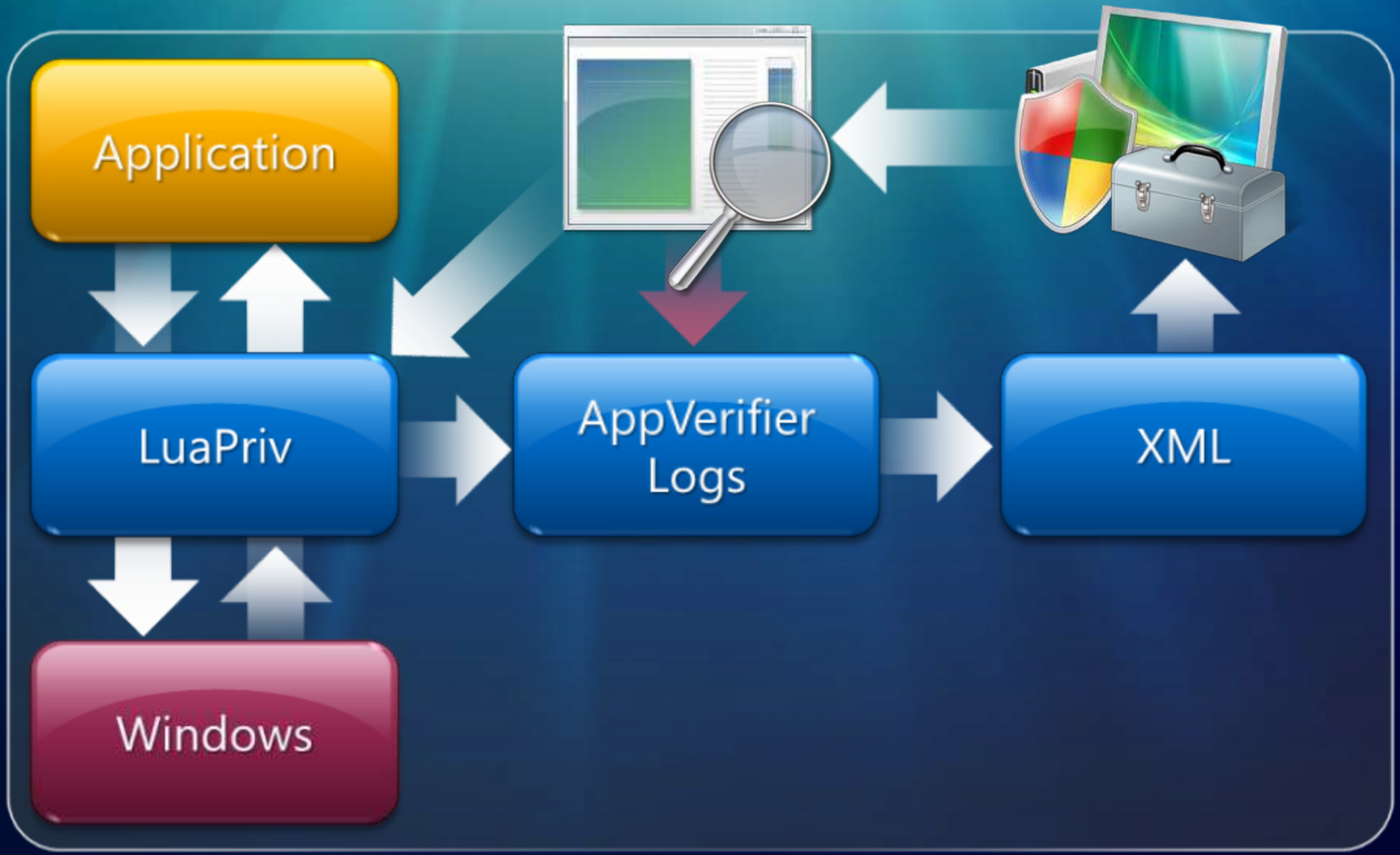
- Run it elevated – does it work?
  - If so, investigate

How Shims Work



Windows 7

Standard User Analyzer



SUA Mitigations

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

ElevateCreateProcess

Symptoms

ERROR_ELEVATION_REQUIRED

Fix description

Tries again, requesting elevation

Windows 7

ForceAdminAccess

Symptoms

Fails explicit administrator check

Fix description

Lies

ForceAdminAccess Shim for IsUserAnAdmin:

```
return TRUE;
```

LocalMappedObject

Symptoms

Can’t create in Global namespace

Fix description

Creates in Local namespace

Windows 7

VirtualizeDeleteFile

Symptoms

Can’t delete files

Fix description

Pretends to delete files

Windows 7

VirtualizeHKCRLite

Symptoms

Can’t register COM components

Fix description

Registers them per-user

VirtualizeRegisterTypeLib

Symptoms

Registering type library fails

Fix description

Registers type library per-user

Windows 7

SUA Mitigations

demo

Windows 7

UAC Manifests

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<assembly xmlns="urn:schemas-microsoft-com:asm.v1"
manifestVersion="1.0">
  <assemblyIdentity type="win32" processorArchitecture="*"
       version="1.0.0.0" name="MyApplication.exe"/>
  <description>My totally sweet Vista application</description>
  <ms_asmv2:trustInfo xmlns:ms_asmv2="urn:schemas-microsoft-
       com:asm.v2">
    <ms_asmv2:security>
      <ms_asmv2:requestedPrivileges>
        <ms_asmv2:requestedExecutionLevel level="asInvoker ||
        highestAvailable || requireAdministrator"/>
      </ms_asmv2:requestedPrivileges>
    </ms_asmv2:security>
  </ms_asmv2:trustInfo>
</assembly>
```

UAC Manifests

- Windows Vista: internal > external
- You didn't write code -> don't manifest
- Removes compatibility features / shims
- mt.exe
- Visual Studio 2008 native support

Checking for Admin in Code

- IsUserAnAdmin?
- GetTokenInformation?
  - TokenElevationType:
    - Default
    - Full
    - Limited
- Best solution: factor and manifest

Windows 7

Run Levels

- RequireAdministrator
- HighestAvailable
- AsInvoker

Windows 7

RunAsAdmin

Symptoms

Requires admin

Fix description

Prompts for elevation

RunAsHighest

Symptoms

Had both admin and standard user views

Fix description

Provides most powerful token

RunAsInvoker

Symptoms

Prompting unnecessarily

Fix description

No more prompt

SpecificInstaller

Symptoms

Not fixed as a legacy setup

Fix description

Flags it as a legacy setup

SpecificNonInstaller

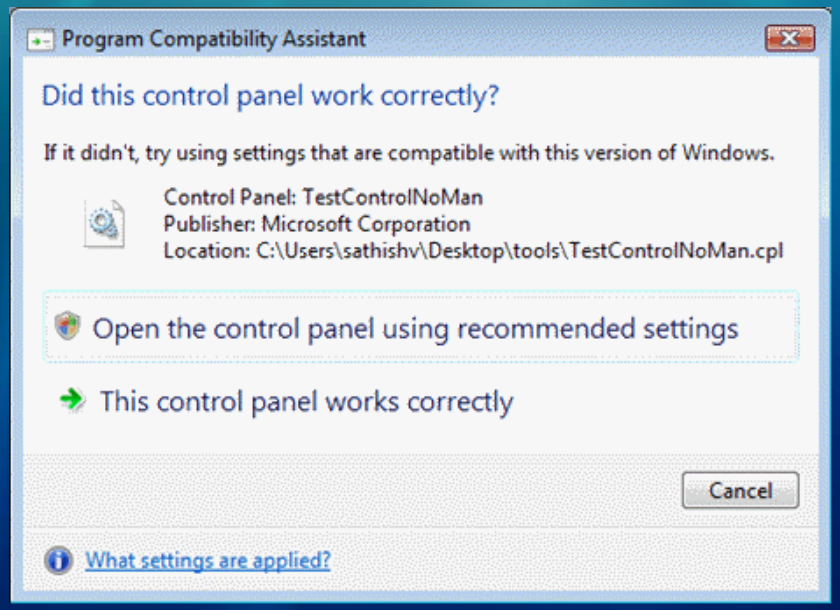
Symptoms

Flagged as a legacy setup inappropriately

Fix description

No longer flagged as a legacy setup

Don't Forget Legacy CPL…



Windows 7

Run Level Specification

demo

Windows 7

Microsoft®

Your potential. Our passion.™

© 2009 Microsoft Corporation. All rights reserved. Microsoft, Windows, Windows 7 and other product names are or may be registered trademarks and/or trademarks in the U.S. and/or other countries.
The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation.
MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.

Windows 7