Bundesamt
für Sicherheit in der
Informationstechnik

Neue Sicherheitseigenschaften von Windows 7

Thomas Caspers

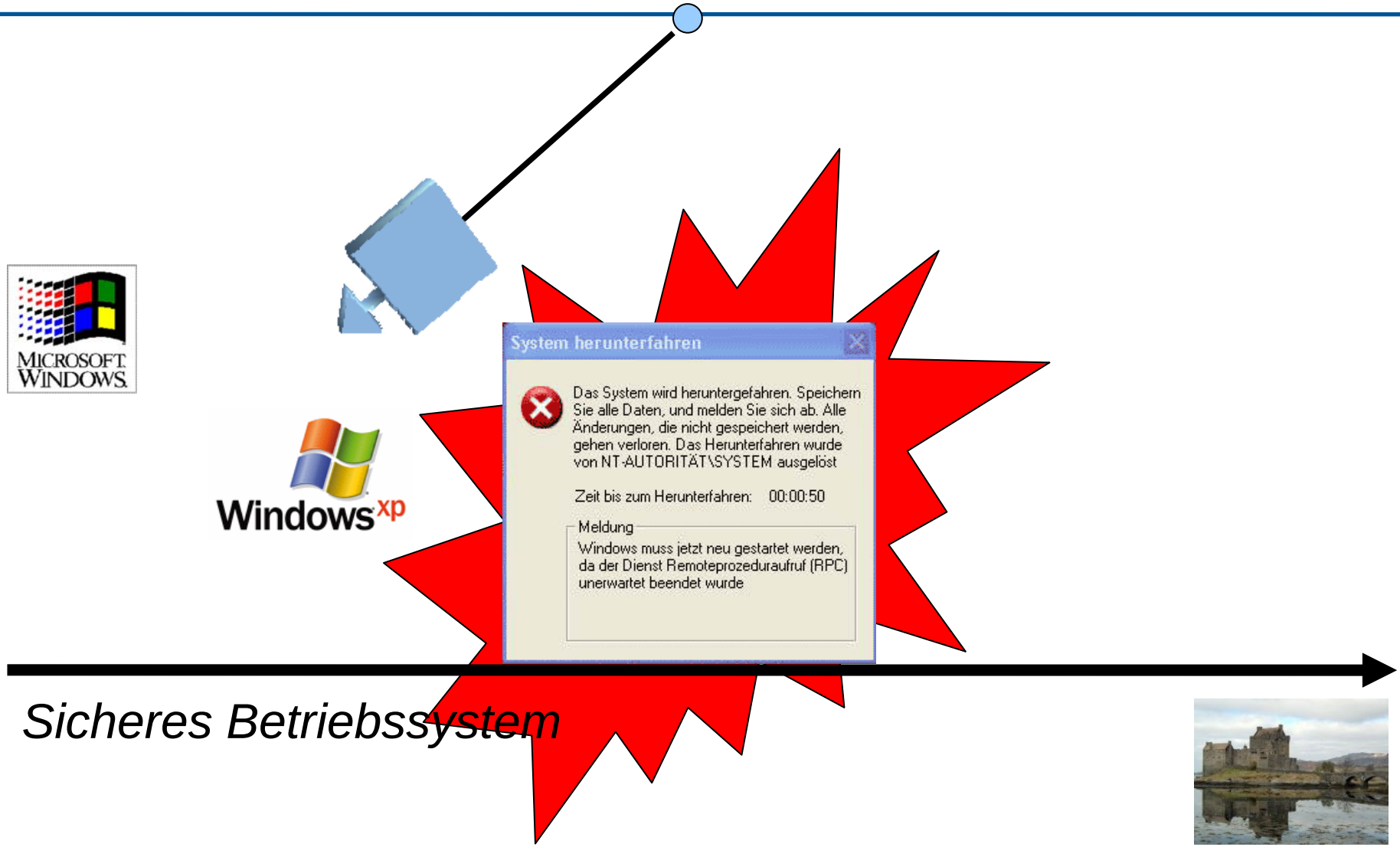
Bundesamt für Sicherheit in der Informationstechnik

1. Workshop: Betriebssystemsicherheit
4./5. Dezember 2008, Universität der Bundeswehr München

Geschichtliches

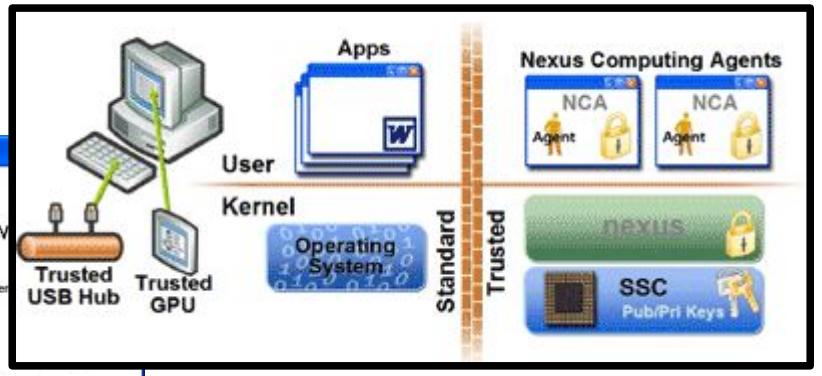
Sicheres Betriebssystem

Geschichtliches



Sicheres Betriebssystem

Geschichtliches



Sicheres Betriebssystem

Geschichtliches

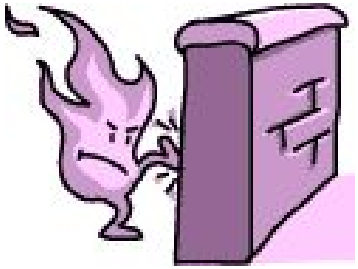
Sicheres Betriebssystem

Geschichtliches

Windows 7

Sicheres Betriebssystem

Ausgangspunkt für Windows 7: Sicherheitsfunktionen von Vista



- BitLocker Drive Encryption (BDE)
- Benutzerkontensteuerung (UAC)
- Windows Integritätsmechanismus (WIM)
- Dateisystem- und Registry-Virtualisierung
- Windows Resource Protection (WRP)
- Speicher-Randomisierung (ASLR)
- Datenausführungsverhinderung (DEP)
- USB Device Control
- Windows Firewall
- Windows Defender (Spyware-Schutz)
- Internet Explorer 7 im geschützten Modus

Ergänzungen durch das Service Pack 1 für Vista

- Win32-APIs für die Datenausführungsverhinderung (DEP)
- Deaktivierung des Reduced Functionality Modes
- Erweiterungen der BitLocker Drive Encryption
  - Authentisierung mit TPM, PIN und USB-Token
  - Verschlüsselung von Datenpartitionen
- Fehlerbehebungen bei der BitLocker Drive Encryption
- Neuer Zufallszahlengenerator
- Verbesserte Smartcard-Unterstützung

Quelle: *http://technet.microsoft.com/en-us/library/cc709618.aspx*

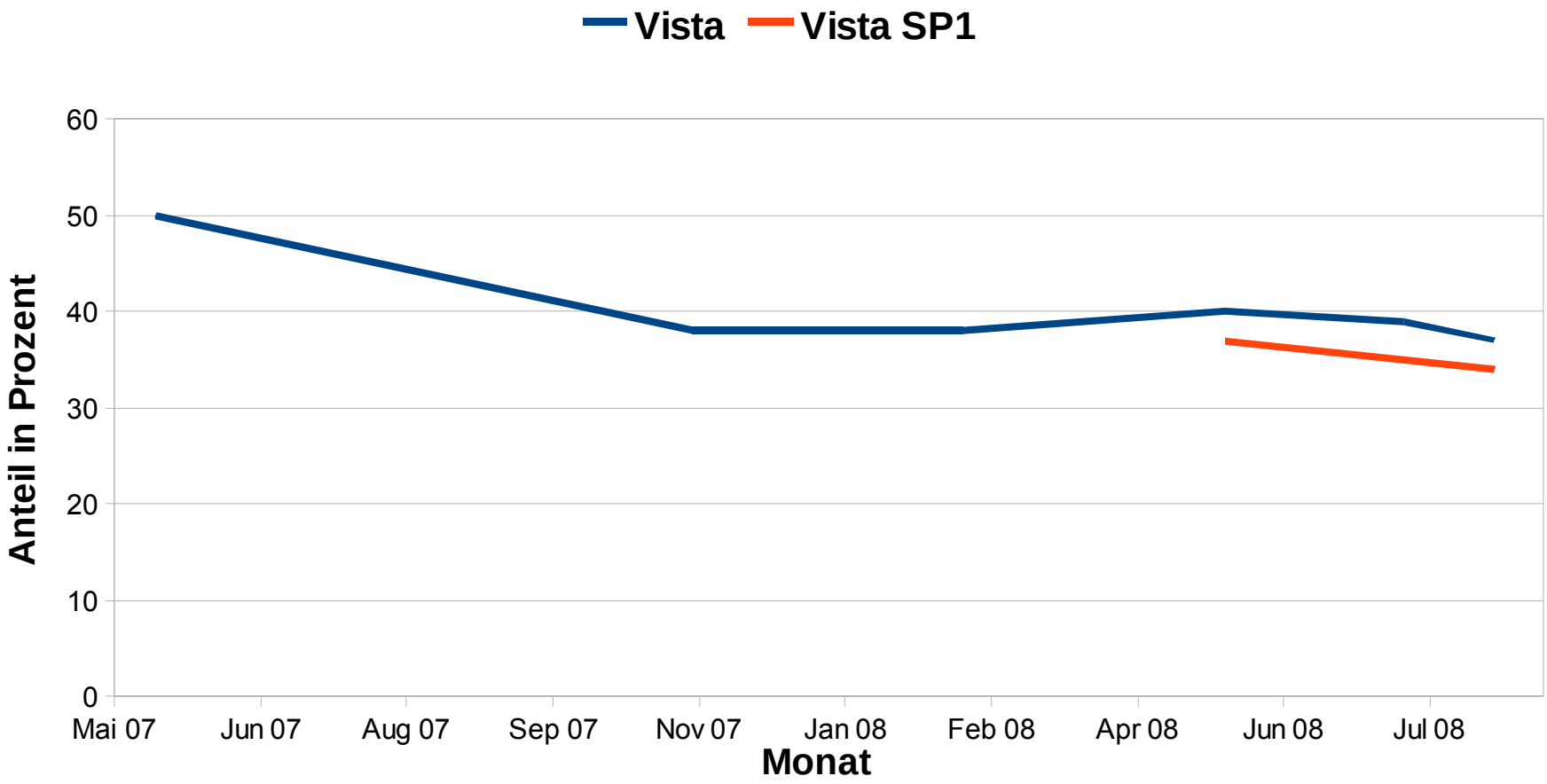
by Denise Begley (Creative Commons Attribution 2.0 Generic)

Benutzerkontensteuerung unter Vista

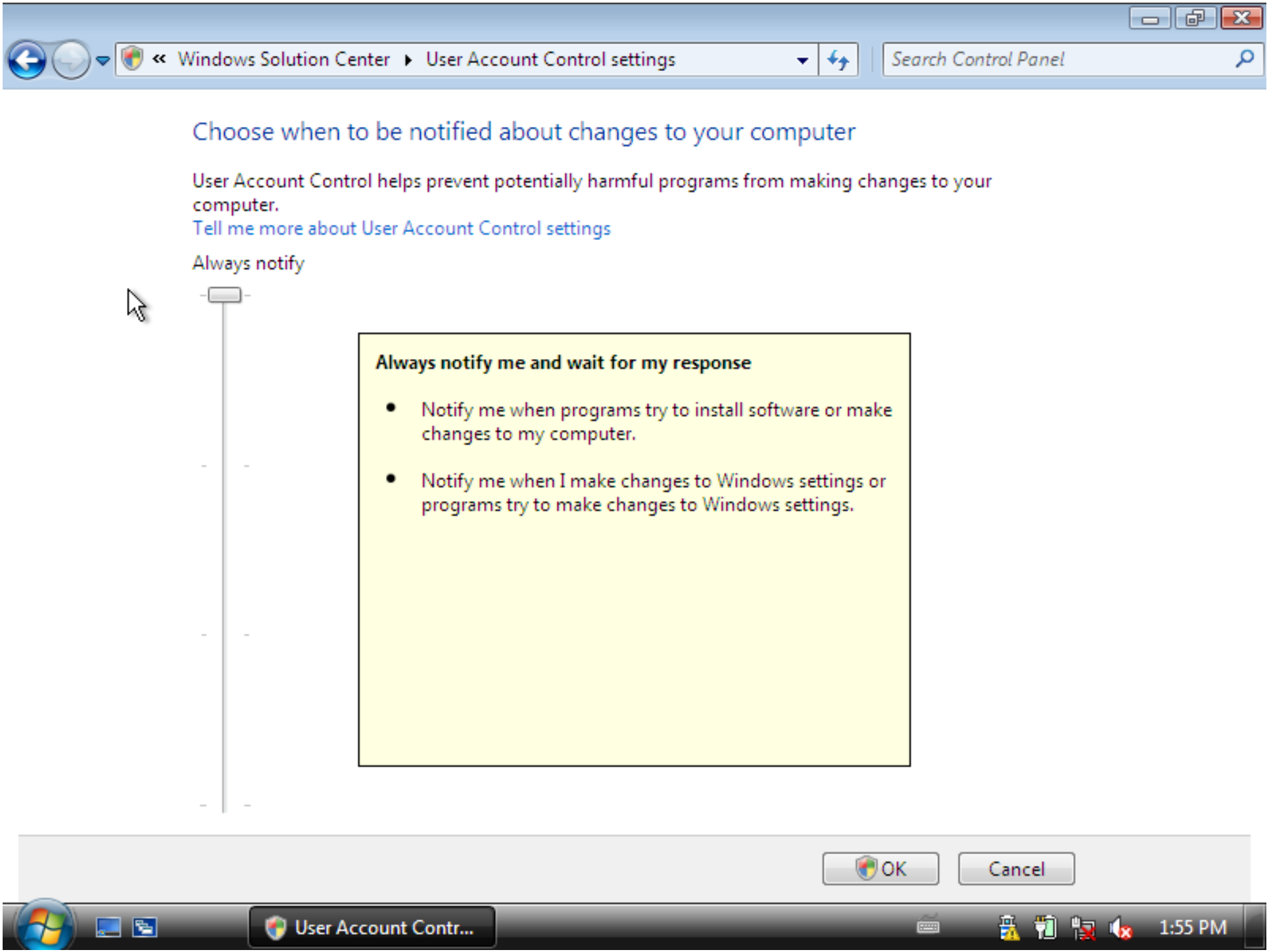
- Benutzerkontensteuerung (User Account Control, UAC) unter Vista verfolgt die Ziele
  - Software auch unter „Nicht-Admin-Bedingungen“ lauffähig zu halten
  - Benutzern begründete Entscheidungen zu Veränderungen am Betriebssystem zu erlauben

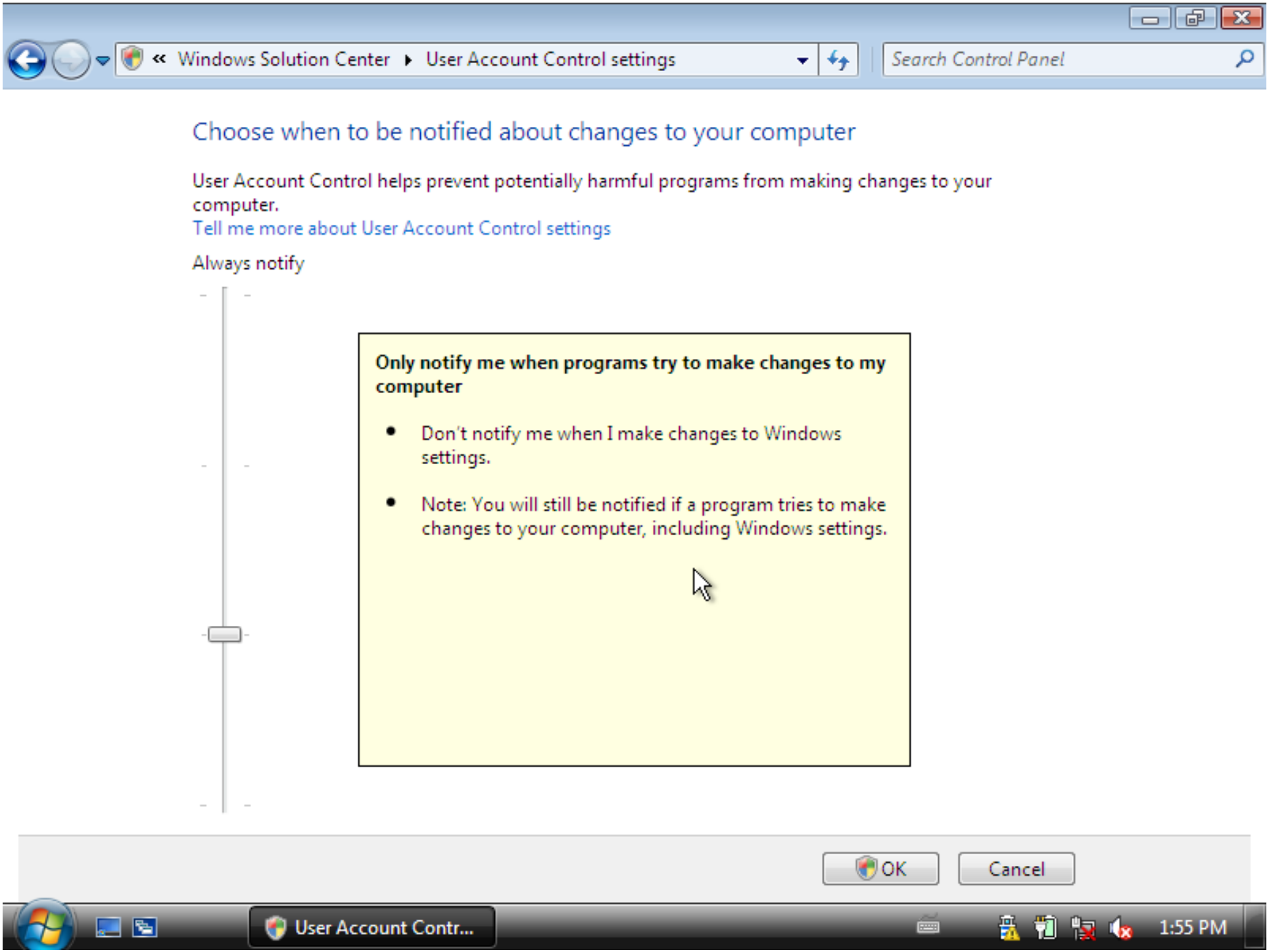
Benutzerkontensteuerung unter Vista

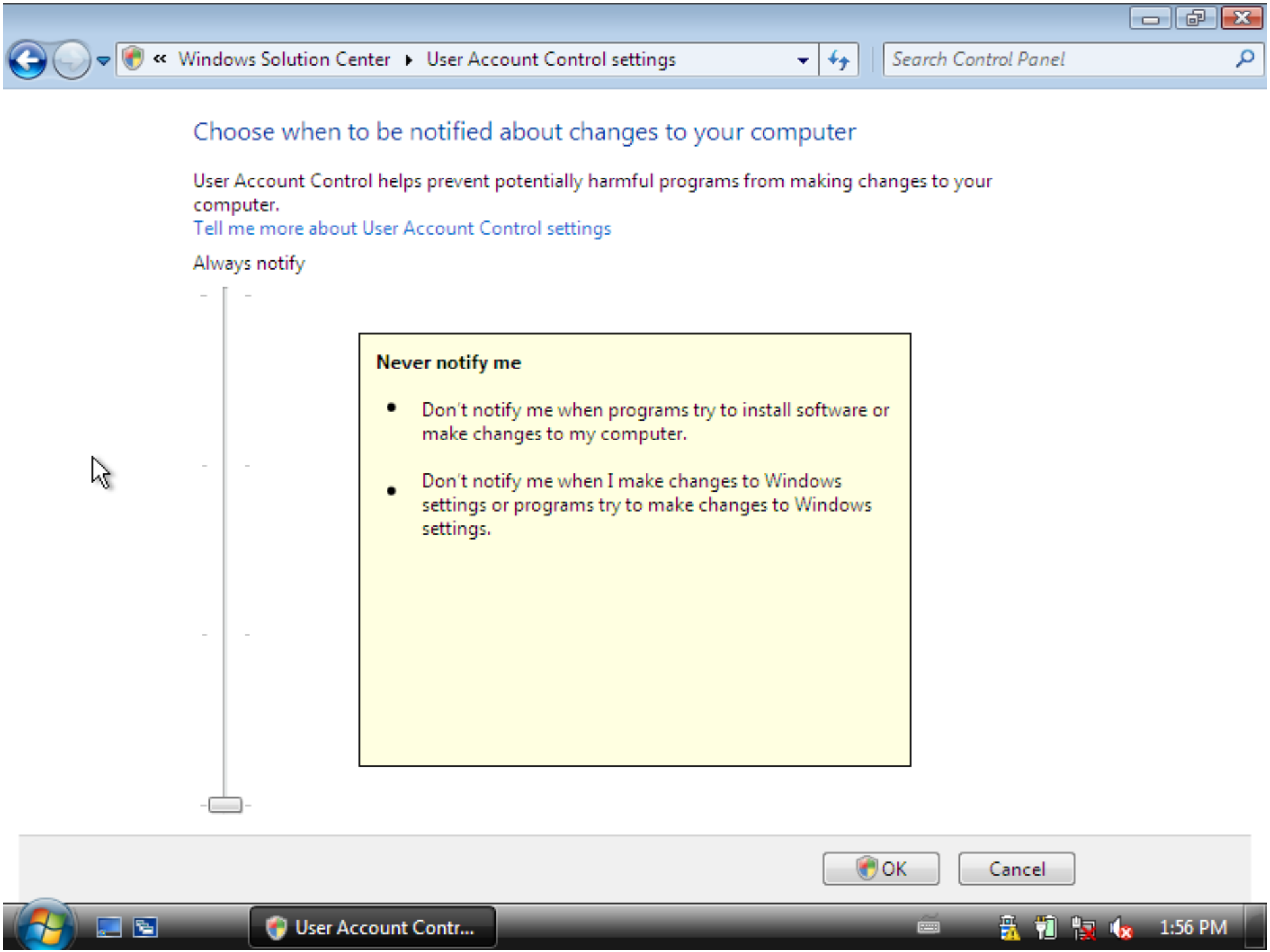
Anteil der Sitzungen mit UAC-Meldungen



Quelle: *http://blogs.msdn.com/e7/*


« Windows Solution Center ▸ User Account Control settings
Search Control Panel
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Always notify me and wait for my response
Notify me when programs try to install software or make changes to my computer.
Notify me when I make changes to Windows settings or programs try to make changes to Windows settings.
OK
Cancel
User Account Contr...
1:55 PM


« Windows Solution Center ▸ User Account Control settings
Search Control Panel
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Only notify me when programs try to make changes to my computer
Don't notify me when I make changes to Windows settings.
Note: You will still be notified if a program tries to make changes to your computer, including Windows settings.
OK
Cancel
User Account Contr...
1:55 PM


« Windows Solution Center ▸ User Account Control settings
Search Control Panel
Choose when to be notified about changes to your computer
User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings
Always notify
Never notify me
Don't notify me when programs try to install software or make changes to my computer.
Don't notify me when I make changes to Windows settings or programs try to make changes to Windows settings.
OK
Cancel
User Account Contr...
1:56 PM

Benutzerkontensteuerung und MS08-067

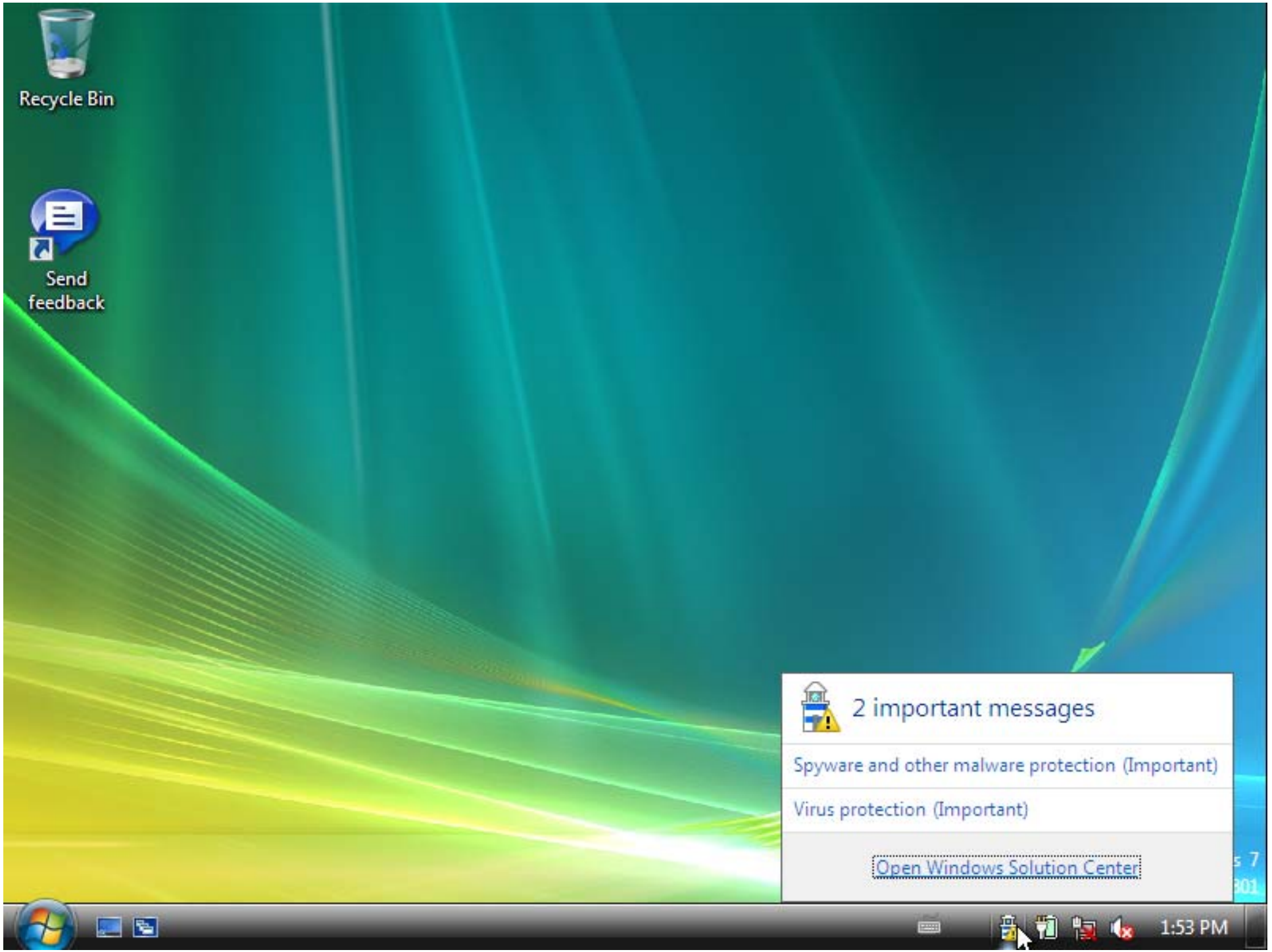
Vulnerability Severity Rating and Maximum Security Impact by Affected Software		
Affected Software	**Server Service Vulnerability - CVE-2008-4250**	**Aggregate Severity Rating**
Microsoft Windows 2000 Service Pack 4	**Critical** Remote Code Execution	**Critical**
Windows XP Service Pack 2 and Windows XP Service Pack 3	**Critical** Remote Code Execution	**Critical**
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2	**Critical** Remote Code Execution	**Critical**
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2	**Critical** Remote Code Execution	**Critical**
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2	**Critical** Remote Code Execution	**Critical**
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems	**Critical** Remote Code Execution	**Critical**
Windows Vista and Windows Vista Service Pack 1	**Important** Remote Code Execution	**Important**
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1	**Important** Remote Code Execution	**Important**
Windows Server 2008 for 32-bit Systems*	**Important** Remote Code Execution	**Important**
Windows Server 2008 for x64-based Systems*	**Important** Remote Code Execution	**Important**
Windows Server 2008 for Itanium-based Systems	**Important** Remote Code Execution	**Important**

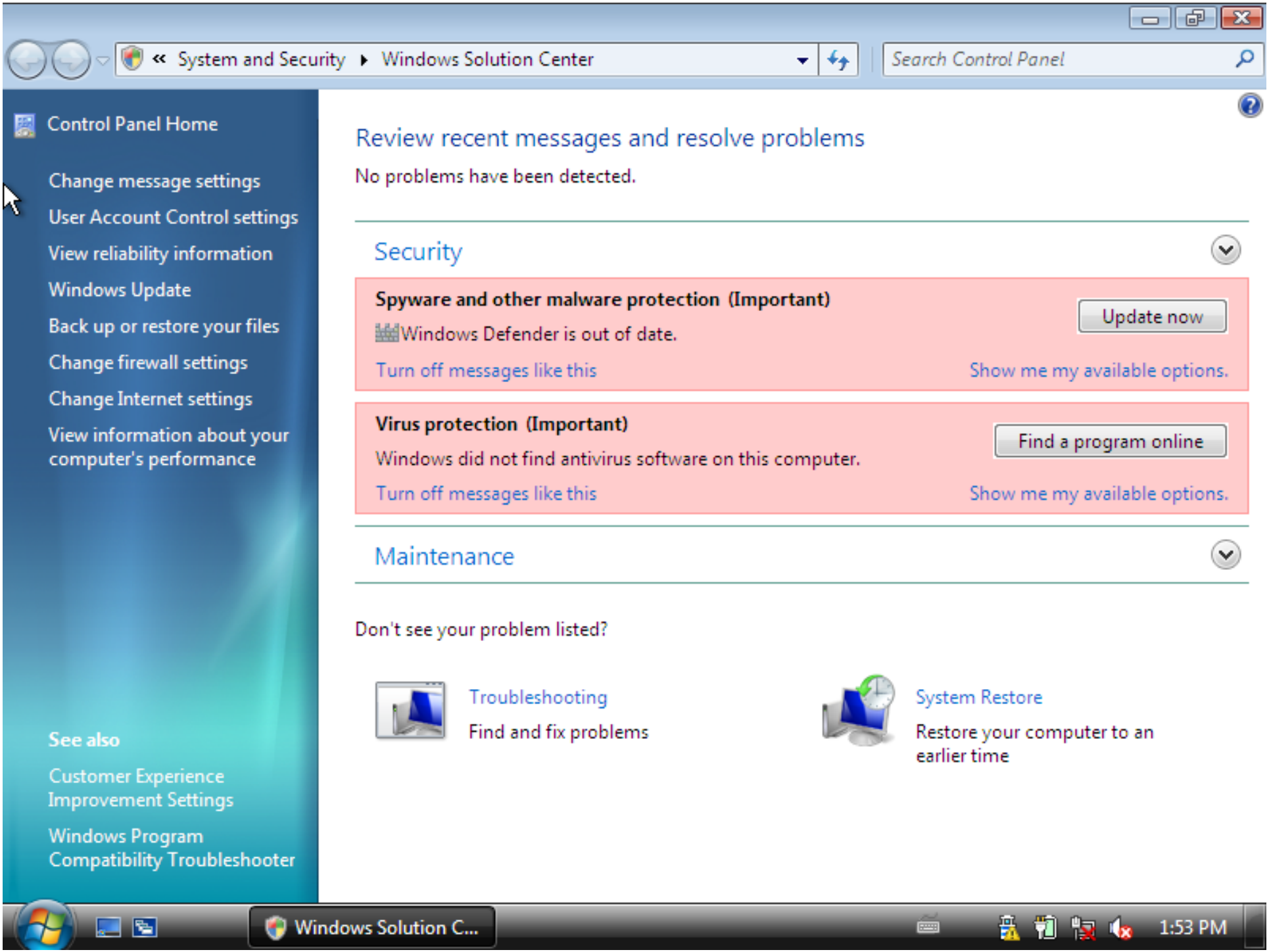
Benutzerkontensteuerung und MS08-067

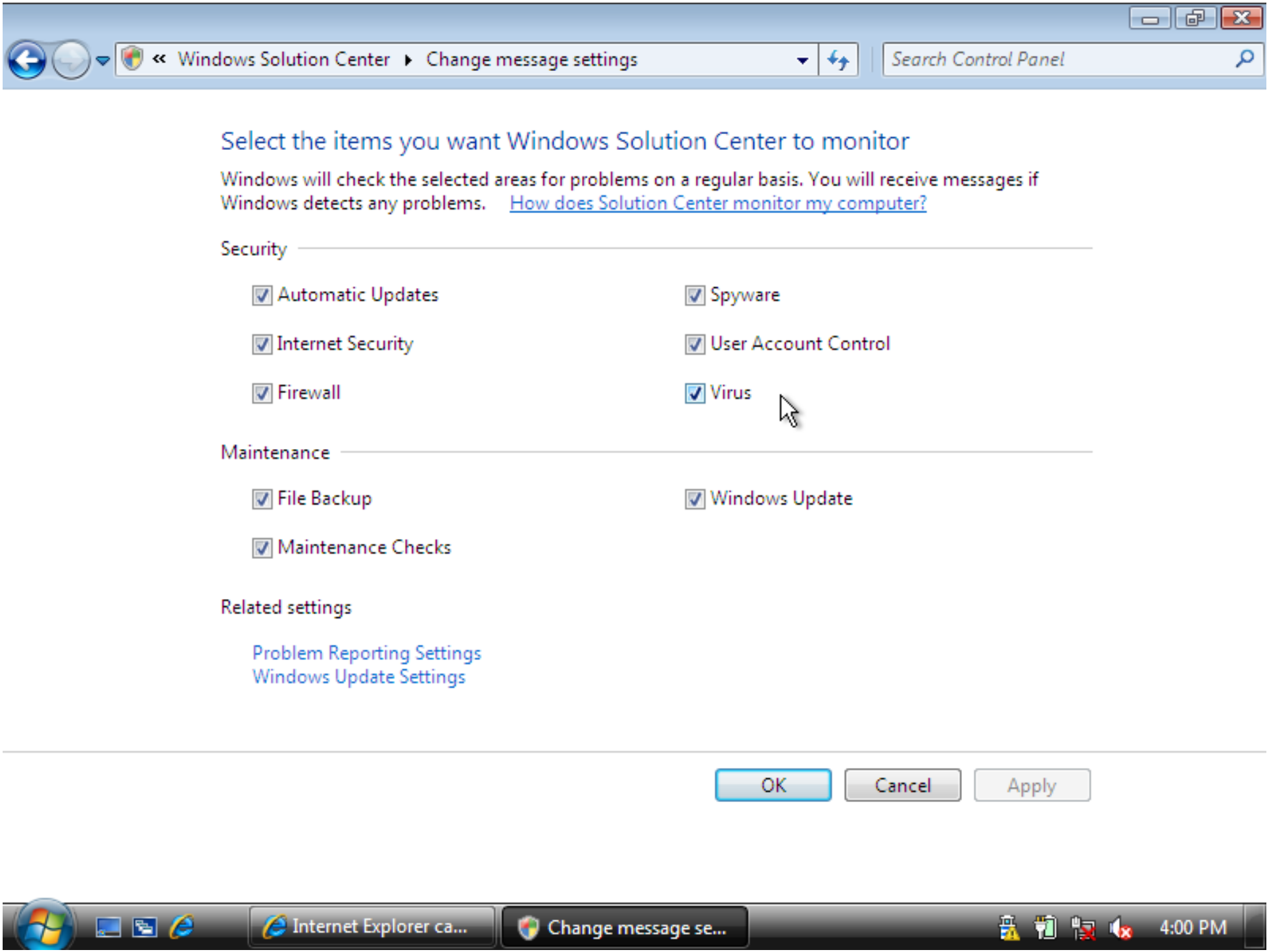
Vulnerability Severity Rating and Max
Affected Software
Microsoft Windows 2000 Service Pack 4
Windows XP Service Pack 2 and Windows XP Service Pack 3
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium-based Systems
Windows Vista and Windows Vista Service Pack 1
Windows Vista x64 Edition and Windows Vista x64 Edition Service Pack 1
Windows Server 2008 for 32-bit Systems*
Windows Server 2008 for x64-based Systems*
Windows Server 2008 for Itanium-based Systems


Recycle Bin
Send feedback
2 important messages
Windows 7
only. Build 6801
1:51 PM


Recycle Bin
Windows 7
2 important messages
1:51 PM
Windows 7
2 important messages
1:51 PM

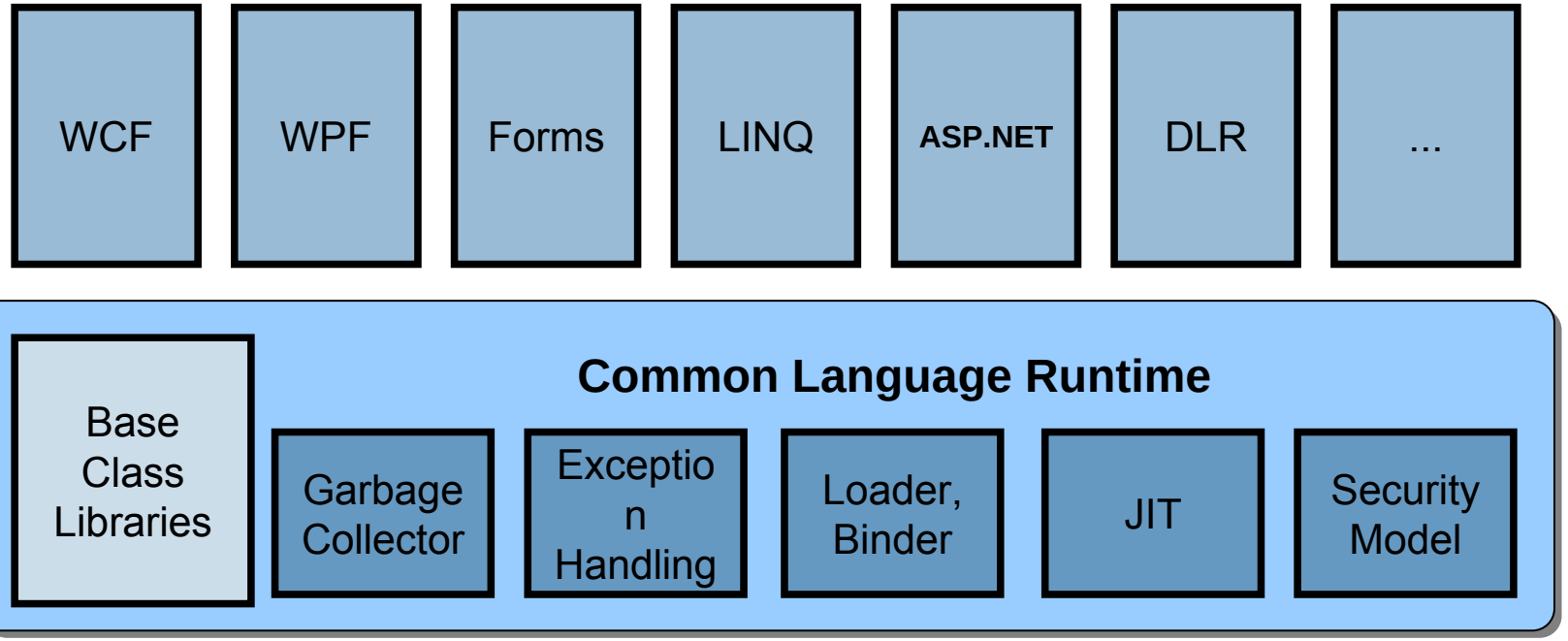

Recycle Bin
Send feedback
2 important messages
Spyware and other malware protection (Important)
Virus protection (Important)
Open Windows Solution Center
1:53 PM


« System and Security ▸ Windows Solution Center
Search Control Panel
Control Panel Home
Change message settings
User Account Control settings
View reliability information
Windows Update
Back up or restore your files
Change firewall settings
Change Internet settings
View information about your computer's performance
See also
Customer Experience Improvement Settings
Windows Program Compatibility Troubleshooter
Review recent messages and resolve problems
No problems have been detected.
Security
Spyware and other malware protection (Important)
Windows Defender is out of date.
Update now
Turn off messages like this
Show me my available options.
Virus protection (Important)
Windows did not find antivirus software on this computer.
Find a program online
Turn off messages like this
Show me my available options.
Maintenance
Don't see your problem listed?
Troubleshooting
Find and fix problems
System Restore
Restore your computer to an earlier time
Windows Solution C...
1:53 PM


« Windows Solution Center ▸ Change message settings
Search Control Panel
Select the items you want Windows Solution Center to monitor
Windows will check the selected areas for problems on a regular basis. You will receive messages if Windows detects any problems.
How does Solution Center monitor my computer?
Security
Automatic Updates
Spyware
Internet Security
User Account Control
Firewall
Virus
Maintenance
File Backup
Windows Update
Maintenance Checks
Related settings
Problem Reporting Settings
Windows Update Settings
OK
Cancel
Apply
Internet Explorer ca...
Change message se...
4:00 PM

.NET Framework

- .NET 3.0 ist in Windows Vista enthalten
- Aktuelle Version: .NET Framework 3.5 Service Pack 1
  - Wird über Windows Update verteilt (ab XP mit .NET 2.0)



.NET Framework Sicherheitsmodell

- Pragmatische Änderung:
  .NET Framework 3.5 SP1 Allows managed code to be launched from a network share!

  Quelle: *http://blogs.msdn.com/vancem/archive/2008/08/13/net-framework-3-5-sp1-allows-managed-code-to-be-launched-from-a-network-share.aspx*

- Tatsächlich:
  FullTrust on the LocalIntranet

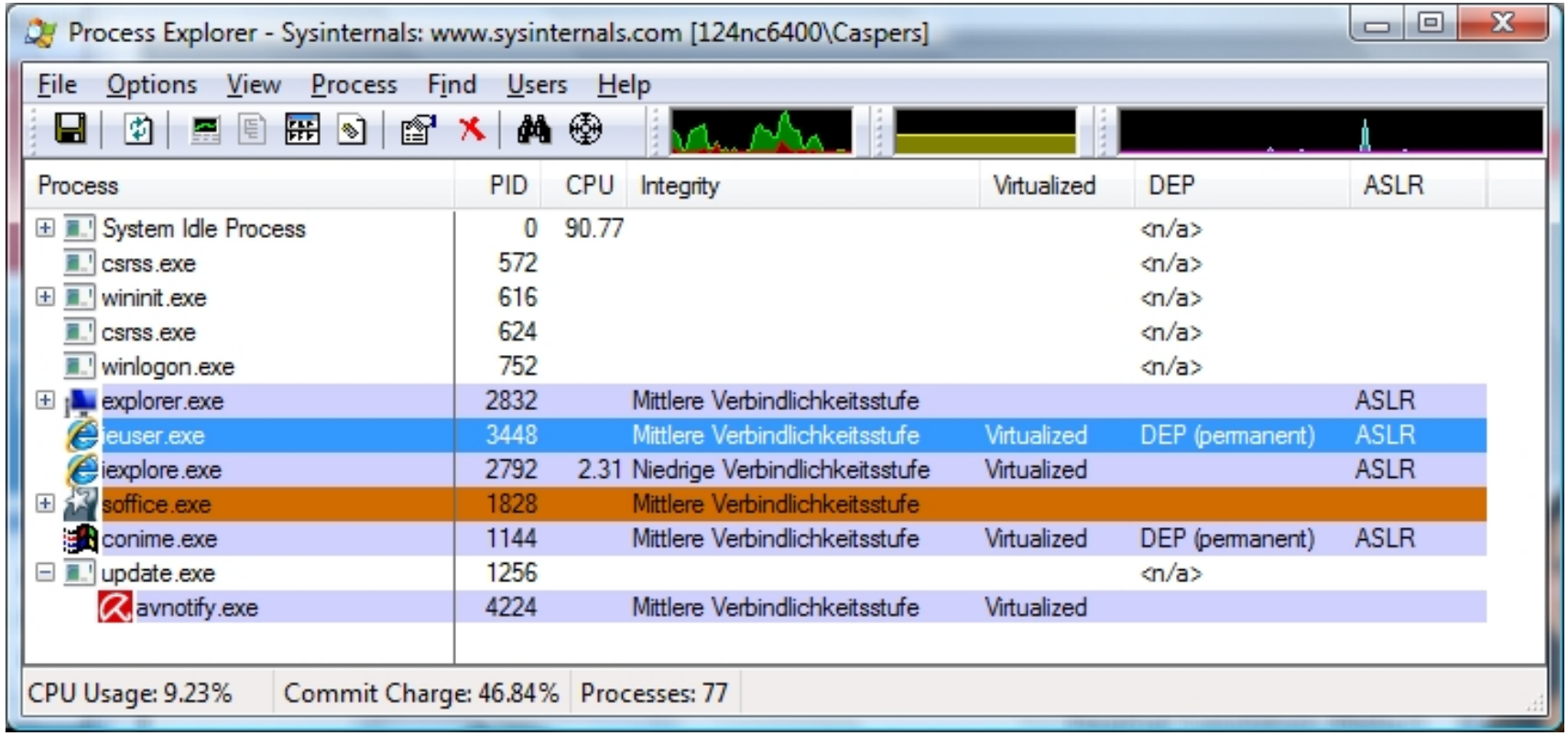
  Quelle: *http://blogs.msdn.com/shawnfa/archive/2008/05/12/fulltrust-on-the-localintranet.aspx*

- Neue Empfehlung von Microsoft für .NET:
  Software Restriction Policies
  - Zusammenspiel .NET Security Policies und SRP unklar
  - Strategie zur Code Access Security derzeit nicht erkennbar
  - Konkrete Umsetzung in .NET 4.0 (im September 2008 erstmals angekündigt) bleibt abzuwarten

Windows 7 und TPM

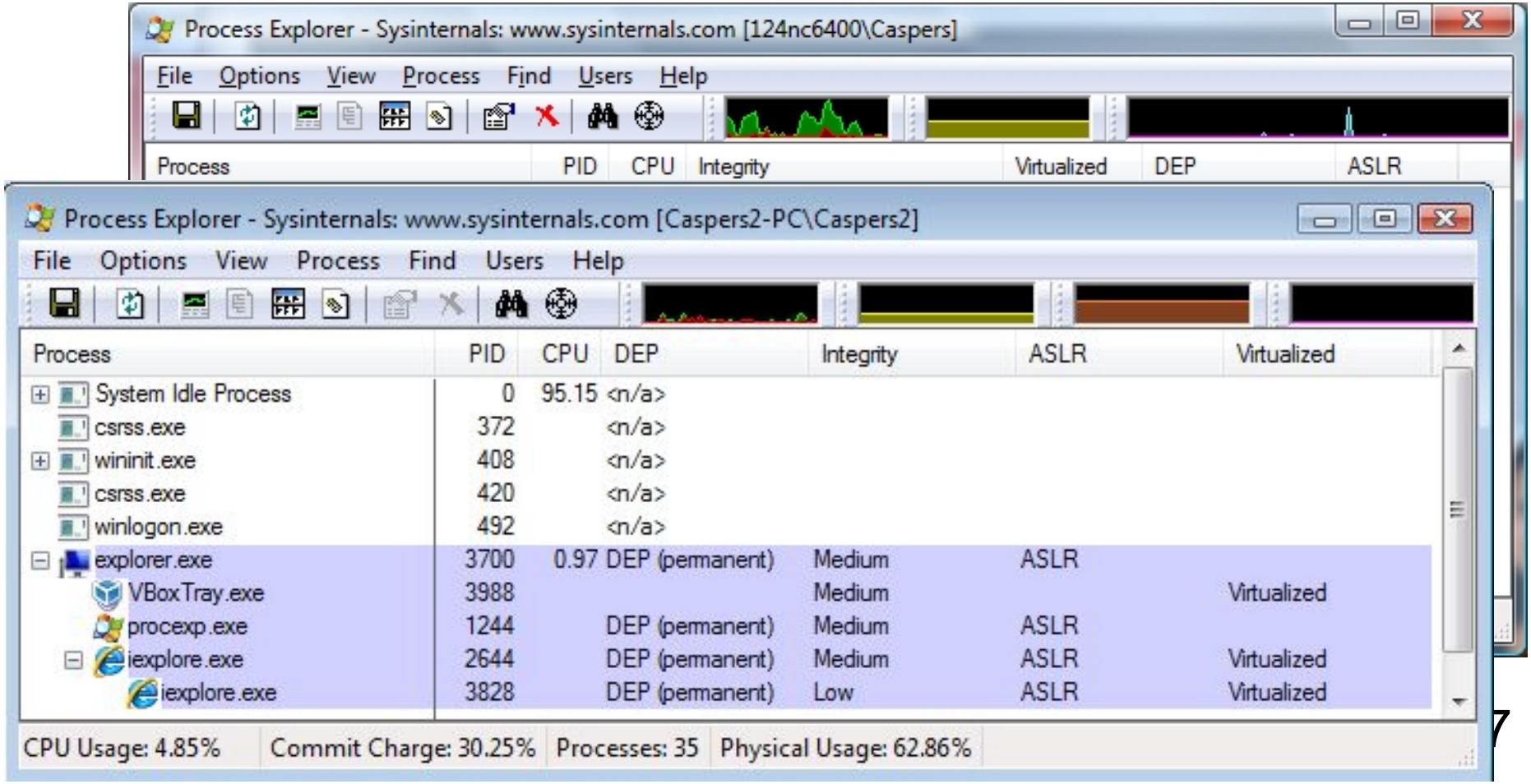
- Grundsätzliche Ziele
  - Höhere Stabilität
  - Bessere Unterstützung für TPM-Anwendungsentwickler
  - TPM-Selbsttest durch Treiber (falls nicht durch das BIOS)
- Verbesserung der Event-Log-Nutzung
  - TPM Treiber, TPM Base Services
  - Bereitstellung des TCG Event Logs durch Windows
- Entropie-Generierung allein durch TPM-Treiber
  - Vista SP1 benötigt noch TPM Base Services
- Zurücksetzen des Schutzes gegen Wörterbuchangriffe durch Windows (mmc.exe, TPM_ResetLockValue)
- BitLocker für USB-Massenspeicher

Windows 7 und Speicherschutz



Vista/IE7

Windows 7 und Speicherschutz



Windows 7/IE8

Weitere Sicherheitsaspekte von Windows 7

- Morro
  - Kostenloser Virenschutz für Windows 7 (und Vista/XP)
  - Unklare Abgrenzung zu Windows Defender und MSRT
- Gadgets
  - Weiterentwicklung des Windows Sidebar in Vista?
  - Zementierung einer industrieweiten Fehlentwicklung
- Identitätsmanagement
  - Live ID als Single Point of Failure
  - Geneva (Framework, Server, CardSpace)
  - Windows Azure
- Rückkopplung von Singularity-Forschungsergebnissen?
- Aktivierung, Windows Genuine Advantage, Verfügbarkeit


Shutting down...
Windows 7 Ultimate

Kontakt

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Thomas Caspers

Referat 124 – Sicherheit in Betriebssystemen
Godesberger Allee 185-189
53175 Bonn

Telefon 022899-9582-5452
Fax 022899-10-9582-5452
E-Mail thomas.caspers@bsi.bund.de

www.bsi.bund.de