Global Information Assurance Certification Paper

Enterprise Security Administration

System and Application Access Management Exposures and Vulnerabilities

Wiley Vasquez

Improper access management is in many cases a key vulnerability for potential information theft, manipulation and exploitation. This document outlines exposures and vulnerabilities that exist within because of improper access management. Security administration involves the function of enabling people and programs to perform particular actions. The actions themselves may not seem to be of significant importance. It is very important however, that the abilities be managed appropriately. This is for the protection of the user for which the accesses and the organization as a whole.

It is typical for users to inadvertently read, delete or modify a file. Depending on the circumstance, any one of these actions could be disastrous.

Company's employ information security administration professionals, which are responsible for managing user, system and application ID's and access permissions of these ID's.

In itself, the definition of security administration access management is quite simple. In practice however, it is involved, detailed, and requires extreme attention. Of concern of improperly managed security accesses are exposure and vulnerability. At risk, are company and personal assets, resources and sensitive and business-operational information.

Unauthorized Accesses

In any organization, change is eminent. In particular, we will focus on personnel changes. These changes can result from promotion, re-organizing, departures, terminations, etc. Historically when these personnel changes occur, the appropriate access control measures are not taken. This oversight or incompleteness creates an exceptional vulnerability. Especially when proper access control review maintenance policy does not exist or practiced. This is important because we have to remember that security administrations are not excluded from personnel changes.

UserID's that fall into this category can be identified as:

- User ID's that exist for persons whom are no longer employees
- User ID's which are given additional to the accesses previous in a different position.
- Special purpose ID's for programs or tasks that are no longer necessary

When UserID's that fall into this category are not properly accounted for and maintained, the data for which they had access or could create additional accesses for, becomes exposed. More important and subject to many issues outside the scope of this paper, the

data's integrity for which these UserID's had modification access privileges is questionable and possibly even unreliable.

Inappropriate Permissions

In the extremely busy day of access management it is easy to inadvertently add exposures and vulnerabilities. With the many different systems and applications for which access management is required, it is easy to unknowingly create or further grow exposures and vulnerabilities.

This is possible due to two fundamental management techniques.

- User-level Permissions Management
- Group-level Permissions Management

User-level permission management is the most complex access management scheme and in most cases not recommended. User-level permissions are very difficult to maintain especially in enterprises that span many different platforms and applications. User-level permissions are highly subject to the exposures and vulnerabilities listed in *I. Unauthorized Users.*

Group-level permission management allow administrators to manage security accesses by groups of UserID's. It is an effective method and a very popular management technique. However, because of the ability to 'nest' or have groups within groups, it also provides a greater possibility of exposure.

There is a term called 'separation of duty'. This is the mutual exclusivity of accesses for particular UserID's or roles. An example could be a bank teller at a bank. It would not be appropriate for a bank teller to have accesses to approval systems whereby the teller could approve their own transactions. Improper group management schemes create significant system vulnerability, data integrity and reliability exposures.

Access Management Policy Concerns

Many organizations employ distributed security administration models. This includes using system administrators to also perform duties of a security administration for their particular systems. These models while typically valuable in addressing access request volumes, inherently introduce possible system and data vulnerability and exposures. In every organization a certain level of simple trust through compliance with the security administration management policy is expected of administrators. This means then the security administration procedures must be strictly and completely adhered too. This also means that the policy must be very clear and complete as it relates to the necessary procedures.

An important key to this is the approval and authorization process. Administrators with the ability to add/modify/delete UserID's and associated access privileges are very important to the integrity of the company's data. If policy does not clearly identify the procedures for access request, approval and the administrator's necessary compliance to these procedures, unpredictable and unmanageable access management is certain. Who is to stop a system administrator from adding a particular user and granting them

particular permissions? In many organizations methods to detect and prevent this from occurring other than time-delayed reporting do not exist.

Inadequate auditing processes and tools are a serious vulnerability. The need to audit particular security administration activities and report/alert on any exceptions to policy in as near real-time as possible is critical. Scheduled audit procedures and processes should be included in the policy. In a distributed administration model environment this is even more important since remote sites are not as easily monitored from a physical/personal perspective. Knowing who did what, when and how is vital in preventing information and capital loss or exploitation and in the possible recovery.

Security administration products, tools and utilities should be protected both by electronic security access control and by policy. Leaving administration tools unprotected presents the exposure and vulnerability to effectively unlock and open systems and data to persons and programs without a necessary need. This is often an overlooked administration responsibility.

Role Based Access Control

Role-Based Access Control (RBAC) is the management of accesses by the roles within the organization. This is in contrast to managing accesses based on the actual person. Research shows RBAC has strong security management benefits in addition to many financial benefits. Managing roles allows for easier access management while providing the ability to audit a particular position's accesses. Consider a rapidly growing organization. RBAC becomes extremely powerful in the management of accesses in these cases. However, it is important that to consider an RBAC model which incorporates separation of duty rules. Otherwise, it is possible that the same exposures can exist as those described in group permission management above.

IV. Security System Training

Training security administration personnel is extremely important. Security administrators should be very clear on what standards exist and any and all group and role management schemes. Security administration training should be an ongoing process. Administrators that are not familiar with the environment, management techniques, standards, and tools are subject creating or fostering access vulnerabilities and exposures.

Security Administration Automation

In enterprises of all sizes that experience high volumes of security administration transactions, exists a potential for creating or maintaining all of the above exposures and vulnerabilities. This is due to human intervention. Security administration is a manually intensive task. Well, historically it has been. However, with many of the products, utilities and simple scripting languages that exist today, much of the routine and time consuming tasks can be automated. Security administration automation provides accurate and timely access management results. The automation goes beyond just adding/deleting/modifying accesses across many systems and applications. It also

includes the monitoring or management of security administration activities that are occurring. For example, in some instances real-time notification is necessary if a user with certain accesses is added to particular system. Also automated report generation is very helpful.
Automation is a tremendous benefit and is necessary in most environments. However as with all activities occurring in an environment it too is subject to creating or maintaining exposures and vulnerabilities. All scripts and automation tools should be protected and reviewed on a periodic basis. It is possible that automation that is not protected or not properly managed can be inadvertently producing undesired results.

Summary
Integrity of systems and data within an organization that security administration from a systems and application should adhere to strict and manageable policy and processes. Failure to do so can leave information in a state for which it can be compromised.

References

Dacey, Robert. "Computer Security: Critical Federal Operations and Assets Remain at Risk"
URL: http://www.gao.gov/new.items/ai00314t.pdf (September 11, 2000)

Ferraiolo, David and Kuhn, Richard. "Role-Based Access Controls"
URL: http://hissa.ncsl.nist.gov/rbac/paper/rbac1.html (1992)

Vangelova, Luba. "Authentication and Access Control – Software and smart cards keep out the wrong users".

URL: http://www.govexec.com/tech/articles/0597csg2.htm (May 1997)

National Institute of Standards and Technology. "Authorization Management and Advanced Access Control Models". Multiple access control reports.
URL: http://csrc.nist.gov/rbac/