Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Strong Authentication and Authorization model Using PKI, PMI, and Directory

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. Both PKI and PMI are described in X.509 standard 4th edition.

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

Strong Authentication and Authorization model Using PKI, PMI, and Directory

Jong Wook Lee

October 25, 2001

Introduction

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. Both PKI and PMI are described in X.509 standard 4th edition.

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.

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 (e.g.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Directory), without special efforts to protect them.

Generation of key pairs

A user's key pair can be generated in three different ways according to the standards[1].

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.

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.

Certificate validation

Certificates may be revoked by CA prior to their expiration time. Authorities are required to state the way

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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

Certification Path

According to the PKI standards, there are two primary types of public-key certificates, user certificates and CA-certificates. An *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.

Certificate Policy & Certification Practice Statement

X.509 standard[7] defines certificate policy as a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. An indication of certificate policy may be contained in a certificate and a certificate user may use this certificate policy to decide whether he can trust a certificate for a particular purpose or not.

A Certification Authority (CA) may limit the use of its certificates in order to control the risk assumed as a result of issuing certificates. For example, CA may put restrictions on the community of certificate users, the purposes for which they may use its certificates and/or the type and extent of damages that it is prepared to make good in the event of a failure on its part, or that of its end-entities. The certificate policy should define these matters, and all certificates are issued in accordance with the policy.

A certification authority employs Certification Practice Statement(CPS), a statement of the practices, for issuing certificates. A CPS is a detailed statement by a certification authority as to its practices, that potentially needs to be understood and consulted by subscribers and certificate users (relying parties). CPSs will generally be more detailed than *certificate policy* definitions even though the level of detail may be dependent on CPSs. Indeed, CPSs may be quite comprehensive and robust documents. They provide a description of the precise service offerings, detailed procedures of the life-cycle management

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

of certificates, and more - a level of detail which weds the CPS to a particular (proprietary) implementation of a service offering.

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.

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 contains the attributes (privileges) of the holder.

By definition[2], An attribute certificate contains following information and is digitally signed by issuer to provide the integrity.

- Version : the version number of certificate.
- Holder : the identity of the attribute certificate's holder.
- Issuer : the identity of the AA that issued the certificate.
- Signature : the cryptographic algorithm used to digitally sign the attribute certificate.
- Serial number : the serial number that uniquely identifies the attribute certificate within the scope of its issuer.
- Validity : the time period during which the attribute certificate is considered valid.
- Attributes : the attributes associated with the holder that are being certified.
- Issuer unique ID : the issuer of the attribute certificate in instances where the issuer component is not sufficient.
- Extensions : allows addition of new fields to the attribute certificate.

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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

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 intermediary AAs 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.

Directory schema of PKI and PMI

X.509 standard defines the directory schema of PKI and PMI[1], [2].

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[5].

Object Classes:

Object classes define the types of attributes an entry can contain. Most object class 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.

For example, if you define an entry to use the "organizationalPerson" object class, then the 'common name' and 'surname' attributes are required for the entry. In addition, there is a fairly long list of attributes that you can optionally use on the entry. This list includes such descriptive attributes as "telephoneNumber", "userID", "streetAddress", and "userPassword".

The object classes for all objects in the directory form a class hierarchy. For example, the "organizationalPerson" object class is a subclass of the "Person" object class. When creating a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

new Directory entry, you must always specify all of the object classes to which the new entry belongs.

Attributes

A list of all of the possible attributes for object classes is the second part of the schema. Attributes hold information about a specific descriptive aspect of the entry. Each attribute consists of an attribute type and one or more attribute values. The attribute type identifies the class of information given by that attribute (for example, telephone number). The attribute value is the particular instance of information appearing in that entry (for example, 555-1999).

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)

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)

* ACRL : attribute CRL, AARL : attribute ARL

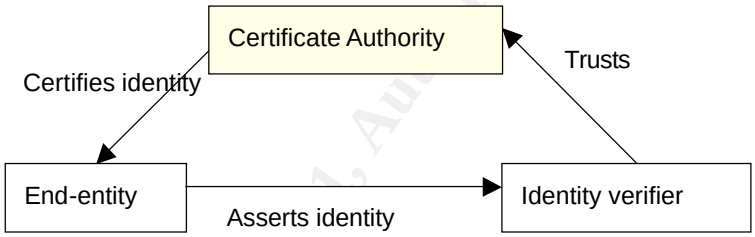
© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Authentication and authorization model in PKI and PMI

Authentication model

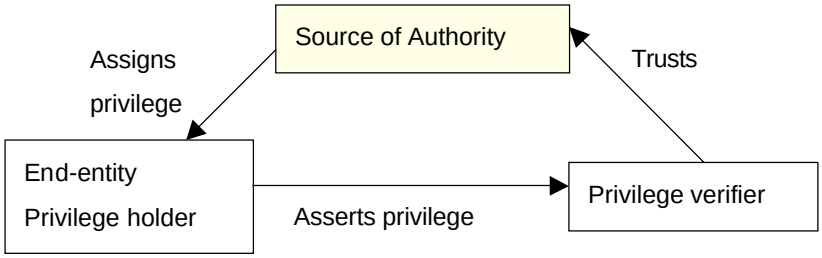
The authentication model consists of three entities: the Certificate Authority, the End-entity, and the identity verifier. The identity verifier is the entity that makes the determination as to whether or not asserted identity is correct. The Certificate Authority certifies the end-entities by issuing 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.



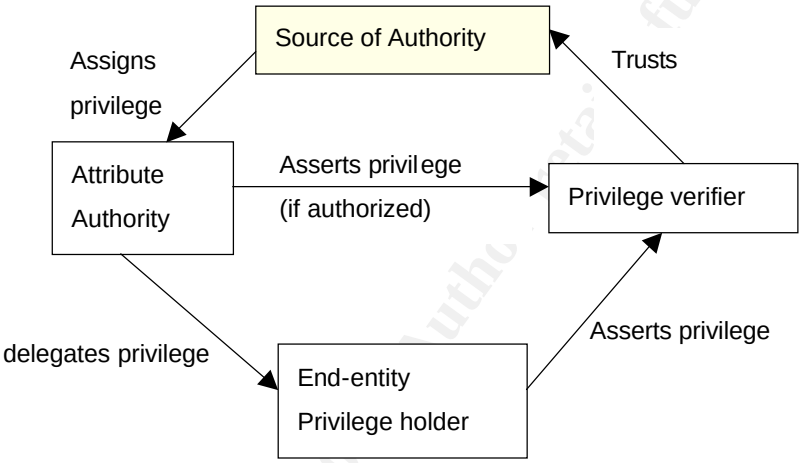
Authorization model

X.509 attribute certificate framework[2] 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 context 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.



© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Delegation model is an optional aspect of the PMI framework. There are four components of the delegation model: the privilege verifier, the SOA, other AAs and the privilege holder. The privilege verifier trusts the SOA as the authority for a given set of privileges for the resource. If the privilege holder's certificate is not issued by that SOA, then the privilege verifier must locate a delegation path of certificates from that of the privilege holder to one issued by the SOA. The validation of that delegation path must include checking that each AA had sufficient privileges and was authorized to delegate those privileges.



References

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

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

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

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

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

[5] Netscape Directory Server Administration Guide

URL : http://home.netscape.com/eng/server/directory/3.0/ag/contents.html

[6] Certificate Revocation in Public Key Infrastructures

URL : http://www.sans.org/infosecFAQ/encryption/cert_rev.htm

[7] S. Chokhani (CygnaCom) & W. Ford (VeriSign, Inc.) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

http://www.ietf.org/rfc/rfc2527.txt (March 1999)

© SANS Institute 2001, Author retains full rights

Last Updated: May 26th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**