EAI Endorsed Transactions
on Cloud System

Research Article EAI.EU

STRENGTHENING SSL SECURITY WITH ATTRIBUTE CERTIFICATE

Rajesh Kumar [1], K.Rekha[2]

[1] School of Computing Science and Engineering, VIT University, Chennai, India, rajesh.kumar@vit.ac.in
[2] School of Computing Science and Engineering, VIT University, Chennai, India, rekhakatkam086@gmail.com

Abstract

Now-a-days many people do multiple activities, transactions in fields such as finance, banking, business sector etc over internet. These activities, transaction should be secure. Providing security and authorization control has became the major concern in the globalization of internet. We are inspired by the need and urgency to handle the present situations and to put forward a strong authorization methodology in the globalization of web environment. Public Key Infrastructure which we are using now is meant to provide strong authentication by the use of digital certificates. In this paper we introduce a new technology of Privileged Management Infrastructure which provides strong authorization by the use of attribute certificates. Also in order to introduce attribute certificate we primarily need to check the genuineness of SSL digital certificate i.e. whether the SSL digital certificate is genuine or it's a fake certificate.

Keywords: SSL, Attribute Certificate, PMI, PKI.

Received on 01 March 2018, accepted on 03 April 2018, published on 11 April 2018

doi: 10.4108/eai.11-4-2018.154465

1. Introduction

Secure Socket Layer(SSL) is one of the reputed methods for providing securing for the internet transactions all over the world through world wide web(WWW).SSL was primarily introduced in 1994 by the Netscape company which have got familiarized very rapidly among various web browsers such as Microsoft and Netscape[1]. Its main intention is to provide security for the confidentiality of on-line transactions. It also provides security for the E-commerce. SSL has now developed to pave the way of communicating various types of tactful data like tax returns, bill payments, banking statements, and stock purchases on the Internet. Through various forms of Internet spies or intruding such as hacking, uncertified people can steal privileged data, such as PIN numbers, credit card numbers and other peculiar data. SSL protocol has made rapid progressed to dispatch the data confidentially and firmly over the Internet.

In SSL protocol handshake process (Figure1, Figure2), there exists a procedure of reciprocating each other's certificates among client and server for individual attestation which will increase the safety of the connection established among client and server, while still there are some limitations or security flaws: SSL protocol doesn't allow control of access function, diverse users connect to the same server use the same access rights(authorization) which is inadequate for real time applications; SSL protocol can reinforce only peer–to-peer(one-to-one) SSL connection ,we cannot acquire multiple certificate and multilevel chain of trust relationship. For the above limitations this paper introduces Attribute Certificate to increase the security of faith on both client and server entities. Also it improves the SSL handshake process. The property of an object such as role, security clearance, group, access of identity can be represented by an attribute. These attributes can be used for many real time applications involving online transactions, authentication, access authorization etc. An X.509 certificate provides the users with keys[5]. These certificates may be extended to provide attribute based secure services. These extensions further adds to security services based on authentication, integrity and confidentiality.

The clients can validate the servers by verifying their X.509 digital certificates, exchanged using SSL. The digital certificate is issues by a trusted certificate authority (CA). In the process of verification the client verifies if the certificate is issued by a trusted CA[3]. If the server certificate is not issued by trusted CA, the client can decline connection to server. SSL is used to enable secure HTTP among browsers and websites. It is also used for secure email transfer, and secure exchange of chat messages. The key in certificate exchanged using SSL is used for encrypting the data over internet. SSL enables the confidentiality, integrity, availability for various transactions and activities over internet. In Man in-the-middle (MITM) attack, the attacker sends forged certificate to client as imposter for server. The client may exchange data with attacker thinking it as actual server. MITM can be prevented by verification of certificate by client.

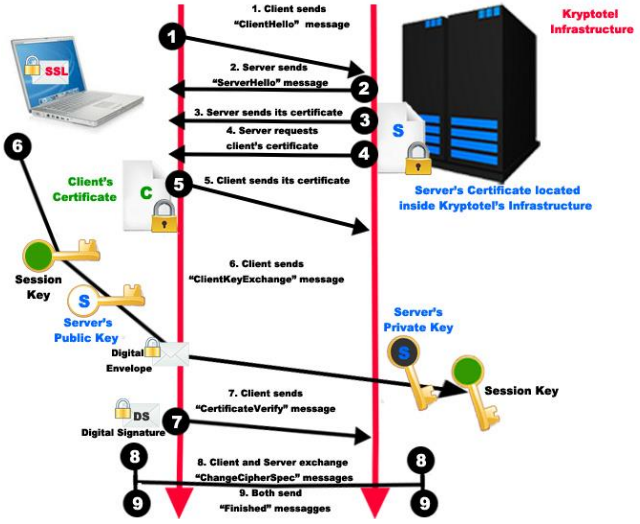
1. Client sends "ClientHello" message
2. Server sends "ServerHello" message
3. Server sends its certificate
4. Server requests client's certificate
5. Client sends its certificate
6. Client sends "ClientKeyExchange" message
7. Client sends "CertificateVerify" message
8. Client and Server exchange "ChangeCipherSpec" messages
9. Both send "Finished" messaggees
SSL
Kryptotel Infrastructure
S
Server's Certificate located inside Kryptotel's Infrastructure
Client's Certificate
C
Session Key
S
Server's Public Key
Digital Envelope
Server's Private Key
S
Session Key
DS
Digital Signature
1
2
3
4
5
6
7
8
8
9
9

Figure 1. SSL Handshake Process.

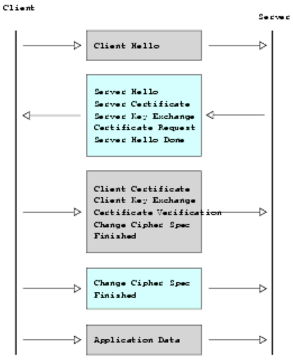

Figure 2. SSL Handshake steps

The application for a websites cannot detect the MITM attack for multiple set of clients. Many clients do not use the certificate at all [2]. Those clients cannot attest server certificate. Hence, the server cannot depend on attestation of server certificate from a SSL client. It is also difficult for server to distinguish between normal client and a MITM attacker. In addition, there are latent SSL connection and the web applications use networking Application programming Interface (API) such as WebSocket, XMLHttpRequest. They do not access SSL handshake directly. Hence, they can not authorize the SSL certificates.

A certificate is a signed document by a CA. It contains the keys for encryption. The CA is the trusted third party, who can be contacted for getting validity of certificate. CA signs the document with its private keys and can decrypted using the public key of CA. For well-known third party, everyone has the public key of well-known third party and can decrypt, ensure the information present in the certificate is authentic and has not been altered. It establishes the trust for information present in the certificate document. The CA identifies the subject in certificate in a proper manner with a property and context for a certificate type. The subject is identified with a id or name and property attached is public key. Such certificate may be extended to bind the identity with a set of attributes. Such a extended certificate is useful for access control in distributed systems, role of a user in a system [2]. The TTP which can extend such a certificate is named as Attribute Authority (AA). The AA issue Attribute Certificate (AC) with binding of user to identification and access rights. For an entity which is responsible for access control of objects under its control, can use the attribute certificate to verify the access rights. The entity then can allow the user with established identity to access objects as per access control. With this the need for Access Control List (ACL) goes away. The advantage with AC is the identity of user is established and the entity in control of object need not repeat verification of subject-identity each time access to object is required like ACL or other methods.

Attribute Certificates which we are introducing here provides a solution for authorization of services. The AC's are designed to say (potentially short-span) attributes about a given subject to provide flexible and scalable privilege management. AC points to a public key certificate which is used for authenticating the identity of AC holder. Access control decisions are made by an authorization policy, and the authorization policy in-turn is driven and verified by an AC.

Privilege Management Infrastructure (PMI) authorizes access to objects after authentication has been completed[4]. AC is use in PMI. PKI uses general digital certificate. The difference between PKI and PMI is former binds identified subject to a public key and later bind a identified subject to set of attributes related to access management. An authorization mechanism is developed in this paper by use of AC, PMI, and PKI.

2. Proposed work

Attribute certificate (AC) is introduced in this paper to enhance the trust level between server and client for real time applications that needs Identity authentication and access to type of data user is authorized to access such as category of information – classified, secret top secret, or access to certain information in database . Handshake process in SSL protocol is changed by applying AC. It improves identity authentication function of SSL. In addition, it helps detect MITM [3] [8] attack on top websites around the globe. Some minute changes or modifications are needed to increase or strengthen the security. The way cryptographic keys are enlarged from the formerly exchanged secret will be improved. The MAC construction is changed to HMAC. Implementations are further required to enhance support for Diffie-Hellman key agreement, the Digital Signature Standard, and Triple DES encryption.

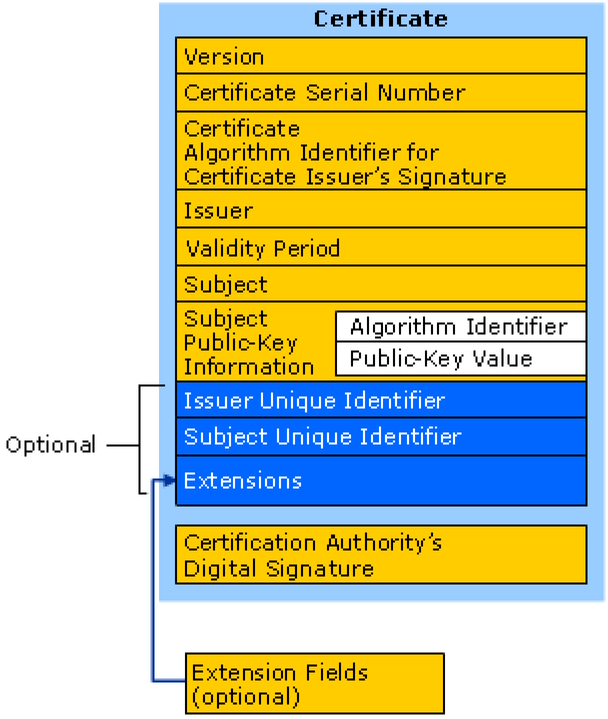
Certificate
Version
Certificate Serial Number
Certificate Algorithm Identifier for Certificate Issuer's Signature
Issuer
Validity Period
Subject
Subject Public-Key Information
Algorithm Identifier
Public-Key Value
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Optional
Certification Authority's Digital Signature
Extension Fields (optional)

Figure 3 Attribute Certificate

2.1. Attribute Certificate

Attribute Certificate (Figure 3) consists of a group of attributes. The attributes relate to owner. It defines the access rights of individual user in systems. Traditional Certificate (TC) is based on Public Key Certificate (PKC) and difficult to forge [6] [7]. AC is build using attributes of TC. In addition, Attributes Authority (AA) issues the attributes. X.509 defines the format of AC as follows:

```
Attr Cert ::= {ORDER
ACinfo             Attr Certinfo,
SignatureAlgo    Algoidentifier,
SignatureValue      BIT STRING}
AttrCertInfo  ::= ORDER{
Version              AttrCertVersion,
Holder               Holder,
Issuer               AttrCertIssuer,
Signature          AlgoIdentifier,
S.NO                             Cert,S.NO,
attrCertValidityPeriod       AttrCertValidityPeriod,
attributes                         ORDER of attributes,
issuerUnique ID           UniqueID OPTIONAL,
extensions                           Extensions OPTIONAL}
```

Handshake process of SSL can be improved by use of AC. The attributes in AC can correctly authorize user for data access by user Identification and access to type of data. It means use of AC results in reduction of security flaws of SSL.

2.2. Checking Attribute Certificate

Handshake process of SSL protocol is analyzed to introduce additional functionality to add AC and to verify the attributes of communication matching the AC. In handshake process the server verifies general certificate of client and then uses two newly introduced functions first one to to load the AC and second to verify it. The Function SSL_XYZ_load_AC_file() loads the AC certificate and function SSL_XYZ_verify_AC_file() verifies the attributes as per AC. Pseudo code of the function is given below:

```
int SSL_XYZ_load_AC_file (SSL_XYZ *xyz, const char *filename)     // Function for loading AC
Holder XYZ ←Holder
Attrcert issuerXYZ←Attrcert issuer
Algo identifierXYZ←Algo identifier
AttrValidityPeriodXYZ←AttrValidityPeriod
ORDER of attributeXYZ←ORDER of attribute
        //add original attribute value,
        // Returns -1, if loading failed.
}
```

After loading the AC, authenticity of AC must be verified. Few of attributes verify are Public Key Certificate(PKC), issuer of public key, user values, role of attribute values as given in Object Identifier(OID). For authentication, we have to verify the owner item present in the server. Attribute values are sent to Attribute Authority(AA). AA verifies the identity of attributes and result is sent to the server.

```
 int SSL_XYZ_Verify_AC_file (SSL_XYZ *xyz)
{
Return -1, if (verification fails).
Communication between AA and server
Sever sends attribute values (Remaining) to AA
 Return -1, If ((AttrCertIssuerXYZ && AlgorithmIdentifierXYZ && AttrCertValidityPeriodXYZ) == false)
Identity is verified at server using OID,
Returns the role for user as int values (role1=secret)
}
```

Correct character type (role of client) is represented by positive return value. Client will be able to access information as per role type. Client will not be authorized to access information if return value is zero. This is contribution of AC for improved trust between client and server.

In the process of client verification, the sever asks the client both general certificate (PKC) and attribute certificate verification. Client shares the public key certificate and attribute certificate with server. The server checks the certificate received from the client, extracts the primary attribute values in attribute certificate and shares it with to AA for further verification. AA verifies the authenticity of attribute values present in AC. Subsequently, the AA determines the job or role of client as in its database. The role data is shared with the server. The handshake process concludes with verification of both the certificates. The server knows the role determined by AA. The server guarantees the client access to system as per role. The client is able to communicate with the server and system as per its role in the attribute certificate. The figure3, figure4 depicts the usage of attribute certificates.

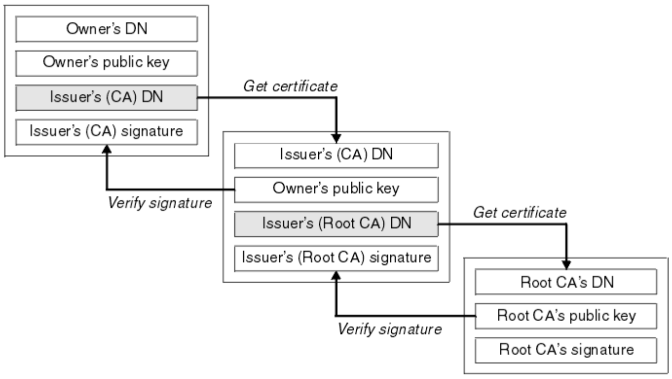

Figure 4. Trusted Third Party relation for Digital certificate

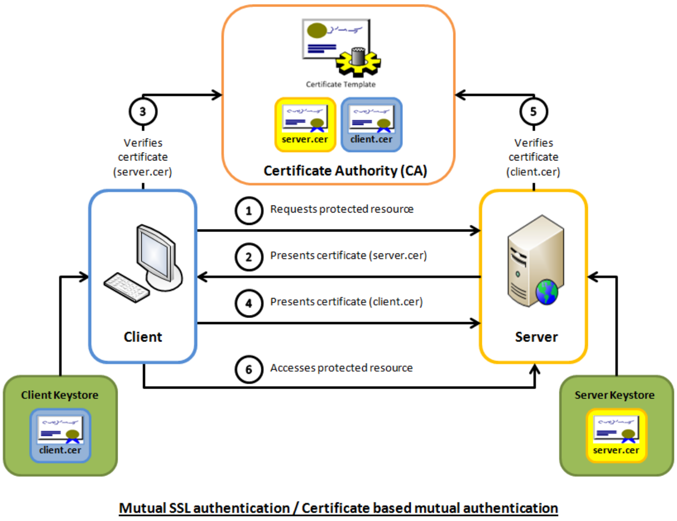
Certificate Template
server.cer
client.cer
Certificate Authority (CA)
3
Verifies certificate (server.cer)
5
Verifies certificate (client.cer)
1
Requests protected resource
2
Presents certificate (server.cer)
4
Presents certificate (client.cer)
6
Accesses protected resource
Client
Server
Client Keystore
client.cer
Server Keystore
server.cer
Mutual SSL authentication / Certificate based mutual authentication

Figure 5. Trusted Third Party relation for Digital certificate

2.3. ALGORITHM DEVELOPED

2.3.1. Crypto Algorithms

SSL accepts a variety of unique cryptographic algorithms, or ciphers, by which it will utilize the ciphers for authentication, exchange of certificates, and constructing session keys. SSL authorized devices can be developed to support a various groups of ciphers, known as cipher suites. If an SSL authorized client and an SSL authorized server support multiple cipher suites, the client and server may obtain which cipher suites they are going to use in an attempt for achieving robust security supported by both client and server parties. SSL reinforce the following cipher suites: -

The constructed algorithm is as follows, Key exchange(asymmetric) algorithms are: -

Algorithm name	Key length(bits)
RSA (Rivest, Shamir and Adleman)	128
Fixed Diffie Hellman	upto 2048

Symmetric key algorithms:

Algorithm name	Key length(bits)
DES (Data Encryption Standard)	56
3 DES (Data Encryption Standard)	192

Hash algorithms

Algorithm name	digest length(bits)
MD5 (Message Digest)	128
SHA-1(Secure Hash Algorithm)	160

The asymmetric algorithms are used to construct the master secret. The symmetric key algorithms are used for encryption of very large amount of data. The hash algorithms are used for message authentication. It is called secure hashing.

3. CONCLUSION AND FUTURE WORK

By the research done in this paper it can be concluded that Identity authentication functionality in SSL protocol can be enhanced using attribute certificate. The trust relationship between server and client is established using many chain certificates at multiple levels. In future, the rate at which the number of transactions occurs in internet for ecommerce will increase and method may be used for trustworthy access control for user. Hence, proposed method can be triumphantly applied in the further advanced levels.

The current work which we are doing in this system is only supported to a level of LAN and this can be further enlarged to the MAN and WAN levels.

References

[1] LI Wei, XIANG Shuyue, CHEN Shuangbao. Improvement Method of SSL Protocol Identity Authentication based on the Attribute Certificate. In proceedings - 2012 International Conference on Computer Science and Service System: From Institute of Control and Computer Engineering North China Electric Power University Beijing.Website: xsy820000@163.com,2012

[2] Mr. Devendra Kumar, CS,UPTU, Mr. Pradeep Kumar Panwar ,MCA,UPTU, Security through SSL , ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering . Research Website: www.ijarcsse.com: From UPTU,India. Volume 2, Issue 12, December 2012.

[3] Rolf Oppliger, Günther Pernul, Christine Strauss. Using Attribute Certificates to Implement Role-based Authorization and Access Controls. Swiss Federal Strategy Unit for Information Technology (FSUIT), Monbijoustrasse 74, CH-3003 Berne, Switzerland.website: rolf.oppliger@isb.admin.ch

[4] Toni Nykänen. Attribute Certificates in X.509. Helsinki University of Technology Department of Computer Science and Engineering Toni.Nykanen@hut.fi.

[5] Ganesh Godavari, and Edward Chow. Secure Information Sharing Using Attribute Certificates and Role Based Access Control. Department of Computer Science, University of Colorado, 1420 Austin Bluffs Parkway Colorado Springs, Colorado 80917 USA gkgodava@cs.uccs.edu, chow@cs.uccs.edu.

[6] Wei Zhou, Christoph Meinel. Implement Role-Based Access Control with Attribute Certificates. FG Institut für Telematik, Universität Trier, D 54286 Trier, Germany {zhou, meinel}@ti.uni-trier.de.

[7] Jiangtao Li and Ninghui Li.”OACerts: Oblivious Attribute Certificates” CERIAS and Department of Computer Science, Purdue University. {jtli, ninghui}@cs.purdue.edu.

[8] Jing-Jang Hwang,Kou-Chen Wu, Duen-Ren Liu. Access control with role attribute certificates. Computer Standards & Interfaces, v 22, n 1, 43-53, March 2000.

[9] Frausto Paul,Antoine Christian. Role based control via attribute certificate. In proceedings - 2004 International Conference on Information and Communication Technologies: From Theory to Applications,April 2004.