Realtime publishers

"Leading the Conversation"

The Essentials Series:
Eliminating Administrator Rights

Understanding Least Privilege

sponsored by

by Greg Shields

Understanding Least Privilege 1
Least Privilege Is More than Eliminating Admin Rights 2
Breaking Apart Least Privilege 3
The User's Role 3
The Available Tasks 4
The Corporate Policy 4
Least Privilege Inhibits Inappropriate Behaviors 5

Copyright Statement

Understanding Least Privilege

"We're still using that ancient corporate application and it requires Administrator privileges on every desktop to run…"

"The CIO told me he needed Admin rights on his laptop due to his travel schedule…"

"Without Administrator privileges, our Help desk is forced to do all the work for customizing users' desktops, and they're just overloaded…"

The likelihood is great that you've experienced one or more of these situations at some point in your IT career. Ancient and poorly coded applications require Administrator privileges at every desktop for their correct functionality. Executives and individuals of power within organizations pull rank to be exempted from company security policy. Strained Help desk personnel succumb to peer pressure from employees to "just give me rights and I'll take care of myself." In all of these situations in the world of IT, individual user privileges are inappropriately expanded due to the operational needs of the day.

But each and every time those privileges are expanded unnecessarily as a global resolution to an individual problem, the end result is a reduction in environment security. Every time elevated privileges are handed out to solve today's problem, this action invariably causes bigger issues down the road.

All of these situations relate to and are resolved through the implementation of the concept of "Least Privilege." The Principle of Least Privilege was developed more than 30 years ago by the US government's Department of Defense (DoD). Looking at computer systems from the perspective of complete security, the DoD defined Least Privilege in that day as:

> *[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges…needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.*

Today, the concept of Least Privilege is used to identify a state at which the lowest level of privileges are assigned to computer system elements while still enabling needed activities to be accomplished.

Least Privilege Is More than Eliminating Admin Rights

The previous definition effectively says that any action you attempt to accomplish with a computer must be done with the absolute lowest level of privileges required to accomplish that task. For many administrators, this equates to getting rid of administrative rights wherever possible within the organization. But eliminating admin rights on servers and desktops only accomplishes part of Least Privilege's lofty goals. Accomplishing its goals means digging deeper into the functionality of the operating system (OS) to enable those fewest privileges necessary to perform authorized tasks. Succeeding requires a few additional steps beyond merely eliminating admin rights on user desktops:

- *First, think outside the "Administrator" box.* Assigning a user to the Administrators group grants that user complete power over the processing of his or her computer system. Yet a user often needs elevated privileges for only a single or a few actions on that system. Granting the user complete power over that system for the purposes of solving a single need is unnecessarily excessive.
- *All types of person-based privileges are too coarse.* Many organizations initially attempt to reduce user access by converting unnecessary Administrators to other access levels such as Power User. Though this movement has the tendency to reduce that user's overall level of access, these "person-based" privileges are still exercised over an entire computer. This process of changing the user's assigned role still grants the user those privileges over every aspect of the computer system. This result is still not granular enough to truly fulfill the needs of Least Privilege.
- *Control privileges at a per-process or a per-application level.* When a user works with a computer system, that user is launching various applications and processes on the system. Those applications and processes enable the user to work with data and accomplish job tasks. Controlling the level of privileges assigned to each process or application eliminates the need for privilege assignment based on who the user is. Rather, privileges can be assigned based on the combination of who the user is and what the user needs to do.

Breaking Apart Least Privilege

Ultimately, the goal of Least Privilege is in assigning privileges to users based on the intersection of the role held by the user, the tasks the user needs to accomplish, and the policy of the organization. Figure 1 provides an example of this intersection. This combination of who the person is as defined by their assigned role within the organization, the actions required as a part of their role, and when those actions are considered appropriate ensures the greatest level of control over the user's interactions with the organization's computer systems. The next three sections discuss each of these three elements in more detail.

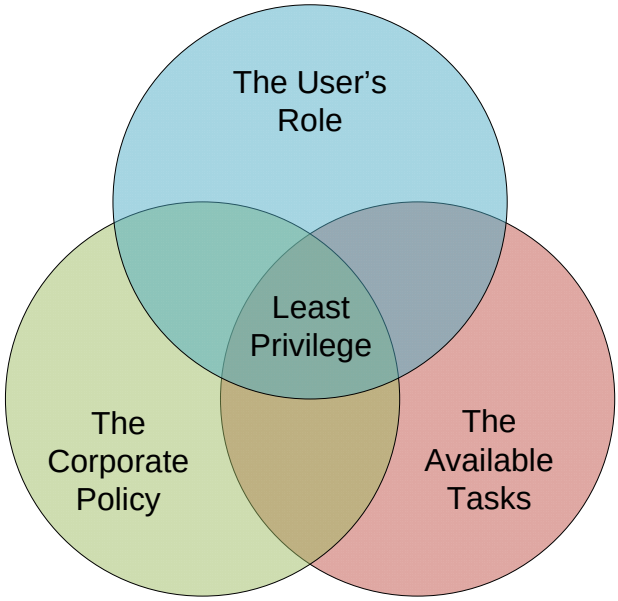

Figure 1: Least Privilege is involved with the intersection of the three elements shown.

The User's Role

Each user within an organization has a role to play in the operation of business. A user in the accounting department may require access to financial documents. A salesperson needs the use of the sales application and customer database. Users in IT require access to administrate systems. Each user's role is involved with completing one aspect of the needs of the business.

The role element of Least Privilege is used first in combination with the task element to be discussed in the next section. Roles in an organization are mapped to logical roles within an OS for the purpose of later identifying the activities allowed and not allowed by that role. Continuing with the previous example, the accounting department user may be assigned to the Accounting role within the OS.

The Available Tasks

Within an organization are also a number of tasks that must be accomplished in order to achieve the goals of business. Mapping those tasks to the services available within the organization's computing environment illuminates a list of activities and applications. As examples, those activities may relate to the ability to add printer drivers, change network settings, or customize a user's desktop. Within the realm of applications, tasks may be related to the ability to launch a spreadsheet tool, connect to a database client, or make use of a customized line-of-business application.

Each of these activities and applications is identified by the OS process that drives its functionality (for example, winword.exe is the process that drives Microsoft Word). Some of these tasks operate natively within the context of a standard user account with little or no added privileges necessary for their functionality. These tasks are configured by default to use the least privileges necessary for their processing. Others may require elevated access within the computer system to complete their actions. When necessary, those specific and identified processes are selectively granted the rights necessary to accomplish their mission.

Through this process of selectively granting privileges based on the need of the process, users can be given the exact level of permissions needed to accomplish their roles as a function of their needed activities and applications. Effectively, instead of applying privileges based on who the person is, privileges are assigned based on what users need to do.

The Corporate Policy

The third segment of Least Privilege relates to the period of use for both the user and the application. This period of use is determined by the goals and standards set by corporate policy. This third segment is necessary as a business changes over time. With that evolution comes changes in the practices and processes of business. For example, consider a user who spends the majority of their time away from the office and in the field. They may require more administrative access to their laptop because they are far removed from the assistance of the local Help desk. Later on, the business may acquire new technology that enables the Help desk to assist remote users, negating the need for them to retain administrative rights. With this change comes the end of the need for the user's elevated privileges on their identified computer.

Individual activities and applications have life cycles as well. Although the organization might desire its workforce to have the elevated rights necessary to accomplish a system task today, the organization may later determine that centralized control is more desirable. Version one of a custom line-of-business application may require elevated privileges due to faults in its code architecture, while version two overcomes these faults and no longer requires the elevated privileges. In all of these cases, the period of use of the user and the application must be controlled in order for Least Privilege to be most appropriately used.

Least Privilege Inhibits Inappropriate Behaviors

Throughout this definition of Least Privilege, the end result is in reducing or eliminating system behaviors that are considered inappropriate by the business. Behaviors—whether invalid software download and installation, the inappropriate changing of system settings, or the unintended introduction of malware and other unwanted software onto computers— can be eliminated or reduced through the application of Least Privilege.

The next article in this series will discuss these behaviors in depth through its discussion of the business benefits of implementing Least Privilege. The third article will continue the discussion by looking at limitations in the native solutions available today within the Windows OS. It will explore feature sets that are necessary to ensure that the goals discussed in this article can be accomplished with success.