PENNSTATE

1855

# Operating in Least Privilege Mode White Paper

**Information Technology Services**

**May 22, 2009**

**TABLE OF CONTENTS**

## I. Introduction

The threat vector of the Internet continues to become more complex, posing an urgent need to secure and protect the information with which we work at Penn State. Additionally, the federal and state statutes that Penn State must meet continue to increase and require more stringent security measures.

The security posture at Penn State must change to a more consistent and protected environment for our networks and systems which stores sensitive data. One of the more prominent areas that need to be enhanced is the protection against evolving threats and vulnerability trends, which often lead to compromises.

A compromised machine with Personally Identifiable Information (PII) could lead to sensitive information being transmitted to unauthorized entities that use the information to steal identities and compromise bank and credit card accounts. The loss of such data can lead to institutional reputation damage and cause significant financial loss to the University. The Pennsylvania State Data Breach Notification Law requires notification to affected individuals for the loss of certain information, including Social Security Numbers (SSNs) or driver's license numbers, among other data considered to be sensitive information.

An essential initiative is underway at Penn State to help mitigate the risk of compromises and loss of PII by practicing the principal of least privilege for computers that are connected to the Internet. Machines that are never connected to the Internet or network may not require as stringent security measures with administrative privileges. A report from BeyondTrust based on all vulnerabilities published in Microsoft's 2008 Security Bulletins and Reports, indicates 92% of critical vulnerabilities can be mitigated by removing administrative privileges.

Users with a valid requirement for administrative privileges may be granted an elevated account by applying for an exception through their chain of command. A need for an exception may include, but is not limited to, faculty or staff who: a) connect to certain equipment or devices that cannot, within reason, be upgraded or replaced to the modern versions not requiring administrative access to operate; b) frequently test or use new software; c) travel frequently and have needs which require specific setting changes. This does not mean the requester may operate as an administrator, but rather they will operate with a set of regular user privileges and work in an elevated mode when it is required by the software or to perform a particular task. When the task is complete, they should switch back to normal privileges.

Several departments at Penn State have successfully gone through limiting the use of local administrative privileges (practicing the concept of least privilege) in their respective areas. Some have reported a significant decline in helpdesk requests after removing administrative privileges. When properly planned and implemented, the process of operating in a least privilege mode will successfully help to mitigate the overall risk and unauthorized exposure of sensitive employee, student, alumni and customer data.

## II. Definitions

### *A. Local account*

A local account controls a level of access to an individual computer and determines rights for running programs, installing and removing programs, accessing files and enabling or disabling services on the local machine.

### *B. Administrator account*

Administrative privilege is the highest level of permission that allows unrestricted access to create, delete and modify files, folders and settings on a particular machine.

### *C. Least Privilege*

The principle of least privilege is based on the nature of work conducted by each employee. Access to electronic and physical systems and files should be restricted to only those with a legitimate business need-to-know. Legitimate needs may include working directly with that systems or data on regular basis in order to conduct normal business activities. Overall, working with the least privilege concept, helps to mitigate vulnerabilities which often lead to computer compromises.

## III. Threats/vulnerabilities

Running as a local administrator has many associated vulnerabilities. This elevated account can allow the common malware infection, such as a "drive-by download" to execute without the end-users knowledge. Malicious code comes in many forms and is often used for profit and organized crime. Infectious malware can be delivered in through a virus or worm. Concealment malware is delivered through Trojan horses, rootkits and backdoors. Generally these are well hidden from the user and very hard to detect even if a compromise occurs. Personally Identifiable Information can become compromised through any of these methods.

Attack vectors can come through well-known, reputable sites and are creating a compromise through SQL injections, malicious advertisements, search engine result redirection, cross-site scripting attacks, vulnerabilities in the Web server or forum hosting software and attacks on the backend virtual hosting companies.

The Commonwealth of Pennsylvania has a Breach Notification Law and requires notification to the affected parties be made for each record lost. According to the Fourth Annual US Cost of Data Breach Study conducted by the Ponemon Institute estimates the cost per lost record at $202.00.

## IV. Exception Process

The System Administrator is responsible for maintaining a safe and secure network environment, per Policy AD 20, "*Computer and Network Security.* Depending on employees' nature of work, the need for administrative privileges may exist. A process should be developed at the administrative area level and approved by the Chancellor, Dean, or Department Head to evaluate each exception and determine whether administrative privileges are really needed, or if another process can be put into place as a work-around. The process should include how to apply for an exception, who will review and approve the exception and how the granted administrative privileges will be implemented. A need for an exception may include, but is not limited to, faculty or staff who: a) connect to certain equipment or devices that cannot, within reason, be upgraded or replaced to the modern versions not requiring administrative access to operate; b) frequently test or use new software; c) frequent travel needs that require specific setting changes.

## V. Using Least Privilege Mode

The Least Privilege Mode can help to alleviate electronic vulnerabilities and helps protect against malware, malicious users, and security breaches. When running in a limited user account mode, the risk of malicious code execution is reduced. Additionally, network and

system files cannot be changed or altered by unauthorized users. The Least Privilege Mode concept goes beyond just electronic security, but also exists to limit access to only those with a business need-to-know or access any type of data, electronic or physical.

## VI. Policies and Guidelines

### *A. University Policy*

University policy AD20, "*Computer and Network Security*". *Direct reference:*" **System administrators** (as defined in the Glossary of Computer Data and System Terminology, ADG01). Unless otherwise stated, system administrators have the same responsibilities as system users. However, because of their position, system administrators have additional responsibilities and privileges for specific systems or networks. For systems which they directly administer, system administrators are responsible for:

Section f of the policy, AD20 "Limiting access to root or privileged supervisory accounts. In general, only system administrators should have access to such accounts." System users should generally not be given unrestricted access to root or privileged supervisory accounts. As with all accounts, authorization for root or privileged supervisory accounts must be approved in accordance with this policy.

### *B. Data Classification Scheme*

The Security Matrix of the Data Classification Scheme Section 3.1.4 "Local Administrator Rights will be disallowed to general users for both public and non-public data." This document can be linked to in the resources section.

### *C. Internal Policy*

Regardless of what method is used to manage administrative privileges, it is recommended an internal department policy be developed which clearly outlines the process and understanding between the end-user and the Information Technology (IT) staff. Administrative area policies need to be developed to outline specific internal policies on administrative privileges and should detail the exception process (process, point of contact, etc.). Resistant employees regarding administrative privileges may be directed to Security Operations and Services (security@psu.edu).

## VII. Available Tools/Options for Local Administrator Management

### *A. Virtual Machine (VM) environment*

There are multiple Virtual Machine (VM) software packages available. The most common is VMware. In conjunction with the Ace security appliance, this tool is an effective method to manage administrative privileges. When properly administered, VM environments are separate from the core Operating System (OS) and other core system components, which pose less of a threat to the overall system. End-users can gain access to the elevated account by simply logging into the VM environment by double-clicking on an icon on their desktop. A system reboot is not necessary to change between the two.

Since the VM environment is separate from the core OS, information installed cannot be moved over to the main OS unless transferred over through another

medium such as a USB Key or CD. The VM environment allows testing to be conducted securely and any flaws that occur during testing will not affect the other applications on the core OS.

### *B. Software*

**BeyondTrust:** BeyondTrust Privilege Manager (www.beyondtrust.com) is a known software tool which enables end-users to run required Windows applications, processes and ActiveX controls while keeping a secure and compliant environment. The operation of BeyondTrust Privilege Manager is transparent to the end user; there are no pop-ups or consent dialogues. The software is integrated with Active Directory and is applied through Group Policy. The policy is applied by creating rules in the Group Policy Object Editor. Through a three step process, policies can be set. Windows 2000, XP, Server 2003/2008, Vista and 64-bit platforms are supported with this software.

**Sudowin** is an open-source add-on that allows for simple privilege escalation on a per-user and per-application basis. Unlike using a "run-as" in Microsoft Windows, Sudowin will allow escalated privileges in the same user mode.

Sudowin comes as a .MSI package which can be configured in two steps:

1. Users can be added to a specially created user group for sudo privileges
2. An .XML file can be configured to control the way the users' sudo privileges work. This step involves the most work and could be more labor-intensive out of the two for large-scale deployments.

### *C. Create two local accounts (administrator and least privilege)*

Creating two local accounts (one with admin privileges and one with least privilege – do not use the root administrator account) is the most cost effective solution which does not require additional funds to implement. End-users should use the least privilege for their everyday operations and only use the administrative privilege account when absolutely necessary, such as when new software needs to be installed or another process needs to be implemented and can only be done with elevated privileges.

Unlike Sudowin, the "run as" command is run from an entirely different user identity, obviously one that has administrative privileges. In some cases, desktop applications running without User Access Control (UAC) privileges may not interact properly with those that are running through UAC since they are not operating in the same user space.

Regardless of what option is selected to manage administrative privileges, each must be clearly written in a local policy stating users should only use the administrator privilege when absolutely necessary, and if an exception has been granted for one of the alternative solutions.

## VIII. Implementation

### *A. Organize a Team*

It is important to involve and gain support from senior leadership in respective areas at the beginning. Multiple teams may be formed to address each initiative for this project.

Suggested representatives for the team may include the dean and/or chancellor, a faculty member, IT director/supervisor, system administrator and an end-user.

### *B. Conduct an Assessment*

Determine who currently has administrative privileges. If a sound inventory of computers has not already been established, the initial assessment may help to build one. When conducting an initial assessment for gauging who has administrative privileges, consider other security-related initiatives that may be implemented during the process – such as encryption or scanning for Personally Identifiable Information (PII). Also consider a standard build for employees and add additional software and hardware as needed.

### *C. Develop a Plan (create strategy and timeline)*

Consider how this will affect each employee and when the best time would be to make the change. For example, the middle of the semester may not be a good time to implement this process for faculty. The process may be rolled out when machines are recycled or in groups.

### *D. Raise Awareness*

It is important to raise awareness prior to implementation to allow employees to digest and become familiar with the proposed change. A plan should already be developed and detailed during the awareness sessions. Some areas of the plan may change depending on the feedback received when raising awareness (valid points may be raised).

### *E. Start Implementation*

- Organize a team to specifically address administrative privileges. Targeting areas for the team to address should include assessment, awareness, and implementation.
- The final step should be implementation. There are several ways to manage administrative privileges and to roll out the process. The team should determine which solution is the best one for the respective college/administrative area or department.

## IX. Frequently Asked Questions

### 1. What is the rationale behind this initiative?

Computer security is the primary driving force behind this change in user account management procedures. In recent years the hackers have significantly increased their ability to compromise systems, making these systems participants in illicit activities or resulting in them being vulnerable to harvesting of institutional data or intellectual property. The majority of daily business related computer operations do not require administrator (privileged) account access because few individuals need to install or update applications every day. Furthermore, there are a significant number of administrative computing users that cannot point to any business reason for having administrator control of their computer.

### 2. Why the change in operating philosophy?

It is true that some systems within the University were originally configured to allow all users to administer their computer; but, this was in a time when computer hackers were not as sophisticated and able to remotely install detrimental software as easily as they can today. Unfortunately, even relatively benign and official/well-known web sites have unknowingly been compromised and contain malicious code that automatically downloads and installs an application merely by a user visiting the site and/or selecting a seemingly valid web page link.

The downloading and installation of malicious code happens in the background; so, unsuspecting users have no idea that their computer has been compromised. A compromise can be anything from installation of software that harvests data from a disk, monitors keystrokes, or enrolling the computer as a "BotNet" relay.

### 3. How does "Least User Privileges" affect daily operations?

Most users can perform their normal business functions without noticing anything different. However, a user may not be able to install software on their computer while operating in this mode; the benefit is that both hackers and users are prevented from inadvertently downloading and installing a malicious application from the web, infected USB drives, etc.

### 4. How may individuals install software if "Least User Privileges" are enforced?

If an individual has a valid need to install software on their computer and has an exception granted to have administrative privileges, there are multiple ways depending on what mechanism the college/campus/administrative area/department is using to manage the elevated privilege. If an exception has not been granted, contact the local IT staff in your area to request the software be installed.

If dual accounts are being used on a computer, the following procedure can be used for installation.

- The user can run a specific program (such as a software installer) with administrative privileges using the "Run As" feature of Windows XP. Both Vista and Apple OSX simplify this procedure by prompting a user to enter the Administrator account name and password under which to run the installation. In all case, the administrative privileges are terminated once the installation is complete.
- A second alternative is to log out of the "Least User Privileges" account, log into the "Administrator Account", install the software, and then log out of the "Administrator Account" and back into the "Least User Privileges" account.

If using SudoWin and need to install a program using an executable file, you simply right-click it and choose "Sudo" then enter your password in the resultant pop-up box.

VMware will require a login into a separate OS, which will be where the VM host resides.

It should be stressed that the use of "Administrator Account" privileges should be restricted to those individuals that require this type of access: faculty, department IT personnel, and selected individuals that have the need for such an account. Operating computers in a "Least User Privileges" mode is a best practice for everyone; users should never routinely operate their computer in an Administrator Privilege mode.

### 5. Are there any issues with migrating to a "Least User Privileges" account?

Some applications (for example, WordPerfect and Eudora) may encounter problems when a system runs in the "Least User Privileges" mode. Most of these problems have been successfully addressed by modifying the permissions for the folders used by these programs. For the very few programs that must run with administrative privileges, commercial utilities are available to allow these programs to run with system level privileges while the login account continues to run in "Least User Privileges" mode.

**6. Has the "Least User Privileges" account operation been fully tested?**

There have been a variety of college and campus locations that have successfully gone through this process, including the College of Liberal Arts, Penn State Hazleton and the College of Engineering.

## X. Resources:


*"Web Based Attacks White Paper"*, Symantec, February 2009. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf.

"*Reducing the Threat from Microsoft Vulnerabilities: 92% of Critical Vulnerabilities can be Mitigated by Removing Admin Rights*", BeyondTrust Report. http://www.beyondtrust.com/documentation/whitePapers/wp_VulnerabilityReport.pdf
"*Computer and Network Security*", Penn State University Policy, AD20. http://guru.psu.edu/policies/AD20.html

"*Data Classification Scheme, Data Classification Levels and Minimum Security Standards*" Penn State University https://wikispaces.psu.edu/display/DCRFC/Data+Classification+Levels,+Minimum+Security+Standards+RFC

*"Using sudowin to grant administrator privileges in Windows"*, November 2007, Search Security, http://searchsecurity.techtarget.com.au/tips/21905-Using-sudowin-to-grant-administrator-privileges-in-Windows

*"Fourth Annual US Cost of Data Breach Study"* January 2009, Ponemon Institute, http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/2008-2009%20US%20Cost%20of%20Data%20Breach%20Report%20Final.pdf