



TRIANZSM

When Execution Matters

White Paper

Authentication and Access Control - The Cornerstone of Information Security

Vinay Purohit
September 2007



Table of Contents

1	Scope and Objective -----	3
2	Why Access Controls are required-----	3
3	What are Access Control Models-----	3
4	Discretionary Access Control (DAC)-----	4
5	Mandatory Access Control (MAC)-----	4
6	Role Based Access Control (RBAC)-----	5
7	Authentication -----	6
8	Access Control Framework (ACF)-----	8
9	Access Control Techniques and Technologies-----	9
10	Summary -----	10
11	References -----	10

1 Scope and Objective

What is an access control? We can say it's a way to manage access to enterprise resources. If we go with the word definition, access control is a mechanism to control the flow of information between subject and object where subject is always an active entity while object is a passive entity. In its broadest meaning, access control is a three-step process that includes identification, authentication and authorization. In this white paper, the term authentication is generally used to represent both identification and authentication, and access control is used for authorization.

The paper discusses the importance of selecting an access control model that fits with your security needs to provide a lower total cost of ownership and enable strong identification. It also discusses the various authentication solutions and weighs their need to your organization.

2 Why Access Controls are required

As the business of an enterprise increases, so does the demand for access control since it is the first line of defense to protect the organization's resources. When you try to access a certain resource and you are asked to provide your identification - that is access control. Access control solutions provide protection, integrity, availability and auditing capability to the organization.

3 What are Access Control Models

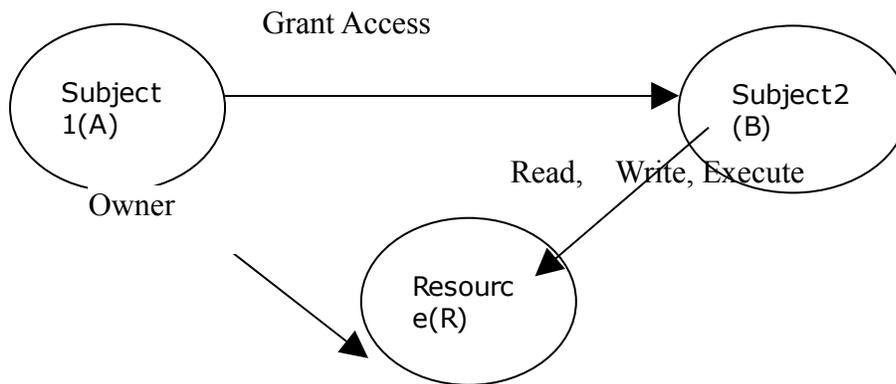
Access control model is a framework that dictates access control using various access- control technologies. There are standard access control models which are highly domain and implementation independent. Each access control model has its own merits and demerits, and the specific business objectives they serve depend on the organization's need, culture, nature of business, etc. We will discuss these models and examine their fitness with respect to an organization's security policy and business goals.

- Discretionary Access Control (DAC).
- Mandatory Access Control (MAC).
- Role Based Access Control (RBAC).

4 Discretionary Access Control (DAC)

Discretionary Access Control is based on ownership and delegation. In a DAC Model, access is governed by the access rights granted to the user or user groups. An organization/administrator/creator can identify a set of operations and assign them to an object and to a set of users (belonging to a user group).

The DAC model is flexible but complex. It creates a paradox in some complex situations. For example, A is owner of resource R of organization O and he has delegated permission P1 and P2 to B who, in turn, have delegated permission P1 to C. Now, if A chooses to revoke permission to B what will happen to the permission that B granted to C?

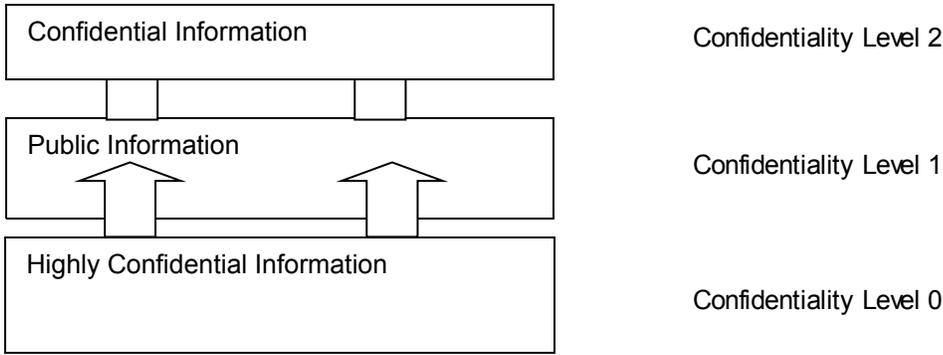


While the model above is complex, it is still flexible enough to handle various access control needs, and therefore is used in various network management applications.

5 Mandatory Access Control (MAC)

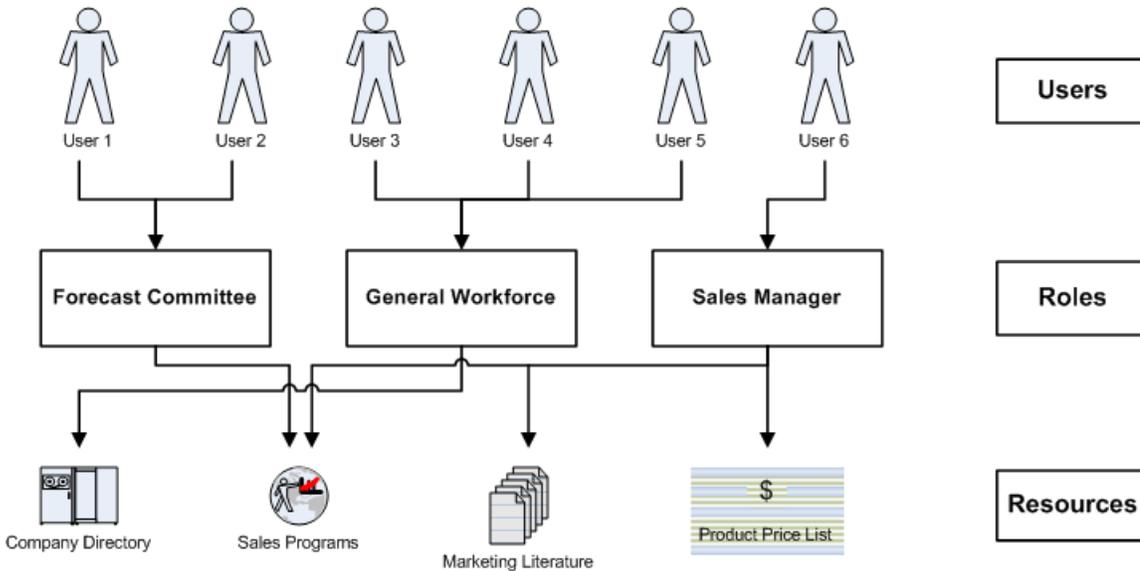
In MAC, the data owner has limited freedom to decide on access control. Information is classified into different categories and each category is assigned a particular security level. For example, resource R is a very confidential resource to the organization and so has been assigned a "Very Confidential" security level. When a user, who has been assigned security level "Confidential", tries to access this resource (R), he is denied access because the security level assigned to him doesn't match.

This model is appropriate when securing confidentiality of data is critical, as in -- for example -- military operation systems.



6 Role Based Access Control (RBAC)

RBAC is a widely used - and dominant - access control model, and most access control security products available in the market today are based on this model because its objectives are architectural. Entrust Get Access is one such product. The model allows access to a resource, based on the role the user holds in the organization. It is based on the concept of “separation of duties”. The privileges to the particular role are decided and thereafter mapped to the user. The diagram below depicts the concept in more detail.



If the environment does not require a high level of security, the choices are usually discretionary and role based. The discretionary model gives data owners the ability to allow other users to access resources, enabling choices to be made with full knowledge of what it entails. If the organization has a high turnover rate, the role based model is more appropriate. If the environment requires higher level of security and it is desired that only administrator should grant the access control, then MAC is the best choice.

7 Authentication

Authentication or identification is the first step in any access control solution. It is the process of identifying the user to verify whether he/she is what he/she claims to be. Normally, identification is done with the help of information that is known to everyone (i.e., user name or user ID) and some personal information known only to the subject (i.e. password). Faced with the threat of identity theft and increasing consequences associated with failing to secure information, enterprises are increasingly looking for stronger forms of authentication to enhance their overall security capabilities. At the same time, enterprises and governments need to take into account other important considerations such as usability, total cost of deployment and maintenance, and integration with existing security solution offerings. Usernames and passwords are the most common authentication techniques. But most organizations do not depend on user name authentication alone since username and passwords are an authentication solution for low-value transactions and for accessing non-sensitive information over the network. Also, experience has shown that usernames and passwords provide relatively weak authentication because they can often be guessed or stolen. They are often difficult to deploy because each application may implement its own scheme, adding to both development cost and user complexity. Also, it is very difficult to maintain and reset the password. Determining the appropriate level of authentication that meets your budget requirements is essential when implementing your secure identity management solution. It is very crucial to identify the appropriate authentication technique depending upon the nature of the business and sensitivity of the information. One has to consider various authentication methods and their pros and cons. The means of authentication are often discussed in terms of “factors” of proof, such as:

- Something you know to prove your identity (e.g., a PIN)
- Something you have to prove your identity (e.g., a smart card)
- Something you are to prove your identity (e.g., a fingerprint)

A good authentication technique contains at least two of the above methods. In a client server environment, strong authentication is a combination of server and client authentication:

- Server authentication is when the server proves its identity to the client.
- Client authentication is when clients prove their identity to the server.

There are various authentication techniques that organizations can choose from. A quick discussion on some of these techniques follows:

1. User Password Authentication

It is the most common form of providing identification. When user accesses the resource, access control framework asks for the user name password provided to the user. The credentials are validated against the one stored in the system's repository.

2. Windows user based authentication

Usually, organizations have a list of users stored in the windows active directory. Access control framework should be able to provide authentication for the user of the Primary Domain Controller (PDC).

3. Directory based authentication.

With the rising volume of business over the web, millions of users often try to access the resource simultaneously. In such a scenario, the authentication framework should be able to provide for faster authentication. One such technique is Directory Based Authentication where user credentials are validated against the one which is stored in the LDAP Directory.

4. Certificate based authentication

This is probably one of the strongest authentication techniques where the user is asked to provide his/her digital ID. This digital ID, known as digital certificate, is validated against the trusted authority that issued the digital ID. There are various other parameters that are checked to ensure the identification of the user.

5. Smart card based authentication

This is also used as a second factor authentication. Smart cards are small devices containing co-processors to process cryptographic data.

6. Biometrics

This is the strongest authentication. Known as third factor authentication, it is based on something the user is. It works after the users have provided something they know (User name password) and something they own (either a grid or token) or something they are (retina-scan, thumbprint or thermal scan). It is required in cases where data is top confidential, such as in Military/Defense.

7. Grid based Authentication

This is used as a second factor authentication. It authenticates the user based on something he knows (User name password authentication) and then asks for something he owns (grid card information). Entrust Identity Guard provides such an authentication.

8. Knowledge-based authentication

One of the simplest mechanisms for gaining additional confidence in a user's identity is to challenge the user to provide information that an attacker is unlikely to be able to provide. Based on "shared secrets", this allows for the organization to question the user, when appropriate, to confirm information that is already known about the user through a registration process, or from previous transactions.

9. Machine Authentication

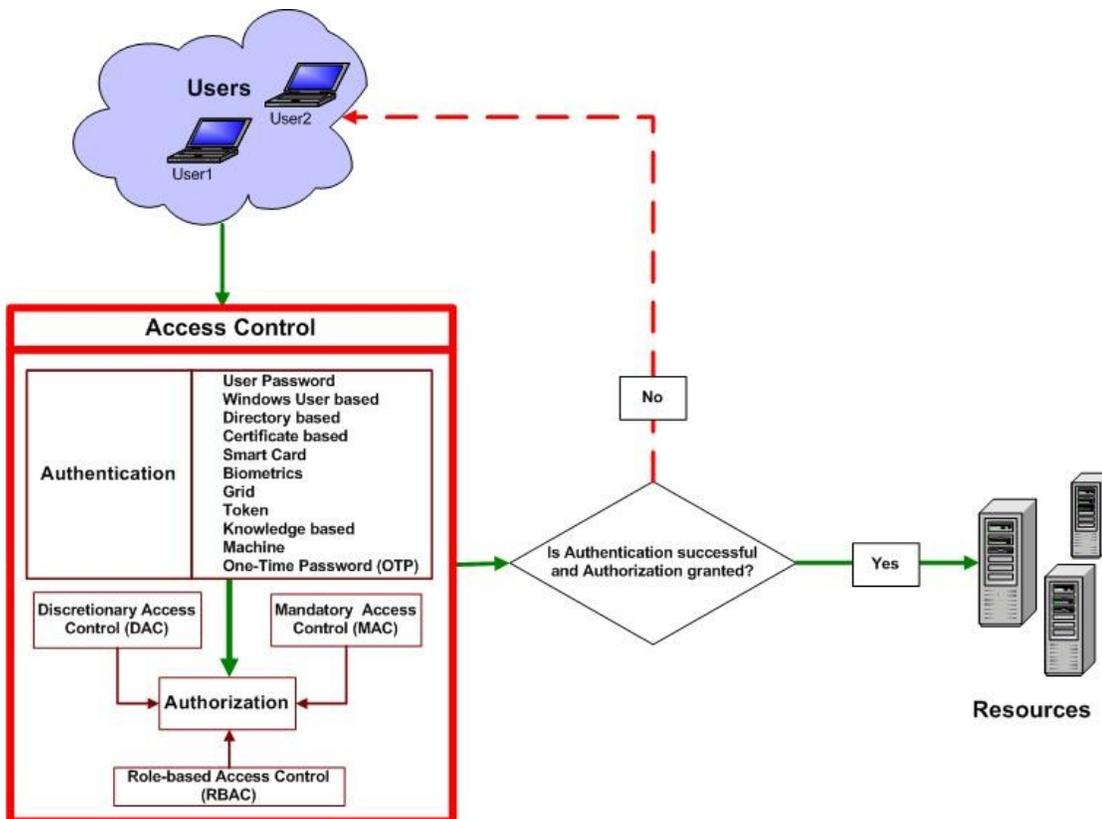
Machine authentication provides validation of the user's computer in a way that secures against a variety of threats in a zero touch fashion, reducing user impact. This is an especially effective method of user authentication where users typically access their accounts from a regular set of machines, allowing for stronger authentication to be performed without any significant impact on the user experience.

10. One Time Password (OTP)

A one time [assword is dynamically generated and it is valid only for once. The advantage of one time password is that if an intruder hacks it, he cannot reuse it. There are two types of OTP token generators: synchronous and asynchronous. A synchronous token device synchronizes with the authentication service by using time or an event as the core piece of the authentication process. A token device, which is using an asynchronous token generating method, uses a challenge response scheme to authenticate the user.

8 Access Control Framework (ACF)

The access control framework (ACF), presented in this paper, is like an umbrella that covers both authentication and authorization. Whenever the user accesses any enterprise resource, ACF can come up with one or more authentication techniques depending on the need of the enterprise. Once the authentication is done, ACF can authorize the request, following any model, depending on the need of the organization.



9 Access Control Techniques and Technologies

Once an organization decides on the type of access control model to be employed, the next step would be to decide on the techniques and technology to be used. Here are some techniques and technologies:

Rule Based Access Control:

Rule based access control is based on rules defined on the object, as defined by the administrator who decides on the operations that can be performed by subject. A rule can be as simple as defining the day of the week on which the resource can be accessible.

Menu Based Access Control:

In a menu based access control, the user interface given to the user controls the operations that can be performed on the object, i.e., If A and B operations can be performed on object O, then the user interface pertaining to A and B options is enabled and the rest of the user interface is disabled.

Access Control List:

Access control list is the list of subjects that are authorized to access a particular object. It also defines the level of authorization.

Content Based Access Control:

In content based access control (CBAC), the access to the object is determined by the content within the object. For example, a manager can access the payroll database but only for employees reporting to him.

Access Control Markup Language (XACML)

XACML is the access control markup language that is used to express the rules that are necessary for authentication and authorization. The vocabulary to express these rules is given by the access control markup language. These rules are used to make decisions regarding the authorization. eXtensible Access Control Markup Language -- or XACML -- provides a mechanism to create policies and rules for controlling access to information.

A typical access control and authorization scenario includes three main entities -- a subject, a resource, and an action -- and their attributes. A subject makes a request for permission to perform an action on a resource. For example, in the access request, "Allow the Sys-admin to create files in the root folder of the production server" the subject is the "Sys-admin", the target resource is the "root folder of the production server", and the action is "create files".

Security Assertion Markup Language (SAML)

SAML is an [XML](#) standard for exchanging [authentication](#) and [authorization](#) data between [security domains](#), that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the [OASIS Security Services Technical Committee](#).

The single most important problem that SAML is trying to solve is the Web Browser single sign-on (SSO) problem. [Single sign-on](#) solutions are abundant at the [intranet](#) level (using [cookies](#), for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. SAML has become the definitive standard underlying many web single sign-on solutions in the enterprise [identity management](#) problem space.

10 Summary

The whole thrust of access control is to restrict unauthorized users from accessing organization resources. The authentication techniques and access controls described in this white paper can be chosen based on an organization's need. The authentication and access control framework should be flexible enough to serve all the authentication techniques and future evolution in the area such as Biometrics. The access control framework should be able to handle an organization's authentication and authorization (access control) needs. Entrust GetAccess and Identity Guard are the products with such features.

11 References

Designing Security Architecture Solutions – Jay Ramachandran.

Security Architecture – Christopher M. King

CISSP Certification - Shon Harris.

About the Author

Vinay Purohit, a Technical Lead at Trianz, has more than six years of experience in implementing various applications in security domain. His expertise is in Access Control, PKI and Web Security. He has successfully led implementation of several security products at companies such as Siemens, Huawei Technologies, Wipro, and Entrust. Since joining Trianz, Vinay has done several implementations where he designed various security features in Entrust products as per security best practices. He can be contacted at vinay.purohit@trianz.com

About Trianz

Trianz is a management consulting, technology, engineering, and outsourcing services firm that helps senior leaders execute business and technology initiatives. A unique mix of business consulting and technology capabilities has helped Trianz rapidly grow since its inception in 2000. Trianz provides services to a diversified global client base. Clients are result-focused leaders employed in businesses ranging from Fortune 1000 corporations to emerging rapid-growth companies. Service offerings focus on the following areas:

Operations Consulting Services

Enterprise Applications Services

Software Product Engineering Services

Transformational Outsourcing Services

Disclaimer for white papers

©2006 Trianz. All rights reserved

Copyright in whole and in part of this document belongs to Trianz, Inc. This work has been provided for informational purposes only, and may be copied for personal use only. This work may not be used, sold, transferred, adapted, abridged, copied, or reproduced in whole or in part, in any media, by enterprises, without the prior written permission of Trianz, AND an acknowledgement of "Trianz" as the source of the content. All trademarks and copyrights mentioned in this white paper are the property of their respective owners. Neither the author nor Trianz bears any responsibility for damage resulting from the use of the information contained herein.

For more information about Trianz and its capabilities, visit 'www.trianz.com'