Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 6, Issue, 05, pp.6792-6797, May, 2014

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SECURITY IN X.509 GRID CERTIFICATES

***Ravi Tomar and Anshuman Saurabh**

Department of CS & ITSwami Vivekanand Subharti University, Meerut, India

ARTICLE INFO

Article History:
Received 05th February, 2014
Received in revised form
19th March, 2014
Accepted 20th April, 2014
Published online 31st May, 2014

Key words:

Ogsa, Ssh, Gsi, Sacred, Ietf, Pkix, Vsc, Kca.

ABSTRACT

Proxy credentials are commonly used in security systems when one entity wishes to grant to another entity some set of its privileges. We have defined and standardized X.509 Certificates issuing procedures for the purpose of providing more secure and remotely available certificate, with the help of Client Authentication via Virtual Smart Card. We present here our motivations for this work coming from our efforts in Grid security, the Proxy Certificate itself, and our experiences in implementation and deployment.

INTRODUCTION

The grid concept is that a distributed collection of resources and services. The grid of the first generation have focused on data processing, where distributed computer groups worked to solve large-scale problems. However, the next generation networks will include a whole new set of skills; such as B2B and B2C transactions. While the nets lacked real standardization, many different companies are starting to use the grid, but run into problems when you try to link these proprietary mesh together. The current lead developer is a consortium of the Globe. The Globus software now uses X.509 certificates as a method of authentication and authorization of persons to use the resources. So far, the Globe was limited to the most basic level of exchange between the individual machines, information and computing resources. The future direction of Globus is already defined as a pull-out services on the basis of the architecture of the Web. This can be seen in the paper of the physiology of the grid and subsequent service Specification Document, which covers the proposed-OGSA (Globus grid-proxy-init http://globus.org) (Open Grid Service Architecture). Globe hopes to integrate this directly into the next issue of the Globus Toolkit. In order to achieve such significant changes in how the software works, Globe there will be many obstacles to overcome. In order to understand the issues raised by the current software architecture basic understanding of claims settlement nets now and in the future is important. The following section describes the main directions, exploring in detail the requirements focus on the area of security.

****Corresponding author: Ravi Tomar***
Department of CS & IT Swami Vivekanand Subharti University Meerut, India.

Security issues in grid computing

Some of the General issues faced in Grid computing are as in Traditional systems are user/client/host centric and Grid computing is data centric based architecture so the whole concentration and implementing structure if completely different in both the fields. Database-centric Architecture or data-centric architecture has several distinct meanings, generally relating to software architectures in which databases play a crucial role. Often this description is meant to contrast the design to an alternative approach. For example, using a standard, general-purpose relational database management system, as opposed to customized in-memory or file-based data structures and access methods. With the evolution of sophisticated DBMS software, much of which is either free or included with the operating system, application developers have become increasingly reliant on standard database tools, especially for the sake of rapid application development. (GSI Henri Mikkonen and Mika Silander2006)

General issues

In Traditional systems the system is protected from direct access from its users and it also protects the data of one user to get compromised from being access by any other user.Where in Grid computing, it does not provide direct access of data to the user and hence protects both data and system application from system where computation is done. Also it requires stronger/mutual authentication for both users and code to ensure that resources and data not provided by an attacker. It protects local execution from remote systems and also adds different admin domains/Security policies to make the system more secure. (Andrew Hanushevsky and Robert Cowles2003)

Authentication

Previously the system used to authenticate user/client to protect system, but in Grid systems the authentication is done differently. There is mutual authentication required to ensure that resources and data not provided by an attacker. Delegation of Identity is done to process that system grants one principal to authorize to act as another individual and also assumes another's identity to perform certain functions. For E.g., in Globus: use gridmap file on a particular resource to map authenticated user onto another's account, with corresponding privileges. Data origin authentication is must in grid systems to validate that the data is genuine and has not been altered.

Also there are different authentication techniques used in grid computing systems, some of them are listed below:

- Password based
- Kerberos based (authentication and key distribution protocol)
- SSL authentication
- PKI/Cert based systems

Authorisation

After Authentication, the next problem which we encounter in grid systems is Authorization. It is most important to authorize the correct user to access the data to avoid the system to compromise. In Previous systems we used to determine whether a particular operation is allowed based on authenticated identity of requester and local information.Where in Grid systems we determine whether access to resource/operation is allowed or not, so that we can access control list associated with resources, principal or authorized programs. It also adds a feature of distributed authorization in which we can authorize different users for different tasks like distributed maintenance of authorization information. There is single approach for systems as there are embedded attributes in digital certificates, also there is restricted proxy in which the user require authorization certificate that grants authority to perform operation on behalf of grantor. There is also an alternative for this problem in the system by providing a separate authorization server, but the solution to the problem is much costlier as comparatively. We may can use CAS (Community Authorization System) only for group authorization.

Integrity and Confidentiality

Next security issue in the Grid systems comes with Integrity and confidentiality with another system data. This issue is near about solved with the well-known methodology known as cryptography. Cryptography is an important part of preventing private data from being stolen. Even if an attacker were to break into your computer or intercept your messages they still will not be able to read the data if it is protected by cryptography or encrypted. In addition to concealing the meaning of data, cryptography performs other critical security requirements for data including authentication, repudiation, confidentiality, and integrity.

Assurance, Accounting and Audit

In grid systems we also face problems such as assurance, accounting and Auditing. It is necessary to assure that the requirement of candidate service provider meet the desired criteria necessary when the service is requested. Also it is necessary to track, limit and change in consumption of resources to account the use of resources in any means. When auditing recording of operations performed by systems and associate actions with principals is done to find out what went wrong, which is the most typical role of Intrusion Detection Systems.

Grid Security Infrastructure Requirement

The Current situation: Globus assumes Hierarchical CA architecture with one top-level CA, also Inter-domain authorization is based on X.509 identity certificates. The process involves both Authentication and Authorization. (Andrew Hanushevsky and Robert Cowles2003)Mapping of user certificates to user accounts is done in Grid Security Infrastructure (GSI). GSI uses proxy credentials to allow for single sign-on and to provide delegated credentials for use by agent and servers, in which Online Credential Retrieval to create and manage proxy certificates in done. And the next development in GSI is to impersonation certificate and restricted delegation certificate.GSI problems: There are thousands of users – thousands of Certs – many of CAs (with different policies) (Andrew Hanushevsky and Robert Cowles2003) to manage under a single system architecture which in itself is a challenging task. Grid-wide user group and roles are needed also in which no grid-wide logging or auditing is done. There is need for anonymous users and protocol to access personal credential for OCR.A Grid security solution should be based on existing standards wherever possible.

GSI Authentication Requirement

1) *Single sign on:* Users must be able to "log on" (authenticate) just once and then have access to any resource in the Grid that they are authorized to use, without further user intervention.
2) *Delegation:* A user must be able to endow to a program the ability to run on that user's behalf, so that the program is able to access the resources on which the user is authorized. The program should (optionally) also be able to further delegate to another program. (Meder *et al.,* 2001)
3) *Integration with various local security solutions:* Each site or resource provider may employ any of a variety of local security solutions, including Kerberos, UNIX security, etc. The Grid security solution must be able to interoperate with these various local solutions. It cannot require wholesale replacement of local security solutions, but rather must allow mapping into the local environment.
4) *User-based trust relationships:* In order for a user to use resources from multiple providers together, the security system must not require each of the resource providers to cooperate or interact with each other in configuring the security environment. In other words, if a user has the right to use sites A and B, the user should be able to use sites A and B together without requiring the security administrators from sites A and B to interact.

GSI Communication Protection Requirement

1) *Flexible message protection:* An application must be able to dynamically configure a service protocol to use various

levels of message protection, including none, just integrity, or integrity plus confidentiality. The choice may be motivated by factors such as sensitivity of the messages, performance requirements, the parties involved in the communication, and the infrastructure over which the message is transiting.

2) *Supports various reliable communication protocols:* While TCP is the dominant, and widely available, reliable communication protocol for the Internet, the security mechanisms must be usable with a wide assortment of other reliable communication protocols. For example, performance requirements may dictate the use of non-TCP protocols for use within specialized environments.
3) *Supports independent data units (IDU):* Some applications require "protection of a generic data unit (such as a file or message) in a way which is independent of the protection of any other data unit and independent of any concurrent contact with designated 'receivers' of the data unit" (Globus grid-proxy-init http://globus.org). For example, streaming media, email, and unreliable UDP datagrams all require this form of protection.

Assurance, Accounting and Audit

1) *Authorization by stakeholders:* Resource owners or stakeholders must be able to control which subjects can access the resource, and under what conditions.
2) *Restricted delegation:* In order to minimize exposure from compromised or misused delegated credentials, it is desirable to have rich support for the restriction of the authorization rights that are delegated.

OCR – Online Credential Retrieval

OCR service defines TLS (SSL) protocol extensions to allow delegation of X.509 Proxy Certificates and secure remote access to private credentials. Its main goal is to avoid drawbacks in personal management of credentials by users (private key protection, mobile/remote access, and need for multiple credentials).Authentication in GSI is based on proxy credentials that proxy credential should consists of proxy certificate and an associated private key, Proxy certificate is an X.509 certificate that is derived from a standard X.509 end entity (EE) (Virtual Smart Card: http://slac.stanford.edu/~abh/vsc) certificate or another proxy certificate and signed with the private key associated with the source certificate and Proxy credential has limited lifetime to limit vulnerability of the EE private key: user create proxy credential once using its private key.

OCR Usage Scenario

The Online Credential Retrieval does perform under the following situations/conditions: (Stephen Farrell 2003)

- When the Credential is initialized
- When the Credential is renewed
- When Transparent Credential is retrieved
- While Adding Delegation to Existing Protocols
- Retrieving Multiple Credentials

OCR Requirements

There are also few requirements of Online Credential Retrieval. The first if the following protocols have be initialized which are Credential Retrieval Protocol, Credential Upload Protocol and Administration Protocol. Second is the Credential Server and at last the Credential Repository, to perform its tasks.

Observations

Today's goal is to know what a credential recovery system is, and how they work and understand the design options, and implications for Security and Usability. The Credential Recovery is the Self-service reset of forgotten passwords using knowledge-based authentication. This service is of types, answering enrolled challenges and probing knowledge shared between system and user. Also this is used infrequently and can be configured to allow a certain number of fails. The main security issue which we face in Online Credential Retrieval are guessing difficulty, observation difficulty and Capture difficulty. The guessing difficulty is an answer space with a uniform distribution and is generally unrealistic. Observation difficulty should be difficult for an attacker to easily retrieve or observe, also answers should not be available from public sources. Observation difficulty will differ for individuals that have different relationships with the user, e.g. family, friends, acquaintances, colleagues or strangers. Capture difficulty covert recording of answers, which means, how many recovery attempts does attacker have to observe in order to launch successful attack? Thus, we are working forward for Online Credential Retrieval which need to be carefully planned and designed.

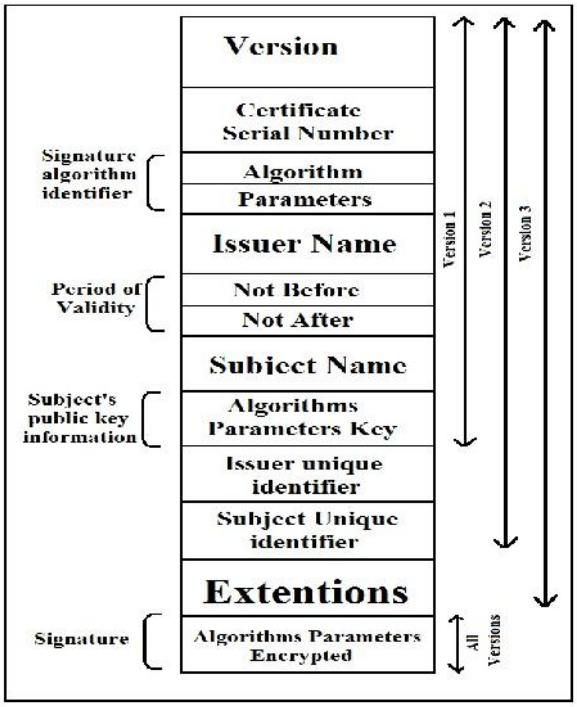

Fig. 1. Overview of a X.509 Certificate

X.509 Certificate

An X.509 certificate binds a name to a public key value. The role of the certificate is to associate a public key with the identity contained in the X.509 certificate. (Tuecke*et al.*,2001; Cooper*et al.*,2001) Certificate X.509 is something that can be used in software to both:

1) Verify the identity of the person, so you can be sure that the person really is who they say they are.
2) Send the person who owns the certificate data is encrypted, that only they will be able to decrypt and read.To be fair, certificates X.509 can be used to make these things more than just people-they are actively used by software applications or computers to do it among themselves as well. (Jackson *et al.*, 2001)

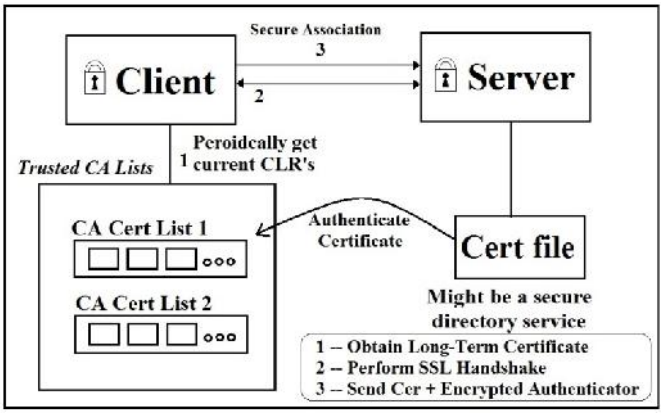

Fig. 2. X.509 + SSL Authentication

X.509 Authentication Overview

The X.509 proxy certificate should comply with some of the requirements that the certificate must be valid (validity date should not be due) also the certificate must have been issued by trusted issuer. Issuer's private key signature must match re-computation done with issuer's known public key. The Certificate Subject proves that it knows private key, and X.509 does not specify how this is to be done also to be noted that the De facto standard is via the SSL algorithm. There are few procedures involved in Authenticating Client with the help of X.509 Certificate (Mary *et al.*, 2002; MyProxy: http://www.ncsa.uiuc.edu/Divisions/ACES/MyProxy) which are as:

- Authenticator must be signed by Certificate's private key. (Authenticator is an MD5 hash of all exchanged handshake bytes)
- Certificate must not be expired.
- Certificate must be signed by a known and trusted CA.
- Client's certificate must not be revoked (I.e., in the CRL).

Security is Tenuous

Previously This Model is predicated on various assumptions as like

- Certificate Authority is trustworthy
- Client was independently authenticated
- Client securely obtain long-term cert
- Client securely maintained private key

This is the most problematic assumption

It is also one that appears to have a solution!

Difficulty in Security

There are also few difficulties in the security of the Model such as secure private keys and users don't mix and also there is no guarantee of good or any password choice. In fact, many users don't want password on their keys. Also there is no guarantee of secure private key location (Butler*et al.*,2001) for e.g., users store keys in network based file systems and hence the private keys are probe to get stolen may get attacked. There is also no guarantee how private key was handled for e.g., users copy/e-mail keys to remote machines & leave them. Even there are several ways by which your private key may get leaked out and you may get exploited. Leaked private key is like your stolen passport and stolen credit card. It may even get exposed from a memory dump. User managed keys should not be trusted.

Possible Solution

The possible solution for this problem may be to protect Long-Term Certificate by the use of proxy-certs to limit key exposure damage. The command used in Globus toolkit for the same is "Grid-proxy-init". The security can also be achieved to an extend by making X.509 certificate handling convenient by limiting avenues for user error for e.g. SACRED, MyProxy. (MyProxy: http://www.ncsa.uiuc.edu/Divisions/ACES/MyProxy/)It can be made easier to protect Identity Certificate with the help of Kerberos Certifying Authority (KCA), Smart Cards and Virtual Smart Cards (VSC). (Just 2005; Grid Giovanni *et al.*, 2004)

Proposed Model

This proposed Model is based on Virtual Smart Card in which user registers with a known organization & typically gets a Kerberos account. Then user requests the VSC server, only once, to obtain a long-lived certificate for them. After obtaining the long-lived certificate the user login via Kerberos (or other) and get proxy certificate signed by long-term certificate. (KCA/x.509: http://www.nsf-middleware.org/documentation/NMI-R2/0/KX509KCA/; Ravi Sandhu *et al.*, 2002) The user will then use VSC proxy certificate as you would a normal proxy certificate.

Advantage: User can obtain a fresh proxy certificate from anywhere in the world & never see the private key (private key never leaves server). Server may require key encryption. As in case of Smart Card the user have to carry electronic or magnetic smart card

Dis-Advantage: Breach of the VSC server exposes any unencrypted certs to compromisecolumns.

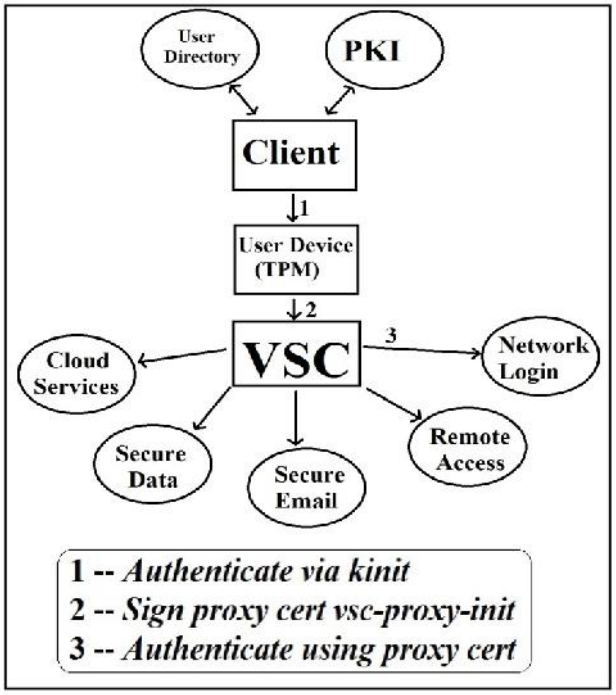

Fig. 3. Proposed Model for X.509 certificate issuing via VCS

In the above figure we can illustrate the issuing service of X.509 certificate from issuer with the help of VSC (Yuri Demchenko 2001), previously we have already mentioned the outcomes of this Model. This complete process is done in three main steps, as shown in Fig. 3.

a) The Authentication of user to ensure that the Certifying Authority requesting for authentication is not fake, which is done using the command '*kinit*'
b) Then proxy certificate is signed using virtual smart card to further reply to the client machine via '*vsc-proxy-init*'
c) Finally the client machine sends the request to Server to authenticate the user request and to proceed further, where so ever necessary.

Practically this model acts as a link between the user data store, credentialing authority (PKI) (Nosseir*et al.*,2005; Intercede, "Windows 8 virtual smart card management," http://www.intercede.com/, 2013), devices (TPM-equipped) and the user. The sequence below is a typical example of initial provisioning:

1) The user is already using a device equipped with an embedded TPM, but is logging on to the domain with a username and password.
2) IDMS instructs Client to issue a VSC to the user.
3) Client generates a 'job' to be collected
4) The next time the user logs onto their device they are notified that they have a VSC to collect
5) The user decides to collect the VSC now and is guided through a simple self-service app
6) During the self-service process Client communicates securely with the TPM to create a VSC
7) Client prompts the user to choose and verify a PIN for the VSC
8) Client then generates keys on the VSC via the cryptographic functions build into Windows 8 (no middleware is required)
9) Private keys remain protected by the TPM and public keys are formed into a certificate request
10) Client sends the certificate request to the certificate authority (CA), e.g. the certificate services capability built into the Windows Server
11) Client retrieves the certificates from the CA
12) Client writes the certificates to the VSC
13) The process is complete and the user can now use their VSC in the same manner as a physical smart card.

B. Advances in this Model

There are few Advances in this proposed model. This Model is simple as initial certificate request is trivial. There is no fear to get your private keys exposed, as they never expose and can also further be encrypted be the user. The Model has the most important advantage as the user can get Proxy certificate anywhere in the world, there is no need to copy public/ private keys. This Model has zero downtime which means it can provide always-on services, perhaps proxy certificate validation is also done. It can provide stronger security guarantee as signed certificate is as secure as institution's account.

Conclusion

From the hereby study we can conclude that the X.509 Security is inherently difficult to protect and need some kind of key service for a practical solution, which means more simple user lives and reduction in security lapses.The Virtual Smart Cards are even more effective as comparative to others as they are simple, relatively transparent and more secure. It provides a path to more stringent security to build more secure Physical smart cards. The study also resulted that the future developments will also promote a congenial grid security environment!

Acknowledgment

Several people have been instrumental in the completion of this work. First of all, I want to thank my advisor Er. Anshuman Saurabh for his guidance, insight, patience, and support throughout my thesis work. Thank you also for helping me find such an interesting and challenging topic as this, and helping me see what research is all about. I would like to thank Gaurav Kumar and Ankur Chaudhary for suggesting me through my work at Subharti University and patiently listening and advising me on my ideas for this research.

REFERENCES

Andrew Hanushevsky and Robert Cowles, "Mechanism to secure X.509 Grid Certificates," Stanford Linear Accelerator Center, Stanford, CA 94025, United States, March 2003

Butler R., D. Engert, K.Jackson, M.Lorch and V.Welch, "Multiple Credentials - Scenarios and Requirements," Internet Draft September 2001

Cooper D., "Internet X.509 PKI Certificate and Certificate Revocation List," Network Working Group February, 2001

Globus grid-proxy-init http://globus.org/

Grid Giovanni, Aloisio, Euro Blasi, Massimo Cafaro, Italo Epicoco, San Fiore and Maria Mirto, "Dynamic Grid Catalog Information Service," CACT/ISUFI, University of Lecce, 73100 Italy, 2004

GSI Henri Mikkonen and Mika Silander, "Federated Identity Management for Grids," Helsinki Institute of Physics, PL 9250, 02015 TKK, Finland, IEEE 2006

Intercede, "Windows 8 virtual smart card management," http://www.intercede.com/ 2013

Jackson K., S. Tuecke and D. Engert, "TLS Delegation Protocol," Internet Draft, July, 2001

Just M., "Designing Authentication Systems with Challenge Questions," In L. Faith Cranor & S. Garfinkel, Chapter 8, 2005.

KCA/x.509: http://www.nsf-middleware.org/documentation/NMI-R2/0/KX509KCA/

Mary R., Doug Olson, Robert Cowles, Shwan Mullen and Mike Helm, "CA-based Trust Model for Grid Authentication and Identity Delegation," Grid Certificate Policy WG, October 2002

Meder S., V. Wech, U.Chicago, S. Tuecke, D. Engert, "GSS-API Extensions," GSI-WG, February, 2001

MyProxy: http://www.ncsa.uiuc.edu/Divisions/ACES/MyProxy/

Nosseir A., R. Connor, and M. Dunlop, "Internet Authentication Based on Personal History – A Feasibility Test Proceedings of Customer Focused Mobile Services Workshop," at WWW2005, 2005.

Ravi Sandhu, Mihir Bellare and Ravi Goswami, "Virtual Smartcards versus Virtual Soft Tokens," 1st Annual PKI Research Workshop—Proceedings, University of California, 2002

Stephen Farrell, "Securely Available Credentials Protocol", Baltimore Technologies, January 2003.

Tuecke S., D. Engert and M. Thompson, "Internet X.509 PKI Impersonation Certificate Profile," Internet Draft February, 2001

Virtual Smart Card: http://slac.stanford.edu/~abh/vsc

Yuri Demchenko, " Grid Security Infrastructure: Overview and problems," PKI-COORD Meeting, Amsterdam, November 2001

****