Published: January 18, 2006
Please direct questions and comments about this guide to secwish@microsoft.com.

To view comments or discussion of this guide, see http://blogs.technet.com/secguide.

On This Page

Introduction

Recent advances in networking technology such as permanent connectivity to the Internet have brought enormous opportunities to organizations of all sizes. Unfortunately, a connection between a computer and any network, especially the Internet, increases the level of risk from malicious software and external attackers, and as old risks are managed, new ones are discovered or created.

Sophos, an Internet security company, found that the number of malicious programs detected rose from 45,879 in November of 1999 to 114,082 in November of 2005, an increase of at least 10 percent every year for the last six years. In November of 2005, Sophos discovered more than 1,900 new examples of malicious software, such as viruses, Trojan horses, and spyware programs. Other antivirus vendors report similar increases in the numbers and types of malicious software.

A significant factor that increases the risks from malicious software is the tendency to give users administrative rights on their client computers. When a user or administrator logs on with administrative rights, any programs that they run, such as browsers, e-mail clients, and instant messaging programs, also have administrative rights. If these programs activate malicious software, that malicious software can install itself, manipulate services such as antivirus programs, and even hide from the operating system. Users can run malicious software unintentionally and unknowingly, for example, by visiting a compromised Web site or by clicking a link in an e-mail message.

Malicious software poses numerous threats to organizations, from intercepting

a user's logon credentials with a keystroke logger to achieving complete control over a computer or an entire network by using a rootkit. Malicious software can cause Web sites to become inaccessible, destroy or corrupt data, and reformat hard disks. Effects can include additional costs such as to disinfect computers, restore files, re-enter or re-create lost data. Virus attacks can also cause project teams to miss deadlines, leading to breach of contract or loss of customer confidence. Organizations that are subject to regulatory compliance can be prosecuted and fined.

Note For more information about rootkits, see the rootkit definition on Wikipedia at http://en.wikipedia.org/wiki/Rootkit.

The Least-Privileged User Account Approach

A defense-in-depth strategy, with overlapping layers of security, is the best way to counter these threats, and the least-privileged user account (LUA) approach is an important part of that defensive strategy. The LUA approach ensures that users follow the principle of least privilege and always log on with limited user accounts. This strategy also aims to limit the use of administrative credentials to administrators, and then only for administrative tasks.

The LUA approach can significantly mitigate the risks from malicious software and accidental incorrect configuration. However, because the LUA approach requires organizations to plan, test, and support limited access configurations, this approach can generate significant costs and challenges. These costs can include redevelopment of custom programs, changes to operational procedures, and deployment of additional tools.

Important It is difficult to find utilities and guidance on using limited user accounts, so this white paper refers to third-party tools and guidance from Web logs and other unofficial sources. Microsoft makes no warranty about the suitability of the tools or guidance for your environment. You should test any of these instructions or programs before you deploy them. As with all security issues, there is no perfect answer, and this software and guidance is no exception.

Audience

This white paper targets two audiences:

- Business decision makers who need to understand the concepts of the LUA approach and the organizational issues that the LUA approach generates.
- IT professionals who need to understand the options for implementing the LUA approach within their organization.

Topics

This document discusses the issues and concerns that organizations may face

when they apply the LUA approach to computers that run Microsoft® Windows® XP. The discussion covers the following topics:

- Risks associated with administrative privileges
- Definition of the principle of least privilege
- Definition of the LUA approach
- Benefits of the LUA approach
- Risk, security, usability, and cost tradeoffs
- Implementing the LUA approach
- Future Developments

This paper also describes the high-level issues that affect implementation of the LUA approach and provides useful links to other online resources that explain these concepts in more detail.

Note This paper does not address issues with running system services with least-privileged accounts. For more information on this topic, see The Services and Service Accounts Security Planning Guide, at www.microsoft.com/technet/security/guidance/serversecurity/serviceaccount/default.mspx

Top of page

Risks Associated with Administrative Privileges

Many organizations routinely give users administrative privileges to their computers. This arrangement is particularly common with portable computers, and usually happens for the following reasons:

- To enable some programs to run properly. Some programs can only run when a user has administrative rights. Typically, this might occur if the program stores user data in registry or file system locations that a non-administrative account cannot access.
- To permit the user to carry out administrative actions, such as changing the computer's time zone.
- To enable mobile users to install work-related hardware or software, such as print devices or DVD writers and associated programs.

Although there may be other valid reasons to provide users with administrative rights, such an arrangement significantly increases the risk of computer compromise and of improper configuration. These risks can affect many areas of an organization's operations.

Consider the situation in which a senior executive regularly visits client offices to give presentations from his portable computer. Because he is a senior

executive, he insists on having local administrative rights on his computer. He is just about to deliver a key sales presentation to an important customer, when an offensive message appears on the screen of his portable computer, which then locks up. When he hastily restarts the computer, the executive finds that the hard drive has been reformatted. Consequently, the sales presentation fails to impress the customer, and the order goes to a competitor.

In this case, the offensive message and subsequent destruction of data resulted from malicious software that infected the computer when the executive browsed a compromised Web site. When he visited that Web site, the executive was logged on to his portable computer as a member of the local Administrators group. The rights and privileges from this group membership enabled the malicious software to disable the antivirus software, install itself, manipulate the registry, and place files in the Windows system directory. The executive's computer was now compromised, and ready to carry out the malicious software's commands.

Other scenarios that can exploit the greater privileges from administrative accounts include situations in which users click links in e-mail messages or play music CDs that include digital rights management software. The common factor is that users who have administrative rights are significantly more likely to compromise their computers than those who use limited user accounts.

Top of page

Definition of the Principle of Least Privilege

The Department of Defense Trusted Computer System Evaluation Criteria, (DOD-5200.28-STD), also known as the Orange Book, is an accepted standard for computer security. This publication defines least privilege as a principle that "requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use."

Top of page

Definition of the LUA Approach

This paper defines the LUA approach as the practical implementation of the principle of least privilege on computers that run Windows XP. Specifically, users, programs, and services on Windows XP should have only the minimum rights and permissions that they require to carry out their assigned tasks.

Note It is important to understand the difference between rights and permissions. Rights define the tasks that a user can carry out on a computer, whereas permissions define what a user can do to an object on a computer. Hence, a user needs the *right* to shut the computer down, but *permission* to access a file.

The LUA approach is a combination of recommendations, tools, and best

practices that enable organizations to use non-administrative accounts to operate computers that run Windows XP. The LUA approach requires organizations to re-evaluate the role of computers and the level of access that users should have to their equipment. It also addresses both strategic and day-to-day considerations from operating under limited user accounts, and addresses the issues that arise. These issues include areas such as remote users needing to make configuration changes to their computers.

The LUA approach should also apply to application development and testing. Developers (and sometimes testers) typically log on to their computers with accounts that have administrative rights. This configuration can result in developers releasing compiled programs that require similar elevated privileges to run. Rather than redesign the application to work correctly, the developers recommend "security workarounds," such as placing user accounts into the local Administrators group or granting users full control to the Windows system folders.

The LUA approach counteracts the tendency simply to grant administrative rights and permissions to every user or program that requires access to a resource. Programs that follow the principle of least privilege do not attempt to deny legitimate requests for resources, but only grant that access in accordance with good security guidance.

For more information on best practices when creating applications, see Running with Special Privileges, at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/secbp/security/running_with_special_privileges.asp.

Windows XP Accounts

To understand the principles behind the LUA approach, you should be aware of the differences between administrative and non-administrative accounts in Windows XP and know how Windows starts and runs programs. It is also necessary to take a brief look at groups in both workgroup and domain-based networks.

Computers that run Windows XP maintain an autonomous security database in the local Security Accounts Manager (SAM). The SAM is responsible for storing local user and group information, and includes numerous default groups, such as:

- **Administrators**. Have complete and unrestricted access to the computer.
- **Power Users**. Have more limited administrative rights, such as to share files, install local printers, and change the system time. Power users also have extensive permissions to access files in the Windows system folders.
- **Users**. Have limited user rights and are prevented from making accidental or intentional system-wide changes. User accounts who are

members of this group *only* are referred to as *limited user accounts*.

- **Guests**. Have fewer rights than limited users.

User accounts are granted their rights through membership in one or more of these groups. For example, the built-in Administrator account has administrative rights because it is a member of the Administrators group. This group membership gives the Administrator account elevated rights, such as the right to force a system shutdown from a remote computer.

The workgroup-based computer is entirely autonomous and only validates groups and users in its own SAM. When a workgroup computer joins a domain, the local group memberships change. In addition to the existing groups, the Domain Users group becomes a member of the local Users group and the Domain Admins group becomes a member of Administrators. This change allows any member of the Domain Admins group to log on to the computer with administrative rights, and any member of the Domain Users group to log on to the computer with limited user rights.

Administrative Accounts

An administrative account is any account that is a member of one or more of the administrative groups. On a domain-joined computer, administrative groups include the following:

- The local Administrators group
- The local Power Users group
- The Domain Admins group
- The Network Configuration Operators group
- Any domain group that has membership in any of the local administrative groups

Anyone who logs on with membership in one or more of these groups can make system-wide changes.

Note The Power Users group is a sub-set of Administrators rather than a superset of the Users group. Placing users in the Power Users group does not comply with LUA principles.

Limited Users

A limited user is an account that is a member of the local Users group and is *not* a member of any of the administrative groups. On a domain-joined computer, any account that is a member of the Domain Users group is also a member of the local Users group.

Limited user accounts significantly reduce the attack surface for malicious

software because these accounts have minimal ability to make system-wide changes that affect operational security. In particular, limited user accounts cannot open ports on the firewall, stop or start services, or modify files in the Windows system folders.

Many organizations would claim that they already implement the LUA approach because their users log on as members of the Domain Users group. However, if those users are also members of the local Administrators group, all the programs that they run will have administrative rights and could potentially cause unwanted changes.

Understanding the Logon Process

Another important area to understand is the authentication process on Windows XP. When a user logs on to a computer, the operating system authenticates the user's credentials and starts an instance of the Windows desktop, most commonly Windows Explorer. This desktop runs within the user's security context with the logged on user's access rights and permissions. When the user starts a program, such as Microsoft Internet Explorer, this program also runs in the user's security context.

Authenticating as an Administrator

If a user authenticates as a member of the local Administrators group, the desktop and any programs that the user starts will run with the full access rights and permissions of an administrator. Users who have administrative rights can carry out the following actions, which are legitimately required to administer a computer:

- Install, start, and stop services and device drivers.
- Create, modify, and delete registry settings.
- Install, run, and uninstall programs.
- Replace operating system files.
- Terminate processes.
- Control firewall settings.
- Manage event log entries.
- Install Microsoft ActiveX® controls.
- Access the SAM.

For the majority of computer users, these rights are unnecessary and significantly increase the risk to the computer. Because a user with administrative rights can make these system-wide changes, so can any program that a user with administrative rights runs, either intentionally or

accidentally. Hence, if a user authenticates with administrative rights, it is far easier for malicious software to install onto that computer.

Authenticating as a User

Users who are not members of the Administrators group can only access a significantly reduced number of resources, and then may only be able to make changes to particular areas. To compare user rights with administrative rights, users can carry out the following tasks:

- View the status of services and device drivers.
- Create, modify, and delete registry settings within **HKEY_CURRENT_USER**, and read registry settings in **HKEY_LOCAL_MACHINE**.
- Run programs.
- Read most operating system files.
- View running processes.
- View firewall settings.
- View system and application log entries only.

Limited users can still carry out tasks that are required for them to do their jobs, such as attach to a wireless network, install signed Plug and Play drivers, and change desktop settings. The LUA approach does not seek to limit those abilities, but to reduce risks by limiting the accounts that have administrative rights.

You should now understand the role of groups in Windows XP and the differences between authenticating with administrative and limited user rights. The next section of this paper reviews the benefits that result from the use of limited user accounts.

Top of page

Benefits of the LUA Approach

The LUA approach provides numerous benefits to organizations of all sizes. In addition to the reduced risk from attack by malicious software, these benefits include:

- Increased security
- Increased manageability
- Increased productivity
- Reduced costs

- Reduced piracy and legal liability issues

This section analyzes these benefits and how they can affect your organization.

Increased Security

The LUA approach is one of a number of security measures that can help to protect your organization and its computer assets from exploitation by attackers. Attackers seek to compromise your network for several reasons, which may include to:

- Gain control of multiple computers for use in distributed denial of service attacks.
- Send spam.
- Compromise proprietary information.
- Steal user identities.
- Distribute malicious software to other computers.

These attacks are more likely to succeed when the user logs on with an account that has administrative rights. For example, software that runs with administrative rights can:

- Install kernel-mode rootkits.
- Install system-level key logging programs.
- Intercept logon passwords.
- Install spyware and adware.
- Access data that belongs to other users.
- Run code when anyone logs on.
- Replace system files with Trojan horses.
- Reset passwords.
- Cover its tracks in the event log.
- Prevent the computer from restarting.

If users log on with limited user accounts, programs that run in those users' contexts can make only minimal changes to the operating system. This restriction significantly reduces the ability of malicious software to install and run, which increases security without preventing users from carrying out their

jobs.

Increased Manageability

Standardization is an important component of a manageable network, particularly with multiple client computers. If an organization has 500 client computers, and each computer has a different configuration of software and computer settings, proactive management becomes extremely complex. This complexity inevitably results when users can install software and make system-wide configuration changes.

Windows XP provides enormous potential to customize the operating system configuration. If users can log on with administrative rights, they often succumb to the temptation to change settings. For example, a user might switch off the Windows Firewall for a wireless network connection, and then connect to an Internet Service Provider through an unsecured connection at a public wireless access point. This action would lead to rapid compromise of the computer, because all network connections (even to trusted networks) should have the protection of a host-based firewall.

User-initiated changes tend to generate more support calls, and each time a modified computer requires attention, the support personnel face a different computer configuration. This lack of standardization makes help desk support, troubleshooting, and repair more difficult, time-consuming, and expensive.

The LUA approach also creates a definite management boundary between users and administrators. This boundary allows users to concentrate on doing their jobs, while network administrators manage the infrastructure. If users have administrative rights, it becomes impossible to enforce this boundary, and standardization cannot be guaranteed.

A network in which everyone is an administrator is effectively unmanaged, because the users can circumvent the systems management settings. If users cannot install unauthorized hardware and software or make system changes, their computers should remain reasonably close to the organizational standard. The LUA approach increases manageability by limiting unwanted modifications to computer environments.

Increased Productivity

Computers have brought enormous increases in productivity for organizations of all types and sizes. However, computers require proactive management to maintain this productivity advantage. In organizations in which users depend on their computers to do their jobs, IT staff should minimize the likelihood of disruption to working patterns, particularly from avoidable causes such as incorrect computer configurations and infection by malicious software.

The LUA approach can maintain productivity through maintenance of client computer configurations. When users cannot change the configuration of their computers, those computers are more stable, which leads to a reduction in

downtime and maintains productivity.

Lost productivity can also occur when malicious software takes over a computer. The computer may require disinfection or even reformatting, and the user may lose documents or data because of the infection. Administrators may have to restore backup copies of files, which may then need to be updated. These additional activities could distract employees from their current tasks or require them to repeat work.

Reduced Costs

Although maintenance of multiple client computers cannot be cost-free, the following factors can significantly increase these costs:

- Unique and untested combinations of hardware and software
- Unknown changes to the operating system
- Personalized system-wide settings
- Non-standard software with unknown file types
- Licenses for user-installed software
- Fines for unlicensed software
- Malicious software
- Beta software and drivers
- Internet bandwidth usage by malicious software

The LUA approach helps to prevent installation of unauthorized, unlicensed, or malicious software. It also prevents users from making unknown changes to their computers. These limits reduce the costs from help desk support and downtime that users with administrative rights can cause.

Reduced Piracy and Legal Liability Issues

Organizations are increasingly aware of their regulatory compliance obligations to prevent illegal use of company equipment by employees. These obligations require companies to take action when employees either knowingly or unknowingly:

- Allow customer data (for example, personally identifiable information [PII]) to be stolen.
- Host Web sites that contain pirated, illicit, or offensive content.
- Host relay servers for unsolicited commercial e-mail.

- Take part in distributed denial-of-service attacks.

Organizations that implement the LUA approach are significantly less likely to be found to have been liable for these types of abuses because their client computers are more difficult to compromise. In addition, users are less likely to be able to install unauthorized software to host illegal content, which significantly decreases the chance of their committing acts to cause such liability. This safeguard results from limited users having only read access to the Program Files folder, the Windows system folders, and to the **HKEY_LOCAL_MACHINE** section of the registry. Programs usually require write access to these locations to install.

Top of page

Risk, Security, Usability, and Cost Tradeoffs

Like many approaches to network management, adoption of LUA methods involves weighing the tradeoffs between risk, security, usability, and cost. When properly implemented, the LUA approach can:

- Reduce risk.
- Increase security.
- Impact usability.
- Reduce administration costs.

Reduce Risk

Any connection to a computer network incurs an element of risk, and connections to the Internet entail higher risk than those to intranet resources. The only way to remove this risk completely is not to connect a computer to a network. Most organizations agree that the business benefits of network connectivity outweigh the risks, but strategies that minimize those risks are a sensible precaution.

The LUA approach can lead to a significant reduction to both the current and future risks that result from programs running with administrative rights. Organizations that do not implement the LUA approach not only increase the risks associated with computer use, but are increasingly vulnerable to newer exploits, particularly zero-day exploits where attackers discover a software vulnerability before the manufacturer. Organizations that do implement the LUA approach are more likely to implement other desktop management strategies, such as automatic security update installation, which further reduces their risk profile.

Increase Security

The LUA approach provides greatly increased security. The tradeoff is reduced freedom for the user to make configuration changes, but not necessarily

reduced usability, as this next section discusses.

It is important to understand that the LUA approach does not provide a complete security strategy, but must integrate with other security defenses as part of a defense-in-depth strategy. These multiple defenses include user awareness, perimeter and host firewalls, regular security updates, and up-to-date scanners to detect malicious software. The LUA approach provides additional security that reduces the ability for malicious software to spread within an organization.

Impact Usability

The truism for network management is that usability and security are inversely proportional to each other, and that increased security reduces usability.

Note The important consideration is that usability should be about ease of use, not the ability of a user to make any change they want to their computer.

The LUA approach prevents users from administering their computers, not from using them. Removing administrative rights makes users more productive, because they have fewer distractions from their work and reduced opportunities to configure their computers incorrectly.

However, if the user can see a configuration option, but cannot change it, this can be a source of frustration and can generate help desk calls. Group Policy allows you to hide elements of the Windows interface from the user. If users only see the options that they can change, the configuration restrictions become significantly less frustrating. Implementation of the LUA approach in conjunction with Group Policy allows you to create a simplified interface that only shows the configuration options that the user can change.

Reduce Administration Costs

Studies from independent organizations have illustrated the long-term savings that network systems management can provide. The LUA approach ties in closely with a systems management strategy because limited users cannot change the enforced management settings. However, to realize the cost savings from systems management, organizations must be prepared to make the investment that the LUA approach requires, and understand the costs both of implementing and of not implementing the LUA approach.

Implementing the LUA approach incurs costs to:

- Plan and pilot the project.
- Test custom programs in a LUA environment.
- Investigate workarounds for limited user accounts.

- Rewrite applications, as necessary.
- Test new programs before deployment.
- Handle initial increase of calls to the help desk.
- Address the political issues of this change.

It is important to balance these costs against the costs associated with not implementing the LUA approach. Not implementing LUA can create costs from:

- Incorrect computer configurations caused by user modifications.
- Unauthorized, untested, unlicensed, or malicious software.
- Potential litigation.
- Lost business due to security compromises.

Analysis of the costs for implementation and non-implementation shows that most of the implementation costs are calculable, whereas the non-implementation costs are unknown. It is possible to assess the cost of rewriting a line-of-business application, but impossible to estimate the cost of a future lawsuit.

The rapid evolution of threats to networked computers and the requirement to simplify and standardize computer configurations will increasingly encourage organizations and individuals to run their networks and computers under limited user accounts. The arguments for the LUA approach are now making significant inroads into organizational inertia and established bad practice. It is now necessary to review how organizations can implement the LUA approach.

Top of page

Implementing the LUA Approach

Implementation of the LUA approach involves applying the following rules to computers running Windows XP:

- Non-administrators should always log on as limited users.
- Administrators should only use administrative accounts to carry out administrative actions.

Although this approach brings the benefits that this paper has already covered and enforces a fail-safe environment, many considerations need to be addressed, particularly when an organization has previously allowed users to log on as administrators.

Implementation Considerations

Implementing the LUA approach also creates technical, administrative, and

political issues within the organization. These issues include:

- Control over the computer
- Installing hardware
- Installing programs
- Running programs
- Updating the operating system
- Configuring the operating system
- Costs

Control Over the Computer

Possibly the most difficult political issue to cope with is that of control of the client computers. Many senior executives and business decision makers expect full control over their computers, and are unaware or dismissive of the risks from this configuration. People who hold executive positions are often intolerant of situations that frustrate them or messages that tell them what they cannot do. A typical response to any warning messages about restricted rights is to insist that the network administrator give them full administrative control.

To manage this situation, it is essential to have a suitably high-ranking and technically educated executive sponsor for the project. For many companies, this executive sponsor should be at least the Chief Information Officer (CIO) or equivalent, and willing to educate fellow management about the growing threat from malicious software and how such software can install from malicious or compromised Web sites. If education does not provide a forceful enough argument, highlight the issues of legal liability that could result from unintentional installation of malicious software on their computers, and explain how the tools in this paper can address any concerns.

User education is another important area to address. Most users will feel threatened by any attempt to remove control over what they see as "their" computer, and may take steps to disrupt implementation of the LUA approach. It is common to receive an increased number of complaints together with exaggeration of the issues that users now face because they no longer have administrative rights. As long as the organization has carried out a thorough testing program, these complaints are likely to be easily addressed.

Installing Hardware

Users with desktop computers in office environments should never require administrative rights. However, mobile computer users may legitimately need to install hardware such as printers and DVD writers to carry out their jobs

when they are not connected to the organizational network.

The hardware installation issue for mobile users is one for which organizations need to consider a range of options, possibly including options that do not conform to the LUA approach. The tools that this paper describes in the next section can also assist with hardware management in this situation.

Installing Programs

Many programs require administrative privileges to install. This behavior helps inhibit unauthorized programs from installing, but may also prevent the installation of authorized programs and upgrades. Program installation may be particularly problematic when the user does not have a domain-joined computer or only occasionally connects to the organization's network. Resolving the issue of how to install authorized programs and security updates may require both changes in operational procedures and the use of tools such as application publishing in Active Directory®, the Elevated Rights Deployment Tool in Microsoft Systems Management Server (SMS) 2003 with Service Pack 1, or Remote Desktop.

Some Internet sites only work correctly with additional software and ActiveX controls that download to the client computer. Management tools such as the Internet Explorer Administration Kit and Group Policy can allow this behavior with sites where the business need is greater than the perceived risk of allowing software downloads from that location.

Running Programs

Some programs require administrative privileges to run. Typically, this restriction comes from coding errors or poor implementation of programming and security guidelines. For example, a program might install a mandatory product key in a location in the registry where a limited user account cannot read the key's value.

Note Programs that follow Microsoft programming recommendations should not experience issues with security restrictions.

In many cases, it may be possible to address the issue by granting the Users group access to the restricted location that causes the application to fail. The Microsoft Windows Application Compatibility Toolkit (ACT) that this document describes in the next section can also address many of these incompatibility issues. Network administrators should not simply accept the argument that because one program only works with administrative permissions, everyone should be an administrator.

Updating the Operating System

The manual installation of operating system updates from the Microsoft Update Web site requires the operating system desktop to run with administrative rights, so, to use Microsoft Update, the user must log on with

administrative credentials. However, the Automatic Updates service runs under system account credentials and does not experience this restriction. If you configure Automatic Updates to check for and install operating system and program updates automatically, there should rarely be any requirement to update manually. For more information, see How to schedule automatic updates in Windows Server 2003, in Windows XP, and in Windows 2000, at http://support.microsoft.com/default.aspx?scid=kb;en-us;327838.

SMS 2003 with Service Pack 1 includes features to identify and install operating system and application updates without the user having administrative rights. Windows Software Update Services (WSUS) provides simplified security update management for organizations that do not have SMS installed.

Configuring the Operating System

Organizational IT policy should define what configuration actions limited users can carry out on their computers. Changes to security policies and registry settings, either locally or through Group Policy, can enable limited users to make these approved changes to their computer, such as when mobile users need to change the computer's time or time zone. The following section in this paper list several tools that address the issue of operating system configuration with a limited user account.

Costs

Finally, the LUA approach can be expensive to plan, implement, and manage. If you have third party or custom line-of-business or mission-critical programs, these costs can be significant.

One example might be a mission-critical program that is not compatible with the LUA approach and requires administrative rights to run. Depending on the age of the program and the developer resources available, the organization may need to:

- Test the program in a LUA environment.
- Identify a mitigating process if the program does not run, such as:
    - Customize registry permissions or amend permissions on multiple computers.
    - Change access rights.
    - Deploy tools to address configuration issues.
- Rewrite the program from scratch.

However, if the organization already plans to update the custom program to a newer technology, the cost of conforming to the LUA approach may be

insignificant.

Tools

Numerous tools are available from Microsoft and other software vendors to assist with the process of managing an environment that uses the LUA approach. This section describes some tools that help manage environments in which users log on with limited user rights. These tools include:

- Secondary Logon service
- MakeMeAdmin
- PrivBar
- PolicyMaker
- Application Compatibility Toolkit
- RegMon and FileMon
- Systems Management Server

Note MakeMeAdmin, Privbar, PolicyMaker, RegMon, and FileMon are not supported by Microsoft, and Microsoft makes no guarantees about the suitability of these programs. Use of these programs is entirely at your own risk.

Secondary Logon Service

The Secondary Logon service (or the runas command) enables users to run programs with alternate credentials. The Secondary Logon service creates another security token with the new credentials and group memberships, which the program uses to access resources.

Although the Secondary Logon service is a useful tool, the secondary account uses separate credentials from the primary account, which creates the following restrictions:

- The user must know the secondary account password, and has to supply those credentials.
- Some programs cannot run a second instance with different credentials from the current instance.
- The secondary account might not have the same printer and drive mappings as the primary account.
- The secondary account might be a local account, and so might not have access rights to network or domain resources, be able to run domain logon scripts, or apply Group Policy.

- Some changes (such as installation of programs) only apply to the secondary account's profile, not the primary. This effect can occur when a program installs for "This user only" rather than for "All users."

The runas command does not work when it is directed to use Universal Naming Convention (UNC) paths, such as to printers and network connections. There are workarounds that address this issue, such as using the runas command to start Internet Explorer and then opening folder-based objects in Internet Explorer. However, this approach lacks the simplicity of the "right-click and then click **Run As**" approach.

Other uses of the runas command include creation of a shortcut to a script in the user's **Send To** menu, which runs the selected program with administrative rights. Alternatively, shortcuts can have the **Run with different credentials** advanced option set. For more information, see How to enable and use the "Run As" command when running programs in Windows at http://support.microsoft.com/default.aspx?scid=kb;en-us;294676&sd=tech.

MakeMeAdmin

MakeMeAdmin circumvents the drive mapping, access rights, and program installation restrictions of the Secondary Logon service through use of two consecutive logon processes. To circumvent these restrictions, the script:

1. Obtains your current logon account details.
2. Invokes the Secondary Logon service so that you can log on with the local Administrator account credentials.
3. Uses the new local Administrator logon session to add your current account into the local Administrators group.
4. Invokes the Secondary Logon service again and prompts you to log on as your current user account, but as a member of the local Administrators group.
5. Creates a new command prompt in which your current account is a member of the local Administrators group. This command prompt has a different background color and title to distinguish it from a standard command prompt.
6. Removes your current account from the local Administrators group.

The command prompt that the script creates runs under your current logon account credentials but with administrative rights, and any program that you run from this command prompt also has administrative rights. Your drive mappings and network access rights are the same as your current account and if you use this command prompt to install a program, that program will install into your current profile, not the local Administrator profile.

For more information about MakeMeAdmin, see MakeMeAdmin -- temporary

admin for your Limited User account on Aaron Margosis' WebLog, at http://blogs.msdn.com/aaron_margosis/archive/2004/07/24/193721.aspx.

PrivBar

PrivBar displays a color-coded toolbar in Internet Explorer and Windows Explorer that shows the user's current privilege level. For example, if a user logs on with administrative rights, the PrivBar toolbar changes to yellow, with a red indicator. This indicator reminds users that they are using administrative privileges to browse a Web site, which increases the risk to their computer. For more information about PrivBar, see PrivBar -- An IE/Explorer toolbar to show current privilege level on Aaron Margosis' WebLog, at http://blogs.msdn.com/aaron_margosis/archive/2004/07/24/195350.aspx

PolicyMaker

PolicyMaker from Desktop Standard consists of a suite of utilities that extend the ability of Group Policy to enable the LUA approach with distributed networks. The PolicyMaker suite also includes tools to check and fix issues with program compatibility. The most significant tools for implementing the LUA approach include PolicyMaker Standard Edition, PolicyMaker Application Security, and PolicyMaker Software Update.

Of particular interest to the LUA approach is PolicyMaker Application Security, which enables network administrators to attach permission levels to individual programs. The network administrator selects the program, and then removes security groups from the process token when that program starts. This restriction then propagates through Group Policy. For more information about PolicyMaker, see PolicyMaker Overview on the Desktop Standard Web site, at www.desktopstandard.com/PolicyMaker.aspx.

Application Compatibility Toolkit

The Microsoft Windows Application Compatibility Toolkit (ACT) is a collection of tools and documents that assist IT professionals and developers to achieve the highest levels of application compatibility with the Windows operating systems. Tools include:

- **Application Analyzer**. This tool simplifies application inventory and compatibility testing.
- **Compatibility Administrator**. This database lists the necessary compatibility fixes to support outdated programs in Windows.
- **Internet Explorer Compatibility Evaluator**. This tool provides detailed logs about Internet Explorer that records application compatibility issues with this browser.

The Compatibility Administrator includes tools that enable a developer to check for user permission issues during the development stage of custom applications. The ACT can generate a compatibility fix that the administrator

can deploy to users' computers. The compatibility fix then enables the program to run in LUA mode by redirecting application calls to locations where the limited user has read and write access. For more information about the ACT, see Windows Application Compatibility at www.microsoft.com/technet/prodtechnol/windows/appcompatibility/default.mspx.

RegMon and FileMon

RegMon and FileMon are two utilities from the well-respected Sysinternals Web site. RegMon displays registry access activity in real time, listing each call to the registry that an application makes, and logging the outcome. This tool allows you to identify when an application cannot access a registry key. Similarly, FileMon displays file system activity in real time, listing each system call that an application makes and registering the outcome.

RegMon and FileMon enable administrators to test an application within a LUA environment and to identify the failure of any calls that the application makes to the registry or file system. The administrator can then mitigate that failure, for example, by changing file system or registry key permissions. Group Policy can propagate these permissions changes to multiple computers. For more information about these utilities, see the Sysinternals Web site at www.sysinternals.com.

Systems Management Server

Microsoft Systems Management Server (SMS) 2003 is a fully featured desktop management system that provides management services for medium and large organizations with either centralized or distributed networks. These management services include installation of sotware and security updates.

SMS provides support for the LUA approach through the ability to install software and security updates without the requirement for users to log on with administrative rights. For more information about SMS, see Systems Management Server 2003 SP1 Product Overview at www.microsoft.com/smserver/evaluation/overview/default.mspx.

Limiting Administrative Credentials

If an organization is unable to implement the LUA approach in full, it is possible to mitigate the risk from running programs with administrative rights by ensuring that any programs that access network resources always run with limited user rights. Although this approach does not comply with the principle of least privilege, it does offer some benefits, and is better than simply allowing everyone to run all programs with administrative rights.

To provide effective security when users log on with administrative rights, you will need to:

- Deploy tools to minimize the risk of running programs as administrator
- Ensure that Internet-facing programs such as e-mail, browsers, and

instant message clients always run with limited user rights. Allowing such programs to run with administrative rights are the most common methods for introducing malicious software into an organization.

- Monitor computers for unapproved administrative usage. For more information on security monitoring, see The Security Monitoring and Attack Detection Planning Guide, at www.microsoft.com/technet/security/guidance/auditingandmonitoring/securitymonitoring/default.mspx.

The following tools help to minimize the risk of computer compromise when users log on with administrative rights. In addition, some of the tools from the "Log on as a Limited User" section also apply in this situation.

- Secondary Logon service
- Software Restriction Policies
- DropMyRights

Note DropMyRights is not supported by Microsoft, and Microsoft makes no guarantees about the suitability of this program. Use of this program is entirely at your own risk.

Secondary Logon Service

The Secondary Logon service provides an option to run a program as a less privileged account. For example, in Windows XP with SP2, users' desktop icons for Internet Explorer could be replaced with versions that invoke the run as dialog, which then shows the **Protect my computer from unauthorized program activity** option. This option disables security identifiers (SIDs) in the user's access token in a similar fashion to the DropMyRights tool described later in this section.

Software Restriction Policies

Software restriction policies are part of Group Policy and provide the ability to regulate unknown or untrusted software. Software restriction policies can apply one of three possible settings to programs. These settings are:

- Unrestricted
- Disallowed
- Basic user

Note Only Unrestricted and Disallowed are visible by default. To view the Basic user setting, you must edit a registry key. For more information, see Browsing the Web and Reading E-mail Safely as an Administrator, Part 2, at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/

html/secure01182005.asp.

In summary, unrestricted programs can run without hindrance, disallowed programs cannot, and programs that have the Basic user setting applied can only run with limited user rights. This approach enables you, for example, to configure a software restriction policy that always runs Internet Explorer as a limited user.

Software restriction policies can also prevent the execution of malicious software from certain locations, such as the Internet Explorer temporary files folder. A software restriction path rule could disallow any program that attempts to run from the temporary Internet files folder. Group Policy can apply this rule to all computers in the domain.

For more information about software restriction policies, see Using Software Restriction Policies to Protect Against Unauthorized Software, at www.microsoft.com/technet/prodtechnol/winxppro/maintain/rstrplcy.mspx.

DropMyRights

DropMyRights disables SIDs and removes privileges from the user's access token, and then uses this restricted token to start a specified program. DropMyRights enables a user to log on with administrative rights and then run a program at one of three privilege levels:

- Normal
- Constrained
- Untrusted

Note The *normal* privilege level corresponds to a limited user account. The *constrained* level is even more limited due to the addition of restricting SIDs to the access token. The *untrusted* level has only minimal access rights, and most applications will not function at this level.

For example, a user with administrative privileges may need to browse a Web site. The user can run Internet Explorer from a shortcut that invokes DropMyRights, and that shortcut would specify that the program should run as a constrained user. This instance of Internet Explorer then has minimal rights on the client computer, which makes it significantly less likely that any malicious programs could install or run.

For more information about DropMyRights, see Browsing the Web and Reading E-mail Safely as an Administrator, at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dncode/html/secure11152004.asp.

For more information about the effects of running Internet Explorer as a constrained user, see Running restricted -- What does the "protect my computer" option mean? at http://blogs.msdn.com/aaron_margosis/archive/

2004/09/10/227727.aspx.

Top of page

Future Developments

Windows Vista includes features that will enhance protection for user accounts. Windows Vista will enable users to work effectively with limited user accounts, and Windows Vista–certified programs will have no trouble running under limited user accounts. When older programs attempt to write to protected areas of the registry such as the **HKEY_LOCAL_MACHINE** section, Windows Vista will redirect those writes to the **HKEY_CURRENT_USER** section instead. However, as vendors update their programs and certify them for Windows Vista, operation under the LUA approach should become common practice.

Windows Vista also improves usability. If a user tries to make a change that requires administrative rights, Vista automatically prompts the user to enter administrative credentials.

Increased protection for user accounts is just one of the major improvements to security in Windows Vista. As organizations upgrade to Windows Vista, the opportunity for malicious software to exploit administrator-level accounts should diminish. For more information about user account protection in Windows Vista, see the Windows Vista Web site at www.microsoft.com/windowsvista/it-professionals.mspx.

Top of page

Summary

The growth in threats to networked computers requires organizations of all sizes to implement a defense-in-depth strategy. Implementing the LUA approach on computers that run Windows XP provides an important component of this strategy.

The LUA approach counteracts the tendency of many organizations to give administrative rights to client computer users through membership in the local Administrators group. This paper highlights the inherent dangers in giving administrative rights to all users, because doing so gives administrative privileges to any program that the user runs. It is particularly important that Internet-facing programs such as browsers, e-mail readers, and instant messaging clients should not usually run with administrative rights, because this configuration renders the client computer significantly more vulnerable to attack.

To return briefly to the example at the beginning of this paper, if the organization had implemented the LUA approach, the executive would have browsed the compromised Web site as a limited user rather than as an administrator. The malicious software may not have been able to infect his portable computer and the executive would have been able to deliver that

knockout sales presentation that could have secured the sizeable order.

Finally, the LUA approach is not a solution by itself, but must integrate with other security defenses. These defenses include user awareness, perimeter and host firewalls, regular security updates, and up-to-date scanners to detect malicious software.

Top of page

Resources

For more information on using the LUA approach in Windows XP, consult the following resources:

- Aaron Margosis' Web Log at http://blogs.msdn.com/aaron_margosis
- Michael Howard's Web Log at http://blogs.msdn.com/michael_howard
- The nonadmin Web site at http://nonadmin.editme.com
- The Administrator Accounts Security Planning Guide at www.microsoft.com/technet/security/guidance/serversecurity/administratoraccounts/default.mspx
- The Windows XP Security and Admin. newsgroup on TechNet at www.microsoft.com/technet/community/newsgroups/dgbrowser/en-us/default.mspx?dg=microsoft.public.windowsxp.security_admin.
- TechNet Webcast: Limited User Access: The Good, the Bad and the Ugly (Level 300) at http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032278618&EventCategory=5&culture=en-US&CountryCode=US
- TechNet Webcast: Tips and Tricks to Running Windows with Least Privilege (Level 300) at http://msevents.microsoft.com/CUI/WebCastEventDetails.aspx?EventID=1032274954&EventCategory=5&culture=en-US&CountryCode=US
- The Microsoft Security Developer Center at http://msdn.microsoft.com/security/default.aspx
- The Developer Best Practices and Guidelines for Applications in a Least Privileged Environment white paper at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnlong/html/AccProtVista.asp
- The Developing Software in Visual Studio .NET with Non-Administrative Privileges article at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dv_vstechart/html/tchDevelopingSoftwareInVisualStudioNETWithNon-

AdministrativePrivileges.asp

- Writing Secure Code, Second Edition by Michael Howard at www.microsoft.com/MSPress/books/5957.asp
- The How to Troubleshoot Program Compatibility Issues in Windows XP article at www.microsoft.com/technet/prodtechnol/winxppro/support/troubleshoot.mspx
- Department of Defense Trusted Computer System Evaluation Criteria (Orange Book) at http://zedz.net/rainbow/5200.28-STD.html.

Top of page

Acknowledgments

The Microsoft Solutions for Security and Compliance group (MSSC) would like to acknowledge and thank the team that produced *Applying the Principle of Least Privilege to User Accounts on Windows XP*. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

Author

Anthony Steven, *Content Master Ltd*

Writer

Mike Danseglio

Testers

Gaurav Singh Bora, *Infosys Technologies*

Mehul Mediwala, *Infosys Technologies*

Editors

Jennifer Kerns, *Wadeware*

John Cobb, *Volt Information Sciences*

Program Manager

Tom Cloward

Release Manager

Flicka Crandell

Contributors

Tony Bailey

Darren Canavor

Karl Grunwald

Kelly Hengesteg

Karina Larson, *Volt Information Sciences*

Chrissy Lewis, *Siemens Business Services, Inc.*

David Mowers

Jeff Newfeld

Bomani Siwatu

Stacy Tsurusaki, *Volt Information Sciences*

David Visintainer, *Volt Information Sciences*

Reviewers

Bob Blank, *Target Corporation*

Jeremy Brayton, an independent reviewer

Derick Campbell

Chase Carpenter

Romulo A. Ceccon, *Dataprom*

Matt Clapham

Chris Corio

Greg Cottingham

John Czernuszka

Michael Dragone, *Titleserv, Inc*

Dana Epp, an independent reviewer

Stephen Friedl, *Microsoft Security MVP*

Guido Grillenmeier, *Hewlett-Packard*

Michael Harradon, *Netivity Solutions*

Robert Hurlbut, *Hurlbut Consulting, Inc*

Mark Kradel

Jamie Laflen

Alex Lee, *Sprint Nextel Corporation*

Kevin Lundy, *CAE, Inc*

Tim C. MalcomVetter, *Truman Medical Centers*

Aaron Margosis

Brian Marranzini

David McClure, *Siemens Medical Solutions*

Don McGowan

Michael Miller, *Media General, Inc*

Charles J. Palmer, an independent reviewer

Keith Pawson, an independent reviewer

Brian A. Reiter, *WolfeReiter, LLC*

Michael Rickard, *Bristol University*

John Robbins, *Wintellect*

Alex Rublowsky

Mike Smith-Lonergan

Mike Sorsen, *Edward Jones*

Didier Stevens, *Contraste Europe*

Eric Wood

Martin Zugec, an independent reviewer