Authentication and Authorization Models

Prof. More V.N. vickymore12@gmail.com
Faculty, Bharati Vidyapeeth University, Pune (India)
Abhijit Kadam Institute of Management & Social Sciences, Solapur

ABSTRACT

In computer science distributed systems could be more secured with a distributed trust model based on either PKI or Kerberos. However, it becomes difficult to establish trust relationship across heterogeneous domains due to different actual trust mechanism and security policy as well as the intrinsic flaw of each trust model. Since Internet has been used commonly in information systems technologies, many applications need some security capabilities to protect against threats to the communication of information. Two critical procedures of these capabilities are authentication and authorization. This report presents a strong authentication and authorization model using three standard frameworks. They are PKI, PMI, and Directory. The trust in this approach is enabled by the use of public key infrastructure (PKI) which is applied for client two-factor authentication and secures the infrastructure. We introduce the preventive activity-based authorization policy for dynamic user privilege controls. It helps prevent successive unauthorized requests in a formal manner. At the core, we apply An Improved Trust Model to facilitate the authentication with the different keys with work flow of model efficiently. Also describes the X.509 standard to define the directory schemas of PKI and PMI to find the object classes and optional attributes.

Keywords: PKI, PMI, Kerberos, An Improved Trust Model, X.509 standard.

1. INTRODUCTION

PKI and Kerberos are two protocols, into which most of the researches in the field of a distributed system are made, and they have got the most widely application. In a PKI protocol, the information security of that system is assured through the adoption of public key technology and digital certificate. The purpose of the digital certificate is to verify the identity of the certificate holder.

Kerberos, based on symmetrical key algorithm, enables the establishment of mutual trust between the two communication sides through session key and ticket authorization. Both protocols, to a certain degree, have been put into application with relatively good results. Net technology are continuously advancing, especially a huge number of large-scale distributed information systems are setting up, which may adopt different authentication technology and its corresponding trust model, as a result, though its own system security is safeguarded, numerous authentication barriers and “information isolate islands” in a network will be also created.

PKI provides a framework to verify the identities of each entities of given domain. The framework includes the requesting, issuing, signing, and validating of the public-key certificates.

PMI provides a framework to determine whether or not they are authorized to access a specific resource. The framework includes the issuance and validation of attribute certificates. Public -key certificates are certificates for trusting public-key and attribute certificates are certificates for trusting privilege attribute.

Directory plays a significant role as an interconnection standard for PKI and PMI. This report describes the form of authentication and authorization information held by the Directory, and how such information may be obtained from Directory.

2. PKI (PUBLIC KEY INFRASTRUCTURE)

A public-key certificate has a special data structure and digitally signed by an authority called certificate Authority (CA). A public-key certificate binds a public key to a subject which holds the corresponding Private-key so that other entities could trust subject’s public-key. Public-key certificate can be used during some period of time specified in a certificate’s ‘validity’ filed. But, for some reasons, the certificate can be revoked by the CA before

the certificate expires. If an authority revokes a public -key certificate, users need to be able to know that revocation has occurred so they no longer use the revoked certificate.
A system using a public-key certificate needs to validate a certificate prior to using that certificate for an application. Since certificates are public information, certificates can be published and placed in public places Directory), with out special efforts to protect them.

2.1 Generation of Key Pairs

A user's key pair can be generated in three different ways according to the standards.

a) By the user
b) By a third party
c) By the CA

The advantage of method ‘a’ is that a user’s private key is never released to another entity. But, the user needs a communication with the CA so that he can transfer the public key and distinguished name in a secure manner. In case of ‘b’ and ‘c’, the user’s private key also needs to be transferred to the user in a secure manner.

2.2 Creation of Public-Key Certificate

A CA issues a public-key certificate by associating the user’s public key and unique distinguished name of the user. It is important that CA should be satisfied of the identity of a user before creating a certificate, and should not issue certificates for two users with the same name. A public-key certificate contains following information and is digitally signed by issuer to provide the integrity.

- Version: the version number of certificate.
- Serial number: an integer uniquely assigned by the CA to each certificate.
- **Signature**: algorithm identifier for the algorithm and hash function used by the CA in signing the certificate.
- **Issuer:** the entity that has signed and issued the certificate.
- **Validity**: the time interval during which the CA warrants that it will maintain information about the status of the certificate.
- **Subject**: the entity associated with public-key found in the subject public key field.
- **Subject public key info**: the public key being certified and the algorithm which this public key is an instance of.
- **Issuer unique identifier**: used to uniquely identify an issuer in case of name re-use.
- **Subject unique identifier**: used to uniquely identify a subject in case of name re-use.
- **Extensions**: allows addition of new fields to the structure.

2.3 Certificate Validation

Certificates may be revoked by CA prior to their expiration time. Authorities are required to state the way for relying parties to obtain revocation information about certificates issued by that authority. The Certification Revocation List (CRL) is a commonly used mechanism for relying parties to obtain this information. The CRL is a periodically published data structure that contains a list of revoked certificate serial numbers. The CRL is time-stamped and digitally signed by the issuer of the certificates.

Generally a CRL is published within an X.500 directory which also stores the certificates for the particular CA domain. Delta-CRL is a partial CRL which is a list of only newly revoked certificates. Delta-CRL is useful when entire revocation list become large and unwieldy. An Authority Revocation List (ARL) is a CRL that is used exclusively to publish revocation information for CAs. It therefore does not contain any revocation information pertaining to end -user certificates.

2.4 Certification Path

According to the PKI standards, there are two primary types of public -key certificates, user certificates and CA-certificates. A user certificate is a certificate issued by a CA to a subject that is not an issuer of other public-key certificates. A CA-certificate is a certificate issued by a CA to a subject that is also a CA. If a Certification Authority is the subject of a certificate issued by another Certification Authority, the certificate is called a cross-certificate. A list of cross-certificates needed to allow a particular user to obtain the public key of another, is known as a certification path.

A certification path logically forms an unbroken chain of trusted points between two users wishing to authenticate.

3. PKI AND ITS TRUST MODELS

PKI (Public Key Infrastructure) is the most widely used security authentication technology, mainly including encryption, digital signature and digital certificate. In a PKI system, CA (Certificate Authority) is the authentication centre of a domain and represents a third institution of credible authority. All communication and authentication between the clients rely on the certificates issued by CA. The trust models of PKI include the strict hierarchy trust model, reticulated trust model and the composite trust model.

3.1 Strict Hierarchy Trust Model

Strict hierarchy trust model is a centralized mode. This model has a tree-shaped structure with the root as the root CA. The branch nodes are the sub-CAs and the leaves represent the clients. All the nodes (sub-CAs and clients) trust root CA and reserve a copy of root CA's certificate with its public key. Before user A communicates with B, they must verify each other's certification through the root CA. Only their certificates have both been verified by root CA, shall the communication between the users established. All the one-way trust relationship must be established through the central authentication server (root CA). Therefore, the structure of this model can be easily extended by adding a sub-CA or more. In this model, the verification path of the certification is correspondingly short. The longest one will be Nlevel + 1; the Nlevel stands for the number of the layers.

Root CA is the unique trust-point. If the root CA is rendered into unreliable, the trust relationship of the whole PKI system will be destroyed right away. It is almost impossible to recover the whole trust relationship. In practical network environment, it is hard to establish an exactly dependable trust-point. It is not even an easy thing to integrate established CAs due to different security policies. Any adjust to the trust relationship would be extremely difficult once a system is established.

3.2 Reticulate Trust Model

The Reticulate trust model includes several CAs to provide PKI service. Each terminal trusts a Certain CA which issues him the certificate. The CAs trusts each other by issuing certificates to each other peer-to-peer. Each user trusts others by means of this kind of certificate. CAs issues the cross authentication certificate with each other, which contains the public key of the issuing CA. In this way, trust relationship will be established and extended. This model can easily add new group of users, because of multiple reliable CAs.

Security weakness of a single CA or a number of CAs will not affect the overall operations of the whole system, because the trust can be reestablished through other paths. It is also easier to renew the trust relationship after malfunction or accidents, only a few CAs or users will be affected. It is a complex and difficult thing to construct a certificate verification path, because there may be many possibilities. The user may try many times to find the proper one. With the increase of CAs, cross trust authentication would become more complex and a heavier burden would be imposed on the management and maintenance of the system. This model is not appropriate to the organizations with strict affiliation, such as the government and the military. Hierarchic relationship of the real entities could not be reflected by this model.

3.3 Composite Trust Model

This kind of trust model is based on the cross authentication, like the reticulate trust model, but is different. There is a bridge CA which is responsible for establishing the cross-authentication for heterogeneous trust-domain. Other CAs from different domains can authenticate each other through the bridge CA. This bridge CA is a medi-point of trust transfer as well as an influx-point. Any structured PKI application or system can be connected with one another without having to modify its own structure so that the trust relationship could be established and extended through the whole system.

The Bridge CA plays a role as a third part sponsor for establishing the trust relationship between different domains. The independent and surveillant status of the Bridge CA is suitable to maintain reliability and seriousness of the model. This model has a wheel-shaped and radiating structure as well as multiple trust chains of many other trust models. The Bridge CA does not manage the end-users, so the change of the user number does not affect it. Using this model, the number of the times of certificate authenticating will be the same as the number of CAs, which could make the management less costly and much easier. When the Bridge CA is disabled, every CA connected with the bridge only needs to release the certificate signed to the Bridge CA. They can still work separately before the Bridge CA returns to work.

4. KERBEROS

Kerberos is a network authentication protocol. It was designed to provide strong authentication based on the reliable third-party authentication system for the project Athena. Now, it is available in many commercial products. Kerberos builds a safe bridge between client and server by providing central authentication service and symmetrical key system. In other words, an appointed server works for the user only when the central authentication server validates the service request and access right sued by the user. The most important part of Kerberos is the key distribution centre, which called KDC for short. It provides two services, one is AS (Authentication service), and the other is TGS (Ticket granting service). The operation flowchart of the protocol is demonstrated in Fig.1.

Kerberos protocol is now widely used in the distributed network applications. Independent development platform, high speed communication of authentication, mutual authentication between entities and transferable relation-ship of trust, and a relatively strong compatibility with heterogeneous domains which may adopt various trust polices, are all the predominance of the Kerberos. However, many security flaws appear during its usage in that the protocol heavily relied on certain aspects when it was designed and the limitation is quite striking. From the point of view of the network attack, some serious problems demanding more attention are as followed:

4.1 Password Guessing Attack

Kerberos is not effective against password guessing attacks; if a user chooses a poor password, then an attacker guessing that password can impersonate the user. Similarly, Kerberos requires a trusted path through which passwords are entered. If the user enters a password to a program that has already been modified by an attacker (e.g. a Trojan horse), or if the path between the user and the initial authentication program can be monitored, then an attacker may obtain sufficient information to impersonate the user.

4.2 The Security of the Application System

At the present time, the worst network attack comes from vicious software. Kerberos authentication protocol depends on the absolute reliability of the software based on the protocol. An attacker may design software to replace the primary Kerberos application, which can execute the Kerberos protocol and record the username and password. Generally speaking, the cipher application which has been installed on unsafe computers will more or less face the problem. Also, Kerberos must be integrated with other parts of the system. It does not protect all messages sent between two computers, and it only protects the messages from software that has been written or modified to use it. While it may be used to exchange encryption keys when establishing link encryption and network level security services, this would require changes to the network software of the hosts involved.

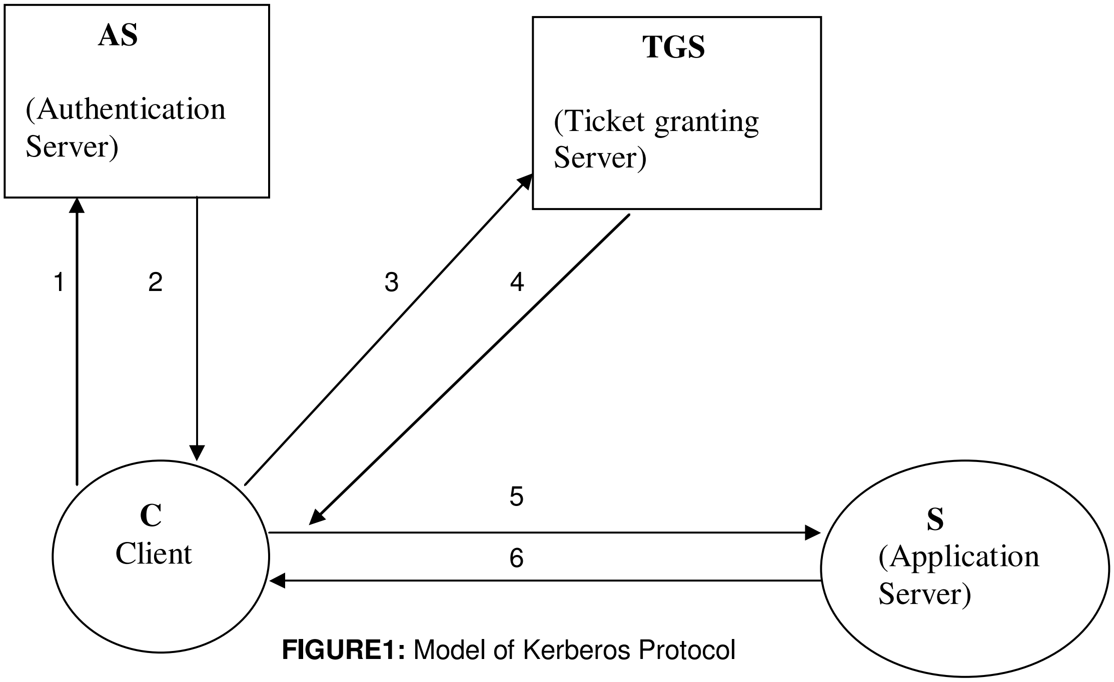


FIGURE1: Model of Kerberos Protocol

4.3 The Problem of Timestamp

Kerberos uses timestamp in order to prevent playback attack. But during the lifetime of the ticket, playback attack may still take effect. For example, in a certain Kerberos trust domain, all the clocks of the equipments keep synchronous. The period of validity for the message is 5 minutes, if the message arrives during the period, it is regarded as fresh.

In fact, the attacker can easily fabricate a message according to the protocol format beforehand. Once he intercepts and captures the ticket from the user to server, the attacker could send the fake message within 5 minutes; server can not easily find what exactly happened.

4.4 Secure Storage for Session Key

In Kerberos system, each user shares a session key with the server. KDC of the Kerberos system must provide a service to store a huge number of session keys. It is arduous to manage or update the keys and information related. Special measures must be taken to protect the KDC.

Naturally, the KDC becomes the targets of the attackers. Especially for the government or the military, it will be a disaster if the KDC has been destroyed which will result in failed communication among users of the domain. It is also quite demanding to store the system. So Kerberos, the authentication and authorization protocol based on symmetric key algorithm, is fitter with the environment which does not own a large number of registered users, but demands high efficiency.

5. AN IMPROVED TRUST MODEL

It is a model for authentication and authorization between trust domains. It is based on PKI and Kerberos.

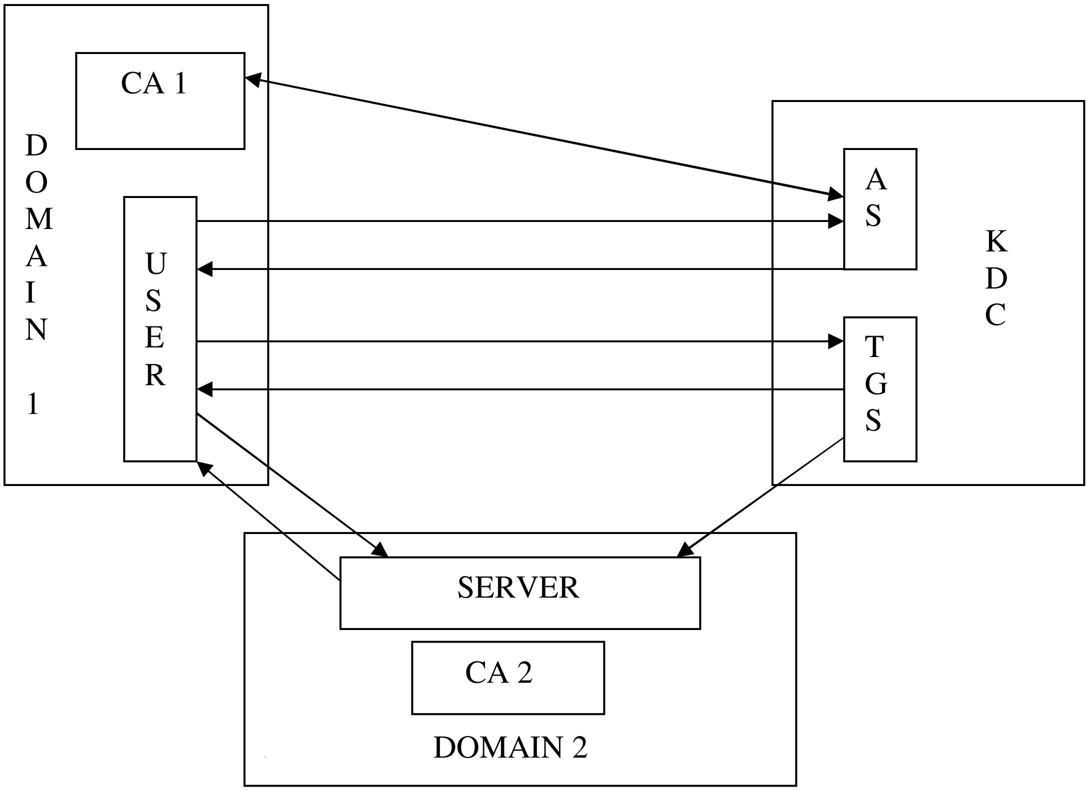


FIGURE2: New model based on PKI and Kerberos

5.1 Model Work Flow

5.1.1 U → AS: PKAS (CertU, U, TGS)

U→S: First, user sends a request to the AS (Authentication server) for establishing session with TGS. The message is encrypted with PKAS (public key of AS) by the user. The message also contains the user's digital certificate CertU, which is issued by CA1.

5.1.2 AS→U: PKU (KU, TGS, KAS, TGS (TU, TGS), PKTGS)

AS→U: When AS decrypt the request, he gets the CertU and verifies the user's identity. If AS can make sure the request sender is unquestionable the one asserted, AS generates the session key KU, TGS which will be used for the communication of the user and TGS. The response to the user from AS will be encrypted by PKU (user's public key). The response contains the session key KU, TGS, the ticket ZU, TGS which will be encrypted by KAS, TGS shared only by AS and TGS.

5.1.3 U→TGS: PKTGS (KU, TGS, S, KA, TGS (TU, TGS))

U→TGS: User uses his private key SKU to decrypt the response, and then he will get a session key KU, TGS and a cipher text TU, TGS. Second, user sends a request to the TGS in order to get the permission for visiting the server S. The request contains the name of the server, the session key KU, TGS shared between the user and the TGS, and the ticket TU, TGS which encrypted with KA, TGS by AS. User can not modify the ticket in private.

5.1.4 TGS→U : KU, TGS (TU, S, KU, S)

TGS→U: When the request arrives, TGS uses his private key SKTGS to decrypt the request and get the session key KU, TGS and the cipher text of ticket TU, TGS. Then, TGS decrypts the cipher text and gets the ticket. If the ticket is authentic, TGS issues the ticket TU, S and the session key KU, S which is shared by the user and the server.

5.1.5 TGS→S: SKTGS (U, H (TU, S), SHA1, KU, S)

TGS→S: While TGS sends the session key to the user, TGS also sends the server a message of notification which contains the name of the user, a message digest of the ticket TU,S , the hash algorithm and the session key KU, S .

5.1.6 U→S: KU, S (TU, S, U, CertU, R1):

U→S: The user access the resource server as soon as he gets the ticket. Before establishing the secure communication between them, user has to send a message encrypted with KU, S. The message contains the ticket TU, S, the user's name U, user's certificate CertU and a random number R1.

5.1.7 S→U : KU, S (R1,"OK"):

S→U: When the server has verified the identity of the user, he sends a response back. From now on, the trust relationship has been established.

5.2 Model Analyses:

- Trust relationship between heterogeneous domains can be established by adopting this model, featuring strong expandability and capability of mutual communication. The demand of interlinking different domains without any modification to the security policy or the architecture of the domain could be met.

- The model uses Kerberos protocol for the authentication between domains, greatly cutting down time waste and resource waste on building and verifying the certificate path, which is a disadvantage of the old PKI model.

- The trust between domains is built on the validity of the ticket, which is issued by the KDC of the Kerberos system. The format and content of the ticket is much more fixed than the certificate based on X.509. In this way, valid certificate regarded as invalid due to its different format will be avoided during the process of authentication.

- The Kerberos system would only store the session keys with which to communicate with CAs of different domains, rather than generate or maintain a large number of session keys for the users.
- The Kerberos server is only responsible for setting up cross-domain communication and granting tickets, while any addition or reduction to the number of the users or authentication registration falls to the CA's Obligation. Users in different domains follow the different security policies based on PKI. Each domain' CA takes the responsibility of user management, such as user's registration, increasing or decreasing a member. This model not only lightens the burden of the system, but will not affect or depend on the domains' architecture which might be different because of various working styles. When the KDC is under attack or fails to work properly, it will not cause trouble to the inter-domain management and communication.

- How the KDC distributes or isochronously updates the session keys to the CAs is not included, as proper answers could be found in the field of security requirement of the actual system.

6. PMI (Privilege Management Infrastructure)

The binding of a privilege to an entity is provided by an authority through a digitally signed data Structure called an attribute certificate. In general case, entity privileges have lifetimes that do not match the validity period for a public -key certificate.

The use of attribute certificates, issued by an Attribute Authorities (AA) provides a flexible Privilege Management Infrastructure (PMI) which can be established and managed independently from a PKI. At the same time, there is a relationship between the two infrastructures. Since PMI doesn't provide the mechanism to trust certificate holder's identity, PKI is used to authenticate identities of issuers and holders in attribute certificates.

6.1 Attribute Certificates

The public-key certificate proves the identity of the entities. However, they do not specify what the entities can do. Attribute certificates were developed to provide this access control. An attribute certificate has the similar data structure as a public-key certificate. But an attribute certificate does not contain the subject's public key. Instead, it contain s the attributes (privileges) of the holder.

6.2 Attribute Authority, SOA

The Attribute Authority (AA) and Certification Authority (CA) are completely independent. The creation and maintenance of 'identity' can be separated from the PMI. The Source of Authority (SOA) – analogous to a 'root CA' in the PKI – is the entity that is trusted by a privilege verifier as the entity with ultimate responsibility for assignment of a set a privileges. An SOA is itself an AA as it issues certificates to other entities in which privileges are assigned to those entities.

PMI framework support privilege delegation as an optional feature. SOA assigns privilege to an entity that is permitted to also act as an AA and further delegate the privilege. Delegation may continue through several intermediaries AA's until it is ultimately assigned to an end -entity that cannot further delegate that privilege. The attribute certificate extension provide one mechanism that can be used by an SOA to make privilege attribute definitions and associated domination rules available to privilege verifiers.
An attribute certificate that contains this extension is called an attribute descriptor certificate and is a special type of attribute certificate.

7. DIRECTORY SCHEMA OF PKI AND PMI

X.509 standard defines the directory schema of PKI and PMI.

Directory schema:

A directory schema specifies the types of objects that a directory may have and the mandatory and optional attributes of each object type. The schema is made up of two things: object classes, and attributes. Following definitions of object classes and attributes are cited from Netscape Directory Administration Guide.

Object Classes
Object classes define the types of attributes an entry can contain. Most object classes define a set of required and optional attributes. This attribute list represents the kind of data that you both must and may store on the entry.

7.1 PKI directory schema

X.509 standard defines PKI directory schema as follows:

Object classes	**Attributes**
Certificate Authority	CA certificates, cross-certificates CRLs, ARLs
Certificate User	Public-key certificate
CRL distribution point	CRLs, ARLs, delta -CRLs
CP & CPS	CPs, CPSs
Certification Path	Certification path(Sequence of cross-certificates)

TABLE 1: PKI directory schema

7.2 PMI directory schema

X.509 standard defines PMI directory schema as follows:

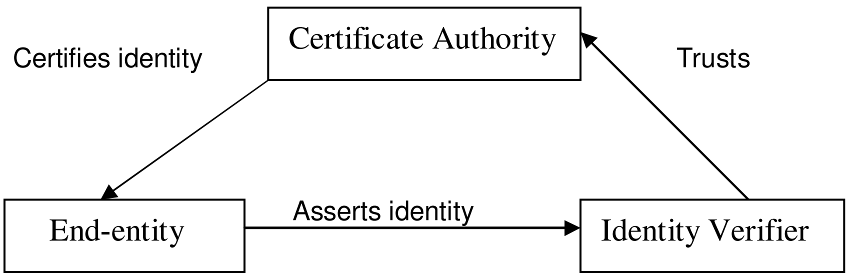
Object classes	**Attributes**
Source of Authority (SOA)	ACRLs, AARLs, attribute descriptor certificate
Attribute Authority (AA)	AA certificate, ACRLs, AARLs
Certificate Holder	attribute certificate
CRL distribution point	ACRLs, AARLs, delta-ACRLs
Privilege Policy	Privilege policies
Delegation Path	Delegation path(Sequence of attribute certificates)

TABLE 2: PMI directory schema

8. AUTHENTICATION AND AUTHORIZATION MODEL IN PKI and PMI

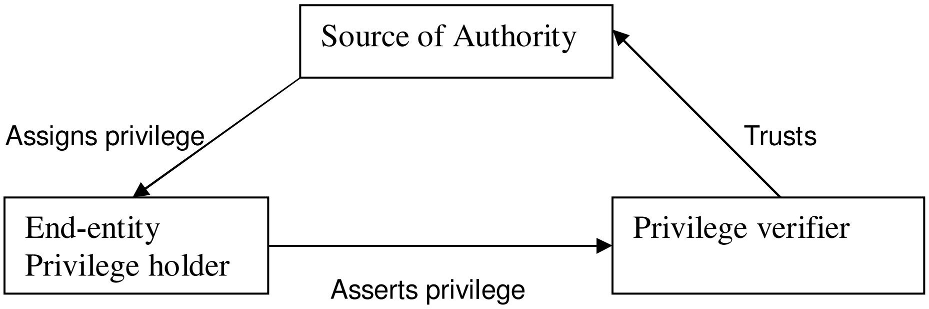
8.1 Authentication Model

The authentication model consists of three entities: the Certificate Authority, the End-entity, and the identity verifier. The identity verifier is the entity that makes the determination as to whether or not asserted identity is correct. The Certificate Authority certifies the end -entities by issuing public-key certificates for them. The identity verifier trusts the CA as the authority for a given certification for the identity. If an end entity's certificate is not issued by that CA, then the identity verifier must locate a certification path of certificates from that of the entity to one issued by the CA.



8.2 Authorization Model

X.509 attribute certificate framework defines authorization models in PMI environment as follows. The basic privilege management model consists of three entities: the SOA, the privilege holder and the privilege verifier. The privilege holder is the entity that holds a particular privilege and asserts its privileges for a particular cont ext of use. The privilege verifier is the entity that makes the determination as to whether or not asserted privileges are sufficient for the given context of use.



8.3 A Comparison of PKI with PMI

Sr. No.	Concept	PKI Entity	PMI Entity
1.	Certificate	Public Key Certificate	Attribute Certificate
2.	Certificate issuer	Certification Authority	Attribute Authority
3.	Certificate user	Subject	Holder
4.	Certificate binding	Subject’s name to public key	Holder’s name to privilege attribute(s)
5.	Revocation	Certificate revocation list (CRL)	Attribute certificate revocation list (ACRL)
6.	Root of trust	Root certification authority	Source of authority
7.	Subordinate authority	Subordinate certification authority	Attribute authority

TBALE 3: Comparison of PKI with PMI

9. OUTPUT OF THE RESEARCH WORK

9.1 PKI: A PKI is not an authentication method; rather it is an infrastructure that uses digital certificates as an authentication mechanism and is built to better manage certificates and their associated keys. A digital certificate is itself a way to reliably identify the user or computer claiming to be the owner of a specific public key.

If we find the use of PKI as authentication we are comes to know that certificate authority checks the user. Different CA's have different identity validation procedures. Some may grant the user a digital certificate with only a name and email address, while others may involve personal interviews, background checks etc. (Remembering that authentication is a process of validating an identity based on risk means that certificate authorities' digital certificate has a wide range of trust…caveat emptor). The user is granted a digital certificate. Often there are two components to this; private and public keys.

The user wishes to send an email to a business associate. The user digitally signs the email with their private key. The email is sent to the business associate. The business associate uses the sending user's public key to decrypt the message. The use of digital certificates in this example provides confidentiality, message integrity and user authentication without having to exchange secrets in advance. PKI was oversold on its capabilities when it was originally introduced several years ago. There were serious problems with browser incompatibilities, costs associated with issuing and managing digital certificates and a business environment that had not yet widely adopted the internet to rethink business processes between enterprises.

9.1.1 What is the PKI Made Of?

A PKI can be implemented within an organization, for the use of the users on its network, or it can be a commercial entity that issues certificates to Internet users, for example. Either way, the PKI consists of the following components:

- At least one certification authority (CA) to issue certificates.
- Policies that govern the operation of the PKI.
- The digital certificates them selves.
- Applications that are written to use the PKI.

9.1.2 Applications of PKI

Applications must be PKI-aware in order to work with the certificates and use them for authentication purposes. Web browsers, email clients and many applications that are built into the Windows 2000/XP operating systems such as EFS and IPSec are PKI-aware, as are the operating systems themselves.

9.2 Kerberos: Kerberos is a solution to your network security problems. It provides the tools of authentication and strong cryptography over the network to help you secure your information systems across your entire enterprise. We hope you find Kerberos as useful as it has been to us.

9.2.1. Benefits of Kerberos

A properly deployed Kerberos Infrastructure will help you address these problems. It will make your enterprise more secure. Use of Kerberos will prevent plaintext passwords from being transmitted over the network. The Kerberos system will also centralize your username and password information which will make it easier to maintain and manage this data. Finally, Kerberos will also prevent you from having to store password information locally on a machine, whether it is a workstation or server, thereby reducing the likelihood that a single machine compromise will result in additional compromises. To summarize, in a large enterprise, the benefits of Kerberos will translate into reduced administration costs through easier account and password management and through improved network security. In a smaller environment, scalable authentication infrastructure and improved network security are the clear benefits.

9.3 An Improved Trust Model:

An Improved Trust Model was introduced which is a model for authentication and authorization between trust domains. It is based on PKI and Kerberos. How the data should encrypt and decrypt by using user’s private, public and session keys through model work flow.

9.4 PMI: PMI is depends on the attribute certificates issued by an Attribute Authorities, PMI doesn’t provide the mechanism to trust certificate holder’s identity while PKI is used to authenticate identities of issuers and holders in attribute certificates.

9.4.1 Significance and use of PMI

Supporting distributed heterogeneous application architecture with a homogeneous distributed security infrastructure leveraged across the enterprise; providing user and service identities and propagation; and providing a common, consistent security authorization and access control infrastructure. It used in the existing standards like ANSI X9.45, ISO 9594-8, IETFRFC 3280 X.509, OASIS SPML, SAML, WS-*, and XACML etc..

9.5 X.509 Standard: X.509 standard defines the directory schema of PKI and PMI where directory schema is describes the types of objects in the directory and its optional attributes.

9.5.1 Applications with X.509 standard

Probably the most widely visible application of X.509 certificates today is in web browsers (such as Netscape Navigator and Microsoft Internet Explorer) that support the SSL protocol. SSL (Secure Socket Layer) is a security protocol that provides privacy and authentication for your network traffic. These browsers can only use this protocol with web servers that support SSL.

9.5.2 Other technologies that rely on X.509 certificates include

- Various code-signing schemes, such as signed Java Archives, and Microsoft Authenticode.
- Various secure E-Mail standards, such as PEM and S/MIME.
- E-Commerce protocols, such as SET.

10. APPLICATION WITH AUTHENTICATION AND AUTHORIZATION MODELS

In case of finding use of authentication and authorization model with system application I am giving example of tool provided by the Microsoft called as SharePoint on the role based membership to access only restricted data. Microsoft SharePoint Foundation supports security for user access at the Web site, list, list or library folder, and item levels. Security management is role-based at all levels, providing coherent security management across the SharePoint Foundation platform with a consistent role-based user interface and object model for assigning permissions on objects. As a result, list-level, folder-level, or item-level security implements the same user model as Web site–level security, making it easier to manage user rights and group rights throughout a Web site. SharePoint Foundation also supports unique permissions on the folders and items contained within lists and document libraries. Authorization refers to the process by which SharePoint Foundation provides security for Web sites, lists, folders, or items by determining which users can perform specific actions on a given object. The authorization process assumes that the user has already been authenticated, which refers to the process by which SharePoint Foundation identifies the current user. SharePoint Foundation does not implement its own system for authentication or identity management, but instead relies solely on external systems, whether Windows authentication or non-Windows authentication.

SharePoint Foundation supports the following types of authentication:

- Windows: All Microsoft Internet Information Services (IIS) and Windows authentication integration options, including Basic, Digest, Certificates, Windows NT LAN Manager (NTLM), and Kerberos. Windows authentication allows IIS to perform the authentication for SharePoint Foundation

Finally, we found that the authentication model consists of three major entities like Certificates Attributes, End-entity, and the identity verifier and authorization model consists of three major entities like SOA, the privilege holder and the privilege verifier. A PMI is to authorization what a PKI is to authentication

CONCLUSION

In this paper, two representative protocols of authentication and authorization are analyzed and compared with. Then a new high-compatible trust model is proposed. This model helps to realize the aim of interlinking heterogeneous domains supported by different authentication technique and security policy. However a security policy or trust model, no matter how ideal it is theoretically, could not speak well for its feasibility. To imperfect this model, future studies will be focused into strengthening the ticket validity and enhancing mutual authentication efficiency according to the characteristics of the distributed network environment. The protocols are described in this paper are basically used on the basis of Certificate Authority to checks the users for security purpose and to introduce that on which major entities the authentication and authorization models are depends. I conclude that data from users are encrypt and decrypt by using the key through these protocols helps for the security of the distributed systems.

REFERENCES

[1] Thompson MR, Olson D, Cowles R, Mullen S, Helm M. CA-Based trust model for grid authentication and identity delegation. In: Proc. of the GGF7. 2003.

[2] Neuman C. RFC 1510, The Kerberos Network Authentication Service (V5) [S]. 1993.

[3] Bellovin S M, Merritt M. Limitation of the Kerberos authentication system [A].Proceedings of the Winter 1991 Usenix Conference [C]. 1991.

[4] Guan Zhen-sheng, Publication Key Infrastructure PKI and the applications. Beijing: Publishing House of Electronics Industry. 2008.1

[5] Wen Tei-hua, Gu Shi-wen, An improved method of enhancing Kerberos protocol security, Journal of China Institute of Communications, Vol 25 No 6. June 2004, pp. 76-79.

[6] Burr W E. Public Key Infrastructure (PKI) Technical Specifications: Part A-Technical Concept of Operations: [WORKING Draft] TWG-98- 59. Federal PKI Technical Working Group. Sep. 1998

[7] [X.509] CCITT Recommendation X.509, The Directory: Authentication Framework, 1997

[8] Internet X.509 Public Key Infrastructure Certificate and CRL Profile
URL: http://search.ietf.org/internet -drafts/draft-ietf-pkix-new-part1-09.txt

[9] An Internet Attribute Certificate Profile for Authorization
URL: http://search.ietf.org/internet -drafts/draft-ietf-pkix-ac509prof-09.txt

[10] X.509 4th edition: Overview of PKI & PMI Frameworks (Entrust, Inc.)
URL: http://www.entrust.com/resources/pdf/509_overview.pdf

[11] Certificate Revocation in Public Key Infrastructures
URL: http://www.sans.org/infosecFAQ/encryption/cert_ rev.htm

[12] Tips for LDAP users
URL: http://www.ymtech.co.kr/ref/java/jnditutorial -may1/ldap/index.html

[13] Netscape Directory Server Administration Guide
URL: http://home.netscape.com/eng/server/directory/3.0/ag/contents.html

[14] S. Chokhani (CygnaCom) & W. Ford (VeriSign, Inc.) Internet X.509 Public Key Infrastructure
Certificate Policy and Certification Practices Framework
URL: http://www.i etf.org/rfc/rfc2527.txt

[15] Kerberos and Authentication
URL: http://web.mit.edu/kerberos/#what_is

[16] Authentication, Authorization and Accounting
URL: www.infosectoday.com/Articles/Authentication.html

[17] Strong authentication and authorization models
URL: www.sans.org/.../strong-authentication-authorization-model-pki-pmi- directory_747

[18] Role of PKI
URL: www.windowsecurity.com/.../Understanding_the_Role_of_the_PKI.html

[19] An X.509 Role-based Privilege Management Infrastructure
URL: www.permis.org/files/article1_chadwick.pdf

[20] ASTM E2595 - 07 Standard Guide for Privilege Management Infrastructure.
URL: http://www.astm.org/Standards/E2595.htm

[21] Recommendation X.509 and ISO 9594-8, Information Processing System – Open Systems Interconnection - The Directory - Authentication Framework, 1988.
URL: http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper075/paper.pdf.