



BlackHat®

USA * EUROPE * ASIA

USA 2004

Managing MSIE security in corporate networks by creating custom Security Zones



EdelWeb

Patrick Chambet

Edelweb – ON-X Group

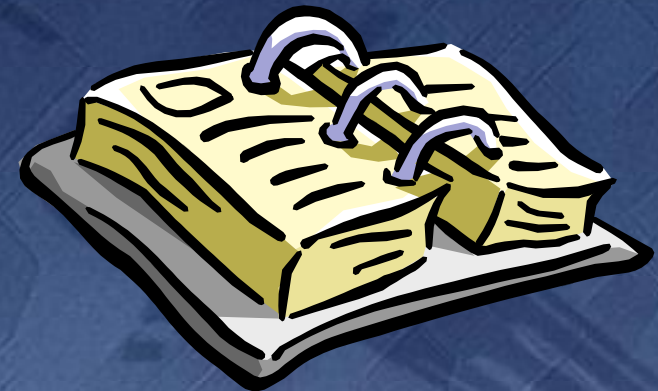
patrick.chambet@edelweb.fr

<http://www.edelweb.fr>

<http://www.chambet.com>

Planning

- u General points
- u MSIE Security Zones creation and settings
- u Conclusion



General Points (1/2)

- u A lot of companies use Internet Explorer internally as their corporate Web browser
- u They need to protect themselves against hostile code
 - o Viruses
 - o Worms
 - o Hostile Web servers
 - o Spyware

General Points (2/2)

- u Companies need several policies, depending on the kind of browsed Web sites
 - ∅ Professional Web sites
 - ∅ “Tolerated” Web sites
 - ∅ “Forbidden” Web sites

- u Which ActiveX are allowed in the company ?
 - ∅ Flash player ?
 - ∅ Media player ?
 - ∅ Company-made ActiveX ?

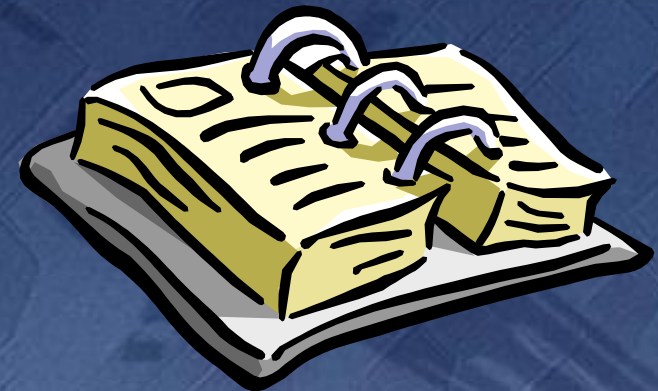
Planning

- u General points



- MSIE Security Zones creation and settings**

- u Conclusion



MSIE Security Zones (1/8)

- u **IE security zones settings are stored in 2 locations in the Registry**

- ∅ `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`
- ∅ `HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings`
- ∅ The settings are additive
- ∅ Only custom Web sites in `HKEY_CURRENT_USER` are visible

- u **To use only computer settings**

- ∅ **Set value**
`Security_HKEY_LOCAL_MACHINE_only` in
`HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\ (DWORD) to 1`

MSIE Security Zones (2/8)

u Sub keys

∅ TemplatePolicies

- ∅ Settings of the default security zone levels (Low, Medium Low, Medium, High)

∅ ZoneMap

- ∅ Contains domains and protocols with custom behavior

∅ Zones

- ∅ Contains the zones settings

MSIE Security Zones (3/8)

u Built-in Zones

- ∅ 0 My Computer
- ∅ 1 Local Intranet Zone
- ∅ 2 Trusted sites Zone
- ∅ 3 Internet Zone
- ∅ 4 Restricted Sites Zone

u Unhide the « My Computer » zone

- ∅ Set value `Flags` in
`HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0` to 71

u The `Flags` DWORD value determines the ability of the user to modify the security zone's settings

MSIE Security Zones (4/8)

- u Proper security zone parameters are used locally for saved HTML pages

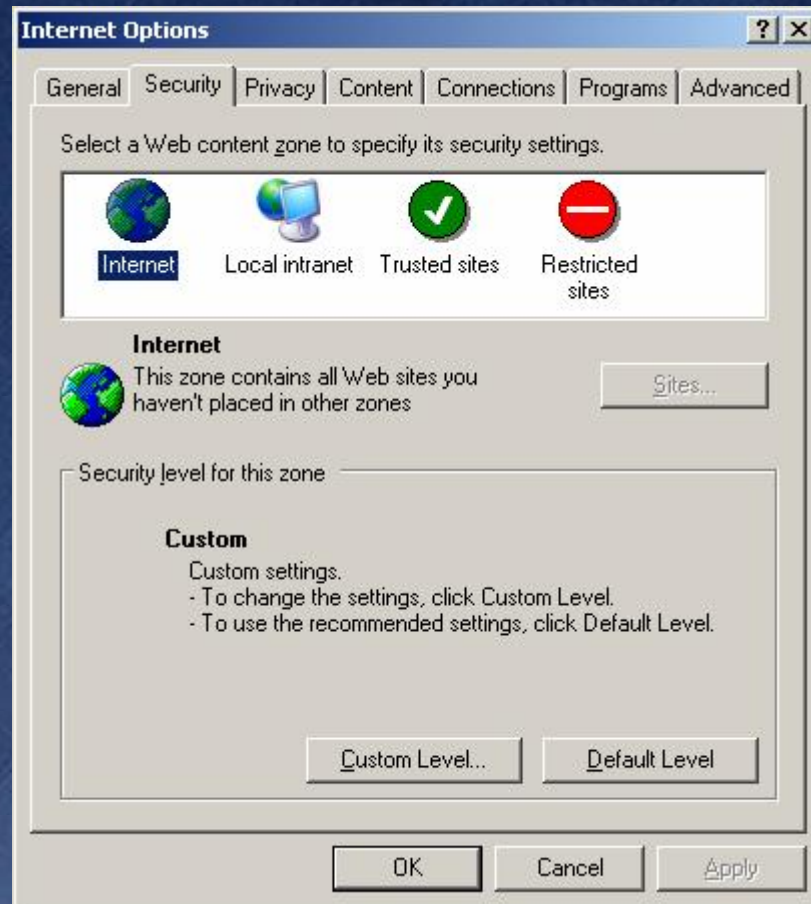
- o “Mark of the Web”
`<!-- saved from
url=(0023)http://foo.example.com/ -->`

 URL length

- u The easiest way to create a new security zone
 - o Export the closest zone (trusted / restricted) to a .reg file
 - o Modify the zone number and some settings
 - o Flags, icon, name, ...
 - o Import the .reg file
 - o Use the GUI to customize your settings

MSIE Security Zones (5/8)

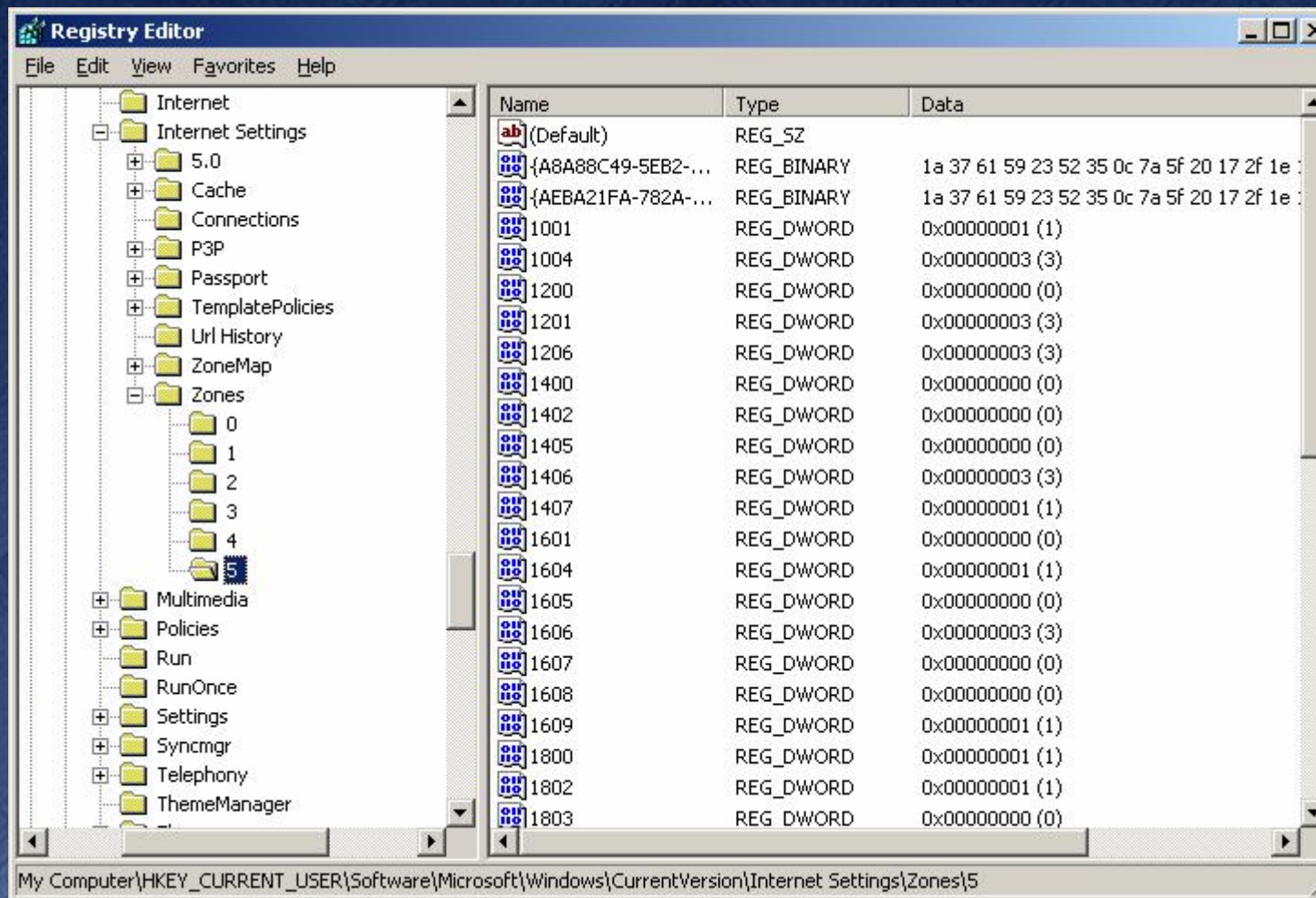
Before



After



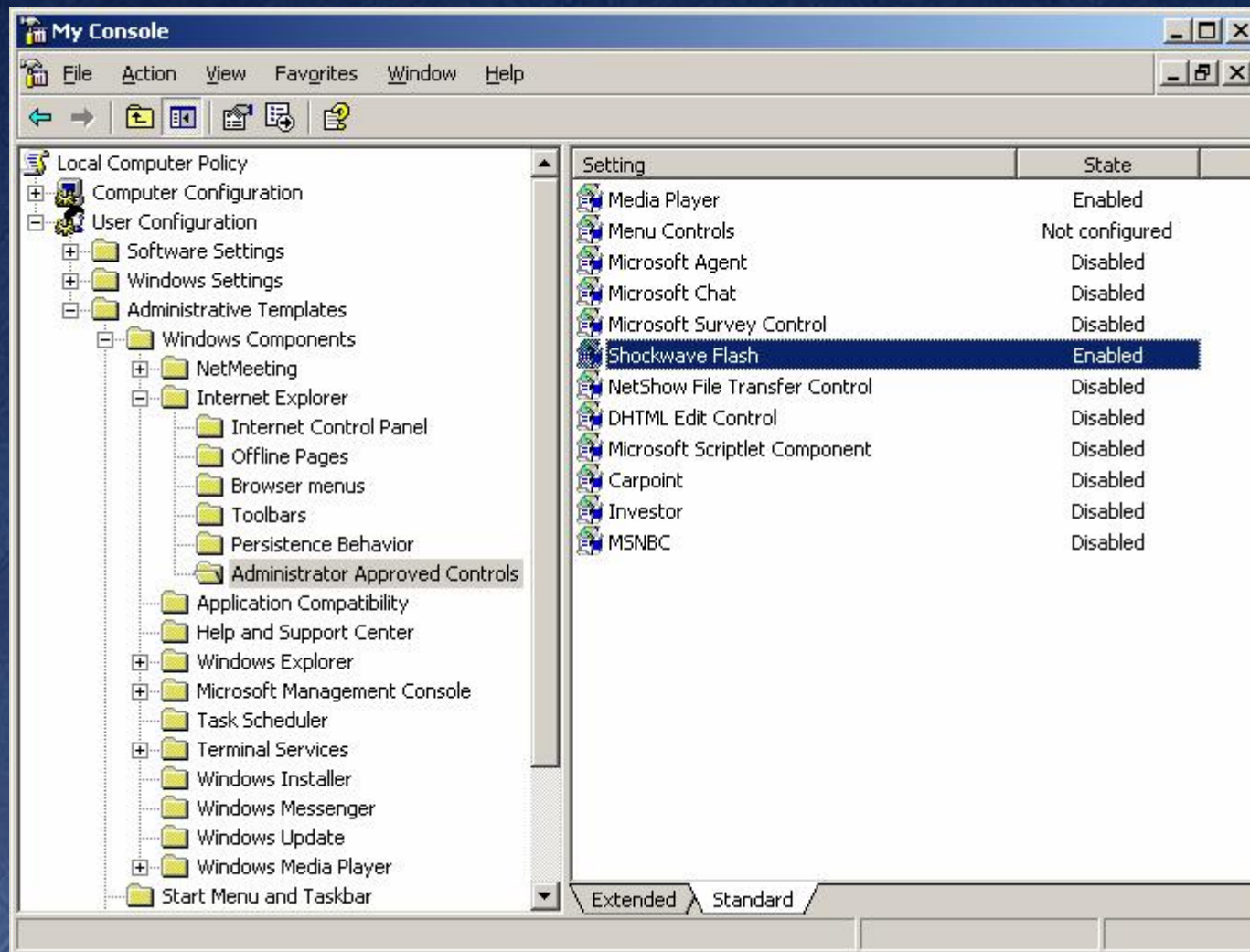
MSIE Security Zones (6/8)



MSIE Security Zones (7/8)

- u Administrator approved ActiveX
 - ∅ Check “Administrator approved” in “Run ActiveX controls and plug-ins” (value “1200”)
 - ∅ The approved controls are stored in `HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\AllowedControls\`
 - ∅ In the MMC
 - ∅ GPO editor snap-in
 - ∅ Local Computer Policy
 - ∅ User configuration

MSIE Security Zones (8/8)

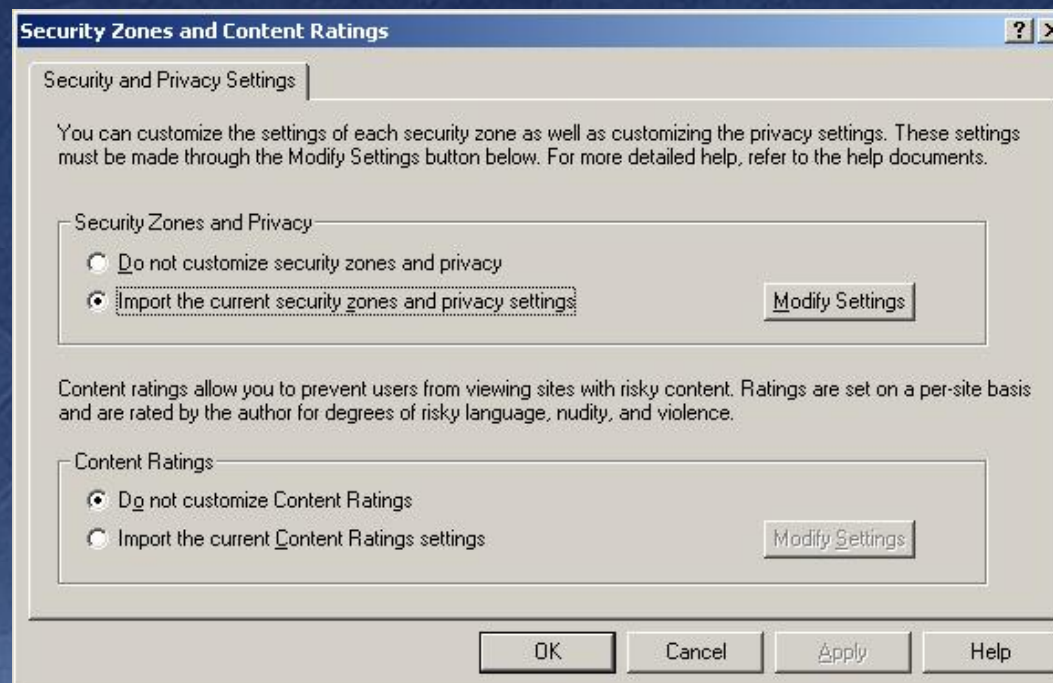


Deployment

- u IEAK

- u GPO

- o User configuration/Windows settings/IE Maintenance/Security



Conclusion

- u MSIE Security Zones in a corporate network can be customized to special needs depending on user working habits
- u The overall IE security is increased
- u But does not replace the security patch management process for IE

Links (1/2)

u Microsoft KB

- ∅ Q182569
<http://support.microsoft.com/?kbid=182569>
- ∅ Q315933 (Local Machine zone)
<http://support.microsoft.com/?kbid=315933>
<http://support.microsoft.com/?kbid=833633>
- ∅ Q240797 (ActiveX Compatibility: the Kill Bit)
<http://support.microsoft.com/?kbid=240797>



u Microsoft Reskits

- ∅ <http://www.microsoft.com/resources/documentation/ie/6/all/reskit/en-us/part2/c04ie6rk.mspx>
- ∅ <http://www.microsoft.com/resources/documentation/ie/5/all/reskit/en-us/part1/ch07zone.mspx>

Links (2/2)

- u Increase your browsing and e-mail safety
 - ø <http://www.microsoft.com/security/incident/settings.msp>

- u MSDN
 - ø URL Security Zones
http://msdn.microsoft.com/library/en-us/dnanchor/html/anch_securityzones.asp
 - ø URL Security Zones Reference
http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/reference/urlzones_ref_entry.asp

Questions & Answers

