

AnalytX

New York

London

San Francisco

Vero Beach

1370 Avenue of the Americas

34th Floor

New York

NY 10019

Ph 212.731.2377

Fx 800.816.0763

www.analytx.com

PRIVATE EQUITY OFFICE (PEO) SECURITY WHITEPAPER FOR IT PROFESSIONALS

Donald Winger and Zeljko Tesic

PRIVATE EQUITY OFFICE (PEO) SECURITY WHITEPAPER FOR IT PROFESSIONALS

Donald Winger and Zeljko Tesic

Table of contents

Private Equity Office (PEO) Security Whitepaper For It Professionals

Introduction

Security Paradigms

Authentication

Authorization

PEO Security Logical Model

User Groups & Entity Groups

How Security is Applied – Entity, Objects and Groups

Objects and Access Rights Permissions

User Roles

An Authorization Session from the System Level

Authentication Auditing

Authorization Auditing

Creating new Legal Entities or Objects

The Recycle Bin as a Safety Net

Private Equity Office (PEO) Security Whitepaper For It Professionals

Introduction

The purpose of this document is to elaborate on security paradigms utilized in the Private Equity Office (PEO) from the perspective of the IT professional. The Private Equity Office (PEO) security is predicated upon three primary paradigms: (1) Authentication, (2) Authorization and (3) Audit. These concepts are very well defined in computer science literature. This whitepaper will spend some time exploring these paradigms, before proceeding into physical architecture discussions. We will then discuss how these paradigms are applied in the physical software incarnation of PEO.

Security Paradigms

Authentication

Authentication is the process of verifying someone's identity. To keep it simple, almost all authentication mechanisms are based on user name and password information. Typically, a user is setup on a computer network with a user name and an encrypted password. An application such as PEO needs to authenticate a user against a trusted source. That trusted source could be a variety of systems (NT domain, LDAP, MS Passport, etc). Note that PEO never has access to the actual password; it can only authenticate the password. Once verified against a secure network, the game moves to Authorization.

Does a User Exist?

Philosophers for centuries have contemplated how to prove the existence of self. Descartes who during the Bavarian Oven Experience declared "Cogito Ergo Sum" or "I think, therefore I am". Alternatively, when David Hume challenged that one could not refute the argument that proof of existence was impossible, an associate replied "I refute it thus!" while kicking a table, breaking his leg, and possibly winning the argument! Fortunately, PEO does not need to resort to any of these measures to prove the existence of a user! - DLW

With identify theft prevalent today - the issue of identify has reached a new crescendo in focus and discussion. The ways to authenticate a user range from finger printing to retina scans. However, from the perspective of a system such as PEO, we simply leave that issue to the authenticating system. PEO authenticates against a target operating system using generic API calls that are built into the .net-programming platform.

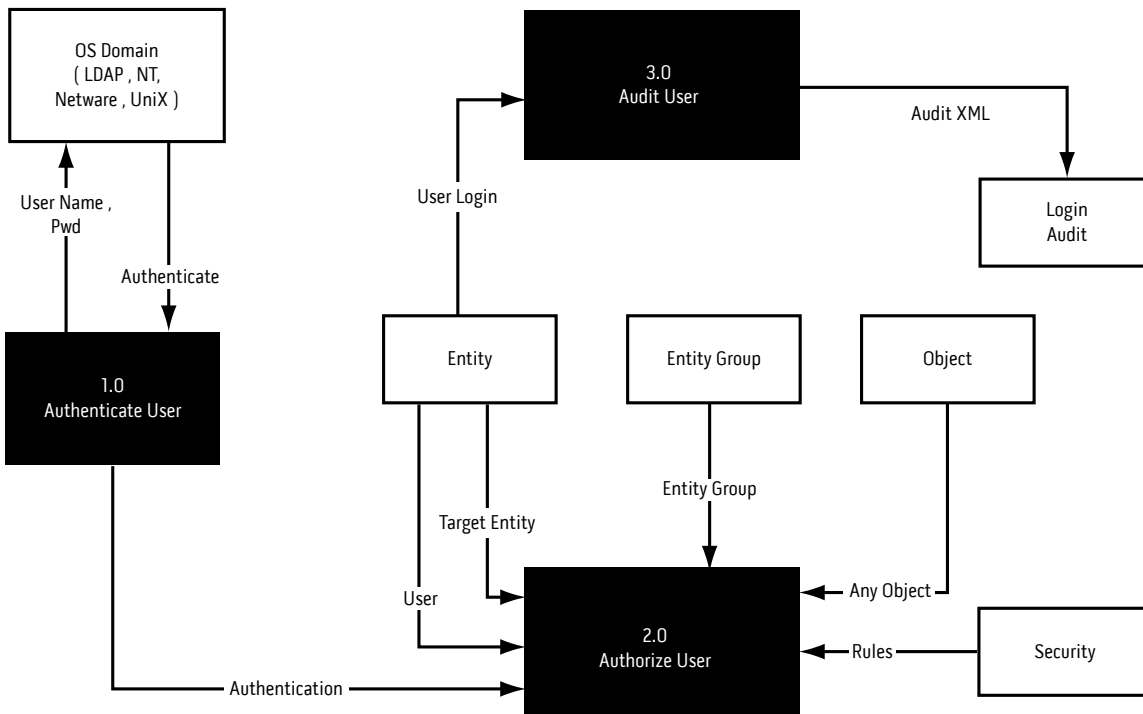
Authorization

Since PEO delegates the essential process of authentication to the Operating System level, the main topic of this whitepaper is Authorization. Authorization is a process of evaluating someone's rights on a requested object in the system. According to IETF (IRTF), AAA working group, (see [1]) the generic authorization process can be viewed as a two step process:

1. Submit well-formatted authorization request.
2. Rule based engine makes decision of your rights on the requested object.

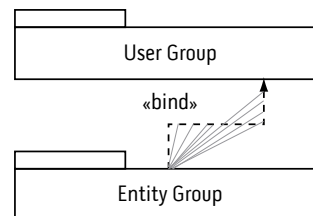
To enforce a successful authorization scheme, a robust security paradigm must separate the authorization rule engine from application specific data. This facilitates two very important objectives: (1) The ease of extension of yet to be created objects and (2) authorization against different object types. Encapsulation is enforced because the authorization engine knows the logic rules and basic information in the request, but the security object cannot access application specific information. This level of encapsulation is an object oriented programming trademark characteristic of PEO.

PEO Security Logical Model



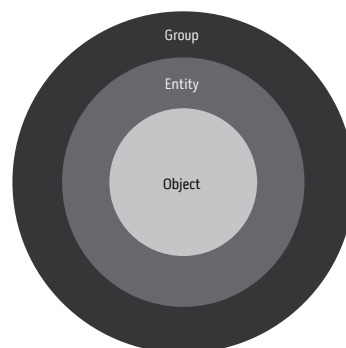
User Groups & Entity Groups

The fact is that administration of individual user right access can become unwieldy rather quickly. The concept of user groups and entity access groups tremendously simplify the assignment of security rights. User and group identification paradigms are, in fact, the input parameters to authorization service. All access rights are checked against individual objects for both user and group id.



How Security is Applied – Entity, Objects and Groups

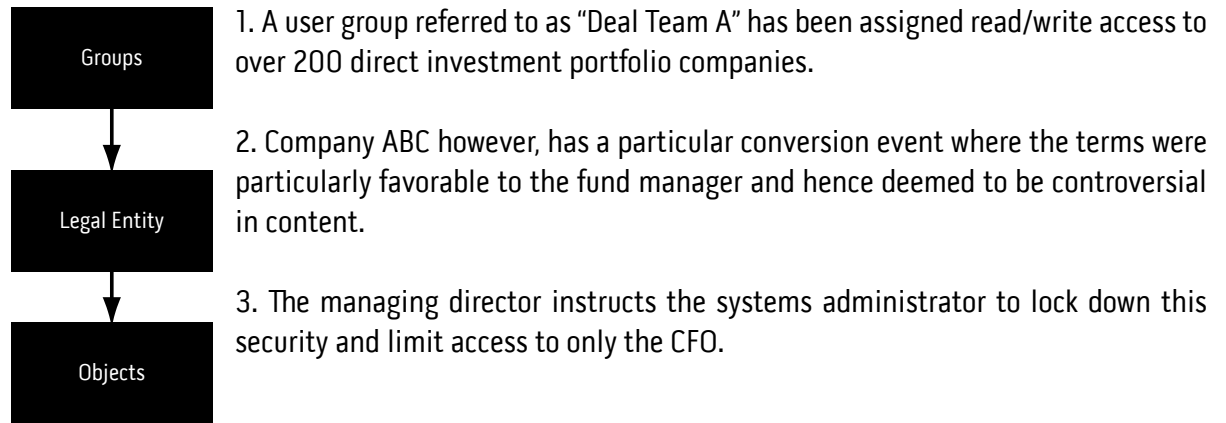
A group of entities is analogous to a top-level file directory in an operating system. When security rights are assigned at the top folder level, it naturally applies to the sub-folders. Below the entity folder, there is the equivalent of files in a directory structure. These are objects in PEO - securities, transactions, capitalization structures and other objects in PEO. PEO allows the application of security to any of these levels with default behavior granted from that level down.



OS Analogy
 Group = Top Folder
 Entity = middle folder
 Object = file

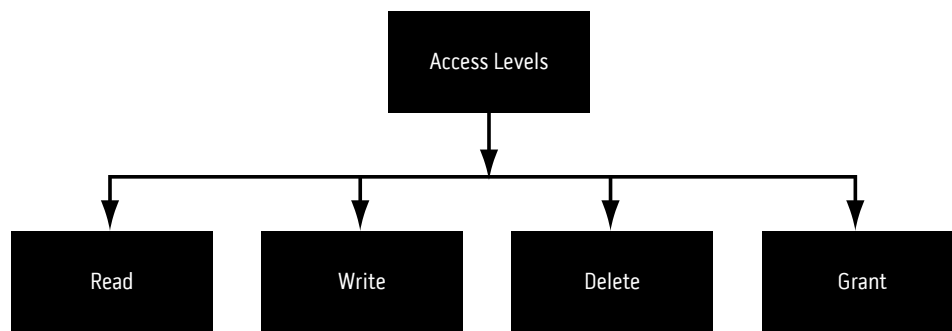
If a user or group is granted access to an entity, the user has access

to the underlying objects by default. However this can be overridden at the object level. For instance, let's postulate the following scenario:



By default then, a member of Deal Team A (Group), that is not the CFO, has read/write access to ABC Portfolio Company (entity) but cannot access the Security referred to as "Preferred Shares A"

Objects and Access Rights Permissions

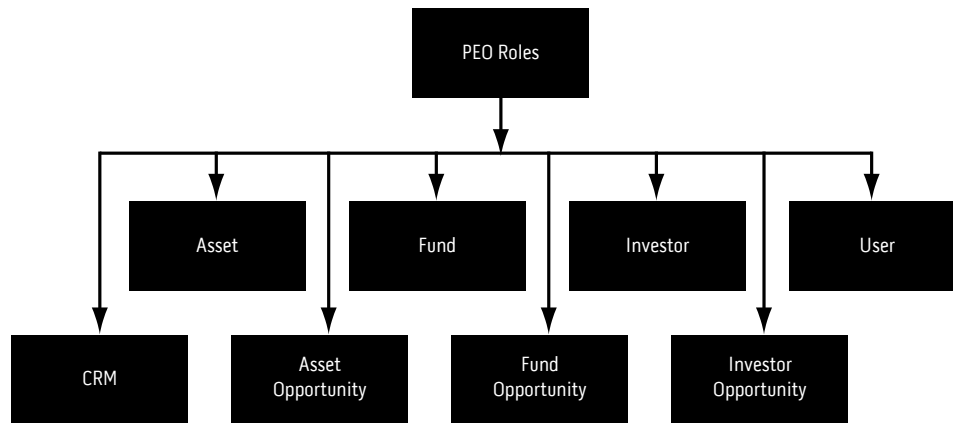


The rights on the group, entity or object fall into the following categories: Again, the rights assigned from the top level, apply to lower levels in the hierarchy unless explicitly over-ridden. Consistent with the folder, object metaphor, a user can be assigned rights to access an entity, and therefore, is granted rights to the objects contained in the entity. Sometimes however, an administrator might want to apply one more level of security at the role level. That topic is covered in the last section of the whitepaper.

User Roles

In PEO there is the concept of dimensional views or roles. Using this paradigm, specific groups of users can be granted security rights based upon the most general behavior with specific entity or object right specialization or over-rides. For instance, say that an administrative assistant named "Bob" requires access to the contact information for 200 legal entities captured in PEO. However, there is no requirement that Bob have access to the asset or fund financial dimensions. Hence, Bob can be assigned security privileges based upon his role, and by default, will be limited to the dimensional profile of CRM for every entity in PEO.

Another example: Say an investment professional "Jill" requires access to deals, but the accounting team prefers not to have the deal professionals enabled with access to asset management. Jill's group could be granted default access to all asset entities, but with access limited to the opportunity dimensional view only.



An Authorization Session from the System Level

In PEO, every user in system is identified by their unique user name. In addition, a user can be a member of one or more groups. Each level of group access is dependent upon the system setup, with the exception of built in groups such as public and administrator. During login, the user logs in as a member of a group. PEO also allows a user to change its group identification at runtime without having to log in (authenticate) again. Below is the PEO algorithm for determining access rights for a particular user, as defined in the following piece of pseudo code:

```

{
  User logs IN with its desired user and group
  credentials.
  Output: two session tracking variables are related to
  its current user and group credentials.
}
{
  User is accessing particular object(s).
  Application code is checking its user and current
  group credentials {
  If(user rights are defined) {
  Use them;
  Return;
  } else if(group rights are defined)
  Use them;
  Return;
  } else
  Use public group rights;
  Return;
  }
}

```

From this algorithm we see that individual user rights, if defined, will over-ride the group rights assigned to a user. Using the folder analogy from an OS once again, it is possible to establish security rights for a top-level file folder, and to specialize the security behavior for an object in that folder. Naturally, the object assignment supersedes the group assignment.

Authentication Auditing

Security auditing falls into two main categories within PEO. First, there is a need for authentication audits when a user attempts to login multiple times, without success. Secondly, there is a need to audit the user activity once authenticated and authorized, in order to monitor user actions while logged into the system.

If the user fails in an attempt to access the system, essential information must be captured regarding this attempt. Further, this attempt should not continue indefinitely. A lockout should occur after n number of attempts – n being defined at the systems configuration level.

For instance, say that an asset manager named “Sam” attempts to login into PEO over 5 times. Perhaps he was out the night before, or perhaps the Espresso machine is broken in the office. Regardless, after 5 attempts, PEO shuts down Sam’s login attempts for 24 hours. However, a user with administrator rights can instantly purge this lockout.

Authorization Auditing

Another topic on auditing is how to track changes made by users once they are authorized and using PEO. These changes are most important as they relate to transactions. When a transaction related record is added, modified, or deleted, a log is created containing the original and target contents, and a clear record of modified transactions is maintained by PEO. This log will accumulate until the administrator purges it.

For instance, suppose that an accountant, referred to as “Wilopedia Potter III” by her close associates, suggests that the IRRs are not calculating correctly. Within PEO, IRRs are built from a vector of cash flows and application of a formula utilizing a stochastic derivative. Despite its status of being, at its essence a series of zeros and ones, it finds itself at odds with a human being – Willopedia in this case. Fortunately, PEO is able to process a user audit report – revealing that Wilopedia captured the wrong valuations for several assets and hence, the terminal values for the IRR event horizon were incorrect. Once corrected, the IRRs tie out perfectly.

Creating new Legal Entities or Objects

Assignment of security rights for new objects are based upon two critical concepts:

- Ownership
- Default group security assignments

The user that creates an object is the object owner. By default, a user created object will have complete access to that object.. Likewise – the login group to which the user belongs will also have read/write privileges to the newly created entity. However – PEO also makes it possible to assign rights for new object creation, by user group. That is – the user group’s implicit rights when creating a new entity in PEO. Thus, even though a user creates a new fund, the user may not have access to all information for that fund. Examples:

- When a new entity is created – the user is the object owner and gains full access to that object by default. For instance, User A creates ABC Portfolio Company and has access to it.
- When a new entity is created, the user’s group also gains full access to that object by default. In the example above, all members of the user’s login group would have access to ABC Portfolio Company.
- However, if the user’s group has a dimensional profile restriction assigned to it – the user is limited to that dimensional profile and the user’s group has the same restriction. If for instance, if the user in the above example was limited to the CRM view only, the user would not have access to other dimensions of the company, including the financial side, even though the user created the new company.
- The above behavior, can of course, be reassigned by a security administrator – post entity creation.

The Recycle Bin as a Safety Net

Even with the security paradigms in place as described in this paper, deletions of objects in any system can go horribly wrong. Virtually disastrous consequences reside with the ability to delete legal entities such as assets, funds, or investors. In order to protect against this

dangerous ability, (even when granted) PEO allows designated users to perform deletes – but only places the deleted records into the users recycle bin. A special privilege administrator is required to purge the user recycle bin. This is the ultimate protection against un-intentional deletes and their direct and indirect consequences.

The Private Equity Office (PEO) implements the security paradigms described in this document utilizing role types, entities and objects. Assignments are made from general, to specific, with time saving features such as security default behavior, entity level assignment, and the ability to lock down specific objects. At the end of the day, however, PEO insulates against the most dangerous type of security privilege – the ability to delete system objects – with an ingenious recycle bin concept.

Bibliography

[1] RFC 2903 Generic AAA Architecture. C. de Laat, G. Gross, L. Gommans, J. Vollbrecht, D. Spence.

August 2000. (Format: TXT=60627 bytes (Status: EXPERIMENTAL))

[2] RFC 2251 Lightweight Directory Access Protocol (v3). M. Wahl, T.

Howes, S. Kille. December 1997. (Format: TXT=114488 bytes) (Status: PROPOSED STANDARD)

[3] RFC 1510 The Kerberos Network Authentication Service (V5). J. Kohl,

C. Neuman. September 1993. (Format: TXT=275395 bytes) (Status: PROPOSED STANDARD)

New York

1370 Avenue of the Americas
34th Floor
New York, NY 10019
(P)+212-731-2377
(F)+800-816-0763

London

International House
223 Regent Street
6th Floor
London W1B 2QD
United Kingdom
(P)+0207 096 0144
(F)+0207 544 1090

San Francisco

750 Battery Street
7th Floor
San Francisco, CA 94111
(P)+415-738-4938
(F)+800-816-0763

Vero Beach

1880 82nd Avenue
Suite 206
Vero Beach, FL 32966
(P)+772-564-8066
(F)+772-564-8254