Non-Admin Today on Windows XP

Bob McCoy
Technical Account Manager
Microsoft Services

Agenda

- **Least Privilege for Admins**
  - **How to elevate only as needed**
- **Least Privilege for Users**
  - **Addressing LUA bugs**

Definitions

- Non-Admin
  - "Power Users" is *not* non-Admin!
  - Typically: "Users", "Domain Users"
- LUA
  - Limited User Account
  - Least-privileged User Account
- LUA Bugs
- User Account Control (Windows Vista)

Principle of Least Privilege

- Most computer use does not require admin privilege
- But, typical usage: "Max Privilege"
- Most malware expects "Max Privilege"

Admin Can, LUA Can't:

- Install kernel-mode rootkits
- Install system-level keyloggers (including capturing passwords entered into the Ctrl-Alt-Del logon dialog)
- Install ActiveX controls, including IE and Explorer extensions (common with spyware and adware)
- Install and start services
- Stop existing services (such as the firewall)
- Access data belonging to other users
- Cause code to run whenever anybody else logs on
- Replace OS and other program files with Trojan horses
- Access LSA Secrets, including other sensitive account information, possibly including account info for domain accounts
- Disable/uninstall anti-virus
- Create and modify user accounts
- Reset passwords
- Modify the "HOSTS" file and other system configuration settings
- Cover its tracks in the event log
- Render your machine unbootable
- …

The Twin Challenge on Windows XP

- **For Sysadmins and Developers**

  How to run with least privilege and elevate only as needed?

- **For regular users:**

  How to always run with least privilege when so many apps (and sometimes Windows) requires more?

Non-Admin Blog

http://blogs.msdn.com/aaron_margosis

"Running as Admin Only When Required":

- **The easiest way to run as non-admin (Fast User Switching)**
- **"RunAs" basic (and intermediate) topics**
- **RunAs with Explorer**
- **MakeMeAdmin – temporary admin for your Limited User account**
- **PrivBar – An IE/Explorer toolbar to show current privilege level**
- **Running restricted – What does the "protect my computer" option mean?**
- **Ctrl-C doesn't work in RUNAS or MakeMeAdmin command shells**

"Not Running as Admin At All":

- **What is a "LUA Bug"? (And what isn't a LUA Bug?)**
- **Fixing "LUA bugs", Part I**
- **Remembering Calculator and Character Map Settings**
- **Managing Power Options as a non-administrator**
- **Changing the system date, time and/or time zone**
- **How to allow users to manage file and print shares without granting other advanced privileges**
- **Workaround for Shutdown.exe LUA bug**

More coming!

How to Elevate as Needed

Fast User Switching

- **Windows XP Home**
- **Windows XP Professional**
  - **If not joined to a domain – *fixed in Windows Vista!***
- **Logon sessions isolated from each other**

Suggestion for home users:

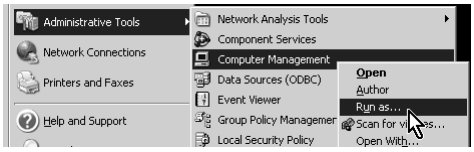
- **One LUA for each person, Guest optional**
- **One admin account**
- **No passwords!**

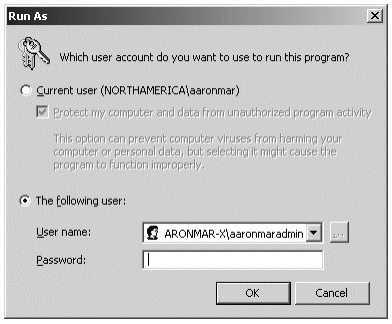
RunAs

- Start a program as a different user
  - Same desktop
- Command line or graphical dialog
- Programs inherit security context from "parent"
  - Start CMD as admin
  - Launch apps from admin CMD
  - Those apps also run as admin

RunAs Dialog

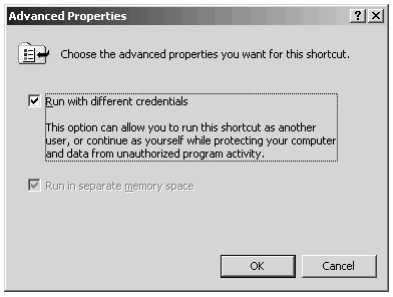
- Right-click context menu
  - Apps, shortcuts
  - Common Console (.msc)
- *Shift*+right-click for:
  - Control Panel applets (.cpl)
  - "Special Microsoft Windows Installer links"



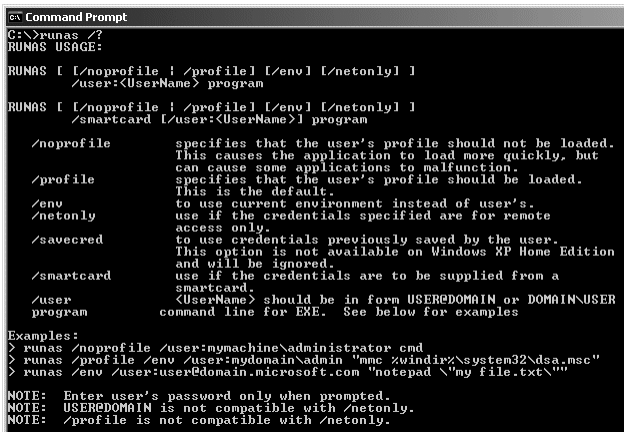


RunAs Dialog

- Make "RunAs" the default for a shortcut
- Shortcut → Properties, Advanced Properties



RunAs Command Line

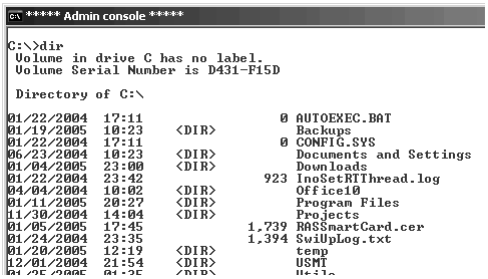


- E.g.,
  `runas /u:Administrator cmd.exe`

RunAs: Visual Differentiation

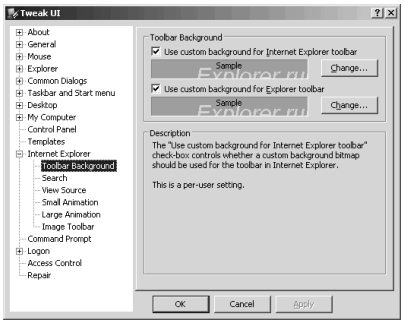
- Set privileged console windows apart visually

```
cmd.exe /t:fc /k cd c:\ && title
   ***** Admin console *****
```



RunAs: Visual Differentiation

- Background bitmap for IE and Explorer
- Set it with TweakUI

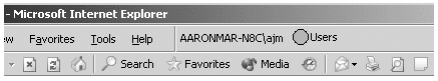


PrivBar

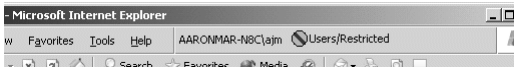
Running IE as admin:

… as Power User:

… as "User":



… with "Protect my computer":



When RunAs Doesn't Work

- Some apps reuse existing instances
  - Windows Explorer
  - Microsoft Office Word
- Some apps get started through the shell
  - ShellExecute[Ex]
  - DDE
- Current version of WindowsUpdate! ☹
  - And Microsoft Update! ☹

RunAs and Explorer

- Two viable options:
  1. Use Internet Explorer, or
  2. Set the flag that lets Windows Explorer run multiple instances
- "The flag…"
  - "Launch folder windows in a separate process"
- Caveats about this setting

Issues Using Local Admin Account

- No access to domain resources
- Different profile settings
- Some apps assume that the installer is the user
- Per-user Policy settings
- Power Options applet
- Resolution? MakeMeAdmin

MakeMeAdmin

- Temporary elevation of your current account
- Result: CMD running with your normal account but with admin privileges
- Apps started from it inherit context
- Posted on Aaron's blog

Tools for Elevating as Needed

demo

Fixing "LUA Bugs"

Most- to least-preferred options:

1. **Make the developers fix it!**
2. **Application Compatibility Toolkit (ACT)**
3. **Copy HKCR data to HKCU, *or*
   Leverage *IniFileMapping*, *or*
   Update SafeDisc**
4. **Loosen ACLs**
5. **Run the one app as admin**

LUA Tools Today

- **Regmon, Filemon**
  → `http://www.sysinternals.com`
- **Issues:**
  - **Not tailored to LUA**
  - **Covers only registry and file system**
  - ***Huge* amount of data**
  - **Nerds only**
  - **Security context**

Non-Admin Blog

http://blogs.msdn.com/aaron_margosis

"Running as Admin Only When Required":

- **The easiest way to run as non-admin (Fast User Switching)**
- **"RunAs" basic (and intermediate) topics**
- **RunAs with Explorer**
- **MakeMeAdmin – temporary admin for your Limited User account**
- **PrivBar – An IE/Explorer toolbar to show current privilege level**
- **Running restricted – What does the "protect my computer" option mean?**
- **Ctrl-C doesn't work in RUNAS or MakeMeAdmin command shells**

"Not Running as Admin At All":

- **What is a "LUA Bug"? (And what isn't a LUA Bug?)**
- **Fixing "LUA bugs", Part I**
- **Remembering Calculator and Character Map Settings**
- **Managing Power Options as a non-administrator**
- **Changing the system date, time and/or time zone**
- **How to allow users to manage file and print shares without granting other advanced privileges**
- **Workaround for Shutdown.exe LUA bug**

More coming!

More Resources

- Non-Admin Wiki: http://nonadmin.editme.com
- Non-Admin blog: http://blogs.msdn.com/aaron_margosis
- Applying the Principle of Least Privilege to User Accounts on Windows XP
  http://go.microsoft.com/fwlink/?LinkId=58445
- "Running Windows with Least Privilege" Technet Webcast
  http://msevents.microsoft.com/cui/eventdetail.aspx?eventID=1032274954
- "Browsing the Web and Reading E-mail Safely as an Administrator"
  Part 1: http://msdn.microsoft.com/library/en-us/dncode/html/secure11152004.asp
  Part 2: http://msdn.microsoft.com/library/en-us/dncode/html/secure01182005.asp
- DesktopStandard PolicyMaker Application Security:
  http://www.desktopstandard.com/PolicyMakerApplicationSecurity.aspx
- Winternals Protection Manager
  http://winternals.com/Products/ProtectionManager
- RunAsAdmin:
  http://www.harper.no/valery/CategoryView,category,RunAsAdmin.aspx
- Microsoft Standard User Analyzer
  http://www.microsoft.com/downloads/details.aspx?FamilyID=df59b474-c0b7-4422-8c70-b0d9d3d2f575&DisplayLang=en

© 2006 Microsoft Corporation. All rights reserved. This presentation is for informational purposes only.
MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.