


# Understanding the Greatest FDCC Technical Challenges

Kurt Dillard  
kurtdillard@msn.com  
fdcc@nist.gov

# The Point

- ▶ The FDCC is a good thing
- ▶ We've seen problems
- ▶ Often they uncover existing problems
  - Reconfigure/redesign
- ▶ Sometimes they cause the issues
  - People will have to change how they work

# Agenda

- ▶ **SCAP Content Issues**
  - ▶ Thorny Settings
  - ▶ Confusing Details
  - ▶ IE 8 & Windows 7
- 

# Account Name Changes

- ▶ Most built-in accounts have a common numerical security ID (SID)
  - OVAL specifies SID:
    - 500 = admin
    - 501 = guest
  - OVAL specifies name:
    - SUPPORT\_388945a0
  - Fails:
    - If the name is changed
    - If the account has been deleted


# User Settings

- ▶ Stored in profiles, in NTUSR.DAT
- ▶ Dynamically loaded into HKey\_Current\_User
- ▶ Problems & work-arounds
  - HKCU doesn't exist if nobody is logged on
  - Scanner can't access if someone is logged on
  - User can't log on if NTUSR.DAT is loaded in scanner
- ▶ Solutions
  - Use impersonation to scan logged on user
  - Scan all profiles by creating copies of NTUSR.DAT
  - If any profile is non-compliant consider the system non-compliant

# Other Settings

- ▶ Vista Firewall rules used to block IPv6 encapsulation within IPv4 packets
  - 6to4 uses IP protocol 41
    - Requires public IP address
  - Teredo uses UDP port 3544
    - Can traverse NATs, but has a larger overhead
  - Can be written to 2 locations
  - Randomly named reg key
  - Complex pattern recognition
- ▶ *Network access: Allow anonymous SID-Name translation*
  - ▶ Both XP & Vista
  - ▶ Stored in an unpublished manner

# Agenda

- ▶ SCAP Content Issues
  - ▶ **Thorny Settings**
  - ▶ Confusing Details
  - ▶ IE 8 & Windows 7
- 

# Breaking IPsec

- ▶ *Access this computer from the network*
- ▶ User right necessary for establishing connection
  - FDCC limits it to Administrators
  - Internet Key Exchange (IKE) fails
- ▶ Breaks a few things
- ▶ Granting the right to “Domain Computers” or “Authenticated Users” should resolve it
- ▶ Default on XP:
  - Everyone, Administrators, Users, Backup Operators



# Breaking Secure Websites

- ▶ Its been the law since 2002 (FISMA act)
- ▶ Everyone has assured compliance for several years
- ▶ Some .gov sites are still inaccessible
- ▶ Numerous commercial sites fail
- ▶ No workaround
  - Persuade the site owners to reconfigure
  - Don't use the sites
  - Become non compliant
- ▶ Breaks RDP too

# How to Disable Autorun (and a Lot of Other Things)

- ▶ How Autorun works
  - Insert a disc
  - Windows opens it using AutoPlay
  - Movie DVDs or music CDs displayed by Media Player
  - Windows looks for a file called autoplay.inf
- ▶ How worms exploit it on writable drives

# Autorun Continued...

- ▶ Microsoft patched this by disabling Autorun on writable drives, but...
- ▶ Workaround published not endorsed by Microsoft.
- ▶ Blogger recommended a registry value to completely disable AutoRun
  - <http://nick.brown.free.fr/blog/2007/10/memory-stick-worms>

# Autorun Continued...



HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\  
IniFileMapping\Autorun.inf @="@SYS:DoesNotExist"

# Autorun Continued...

- ▶ Installer sees invalid registry paths, e.g.

HKLM\Software\Microsoft\Office

Replaced by

HKLM\Software\DoesNotExist

- ▶ How to disable the Autorun functionality in Windows
  - <http://support.microsoft.com/kb/967715>
- ▶ Kudos to Aaron Margosis:
  - <http://blogs.technet.com/fdcc/>

# Refresher: IE Security Zones

- ▶ Internet Zone
  - <http://nist.gov>, <http://0.1.1.5>, <http://3221226219>, <http://0xC00002EB>, etc
- ▶ Intranet Zone
  - <http://hrweb>, \\hrweb
- ▶ Local Machine Zone
- ▶ Restricted Sites Zone
- ▶ Trusted Sites Zone
- ▶ “Locked-Down” versions of each

# Breaking the Web: Java

- ▶ The goal: restrict MS JVM
- ▶ The original idea:
  - configure *Java permissions* to *Disable Java* for all zones.
- ▶ Unintended result: Java-based applications failed
- ▶ FDCC 1.0 fixed this by setting *Java permissions* to *High Security* for
  - Intranet Zone
  - Trusted Sites Zone

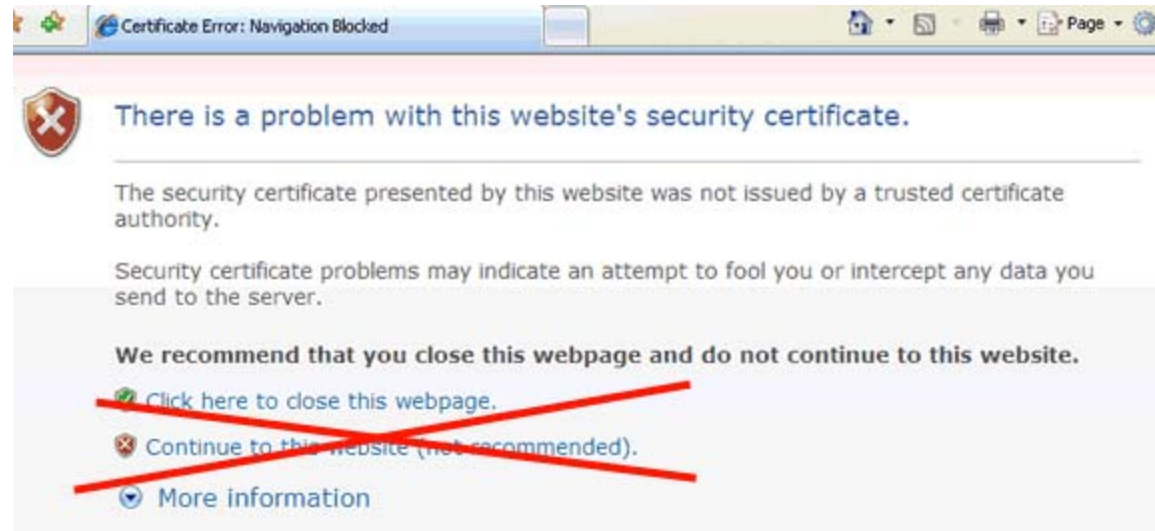
# Breaking the Web: ActiveX

- ▶ Users can't have admin privileges
- ▶ Users can't download and install ActiveX controls
- ▶ No prompts
- ▶ Solutions:
  - Use ActiveX Installer Service (on Vista)
  - Repackage and deploy via Group Policy, Tivoli, etc
  - Rewrite apps using AJAX or other alternatives
- ▶ Down the road...
  - IE8 supports per-user ActiveX controls



# Breaking the Web: Cert Errors

- ▶ Originally *Prevent ignoring certificate errors* was required




- ▶ Can't use `https://hrweb`
- ▶ Must use `https://hrweb.nist.gov` (or vice versa)
- ▶ Many `.gov` sites and network appliances have self-signed certs
- ▶ Removed in FDCC 1.0

# Non-Admin

- ▶ Poorly written apps
  - Use compatibility features, Vista's are better than XP's
  - Update or replace the app with something that works
  - Virtualize using Virtual PC, VMWare, Sun VirtualBox
- ▶ Well written apps may still require admin, e.g. developer tools
  - Give dev 2 accounts, only log in with admin when necessary
- ▶ Give mobile user password for local admin account, reset ASAP
  - Management overhead, but more secure

# Agenda

- ▶ SCAP Content Issues
  - ▶ Thorny Settings
  - ▶ **Confusing Details**
  - ▶ IE 8 & Windows 7
- 

# Disappearing Settings

- ▶ Apply the FDCC settings on Vista SP1
- ▶ Run GPRResults wizard
- ▶ Navigate to

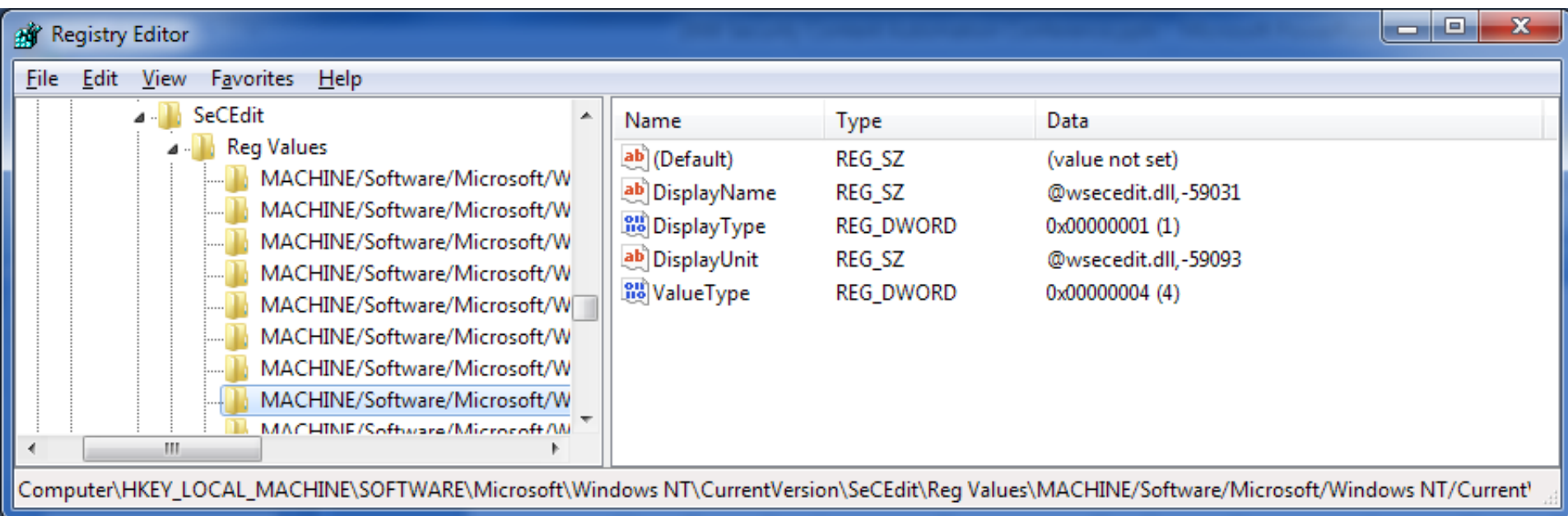
Computer Configuration\Policies\Windows Settings\Security Settings

*An error has occurred while collecting data for Security Configuration Engine (SCE) Extension.*

- ▶ Nothing under Security Settings is viewable:
- ▶ Contact Microsoft Customer Support, KB 955857.

# Settings You Can't See

- ▶ FDCC includes settings prefixed with *MSS*:
  - AutoAdminLogon
  - AutoShareWks
  - NoDefaultExempt
  - Etc...
- ▶ By default they are not visible in the Security Configuration Editor
- ▶ SCEcli.dll renders the security templates UI
  - Customize *%systemroot|inf|Sceregvl.inf*
  - Reinitialize: *Regsvr32 SCEcli.dll*



**Group Policy**

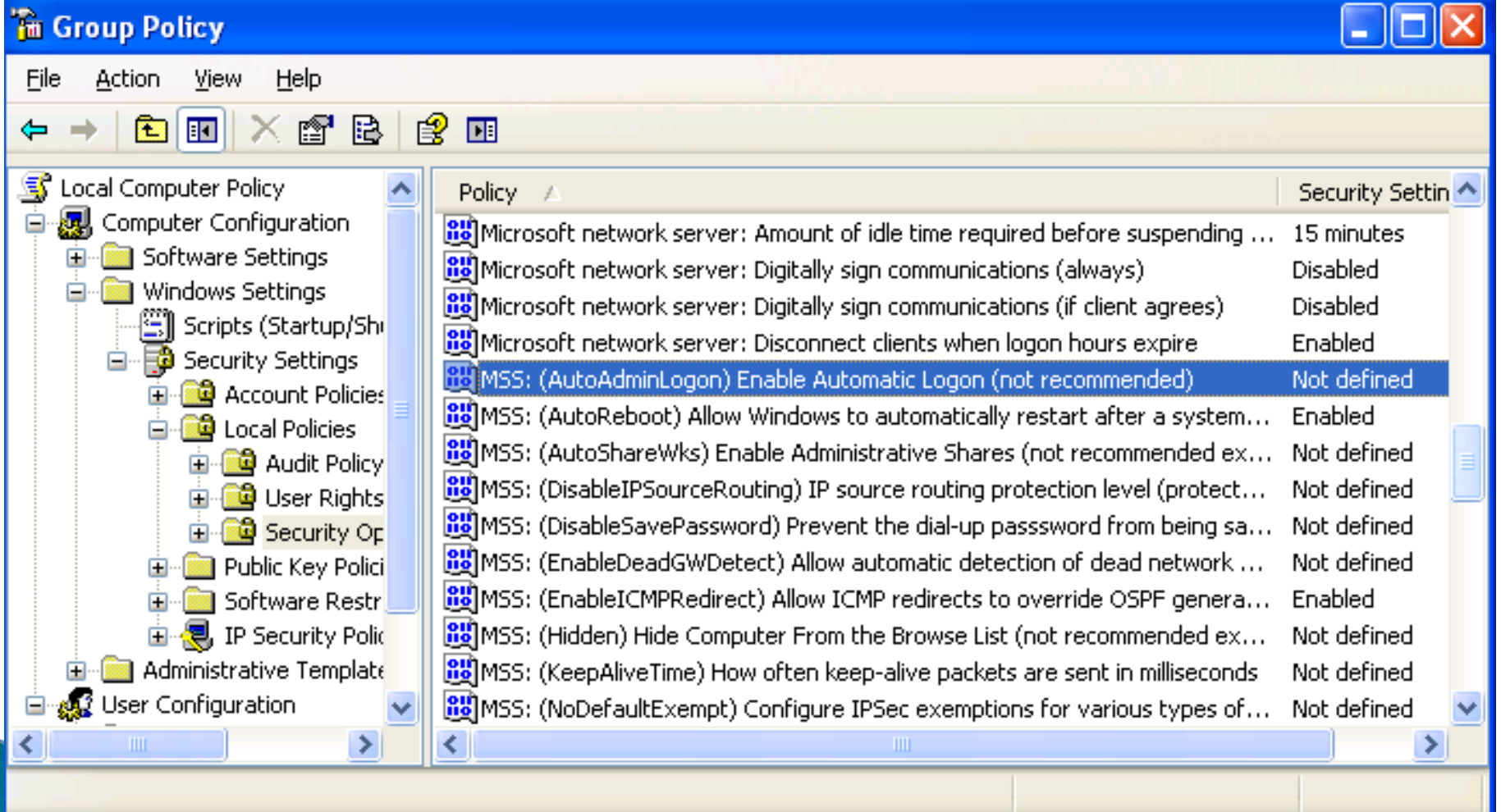
File Action View Help

← → ↗ 📄 📌 📋

Local Computer Policy

- Computer Configuration
  - Software Settings
  - Windows Settings
    - Scripts (Startup/Shutdown)
    - Security Settings
      - Account Policies
      - Local Policies
        - Audit Policy
        - User Rights
        - Security Options
      - Public Key Policies
      - Software Restriction Policies
      - IP Security Policies
    - Administrative Templates
  - User Configuration

Policy	Security Setting
Interactive logon: Prompt user to change password before expiration	14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled
Interactive logon: Require smart card	Not defined
Interactive logon: Smart card removal behavior	No Action
Microsoft network client: Digitally sign communications (always)	Disabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled
Microsoft network server: Digitally sign communications (if client agrees)	Disabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled
Network access: Allow anonymous SID/Name translation	Disabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled





# MSS: Settings Continued...

## ▶ Script & Tools

- Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP:
  - <http://go.microsoft.com/fwlink/?LinkId=15159>
- Security Compliance Toolkit Series:
  - <http://technet.microsoft.com/en-us/library/cc677002.aspx>
- GPOAccelerator:
  - <http://go.microsoft.com/fwlink/?LinkId=107264>

▶ ...


# Confusion with Other Efforts

- ▶ The USAF created the Secure Desktop Configuration (SDC)
- ▶ The FDCC VHD are for XP and Vista with IE7
  - Does not include other applications
- ▶ MCS created a service offering called
  - Federal Server Core Configuration (FSCC)
  - [msfsc@microsoft.com](mailto:msfsc@microsoft.com)

# Managing Without Active Directory

- ▶ Security Templates won't work
  - Most settings are managed via admin templates
  - The FDCC settings cannot be applied using sec templates
- ▶ Local GPO
  - Aaron Margosis from MCS created a tool
    - <http://blogs.technet.com/fdcc>
- ▶ From AD to local GPO works
- ▶ From local GPO to AD does not

# Agenda

- ▶ SCAP Content Issues
  - ▶ Thorny Settings
  - ▶ Confusing Details
  - ▶ **IE 8 & Windows 7**
- 

# Internet Explorer 8 & Windows 7

- ▶ The OMB decides what to add to the FDCC
- ▶ Microsoft worked with the DoD
  - Windows 7
    - <http://go.microsoft.com/fwlink/?LinkId=160808>
  - Internet Explorer 8
    - <http://go.microsoft.com/fwlink/?LinkId=160809>
- ▶ Microsoft will add their guides to the Checklists database
  - <http://checklists.nist.gov>
  - Their submissions will include SCAP content

# Resources

- ▶ OMB directives
  - <http://www.whitehouse.gov/omb/memoranda/fy2008/m08-22.pdf>
  - [fisma@omb.eop.gov](mailto:fisma@omb.eop.gov)
- ▶ Assistance
  - [fdcc@nist.gov](mailto:fdcc@nist.gov)
  - <http://blogs.technet.com/fdcc>
- ▶ NIST Guidance
  - NIST SP 800-68
    - [http://csrc.nist.gov/itsec/guidance\\_WinXP.html](http://csrc.nist.gov/itsec/guidance_WinXP.html)
- ▶ Additional Microsoft Guidance
  - Windows XP:
    - <http://go.microsoft.com/fwlink/?LinkId=14839>
  - Windows Vista:
    - <http://www.microsoft.com/technet/windowsvista/security/guide.mspx>