ISSN 2320 - 2602

Volume 4 No.11, November 2015

International Journal of Advances in Computer Science and Technology

Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst014112015.pdf

Analysis on Certificate Validation mechanisms in Public Key Infrastructure

T. Sujitha[1], Dr. T. Hemalatha[2]

[1]PSNA College of Engineering and Technology, Dindigul, India, sujithathangavelu14@gmail.com

[2]PSNA College of Engineering and Technology, Dindigul, India, hemashek@yahoo.com

ABSTRACT

A Public Key Infrastructure (PKI) facilitates security services in an internet application and enables the identification and distribution of public encryption keys. It ensures users to securely exchange data over networks. Any form of sensitive data exchanged over the Internet depends upon PKI for security. The purpose of a PKI is to provide secure, convenient and efficient acquisition of public key. It helps to maintain a trustworthy environment in key and certificate management. In PKI the certificate validation is done in two ways: (1) Certificate Revocation List (CRL) and (2) Online Certificate Status Protocol (OCSP). The CRL maintains a list of revoked certificates that are issued and maintained by Certificate Authority (CA) in offline. But the OCSP enables real – time revocation status check in online for huge volume of operation. The mechanism to check the revoked certificates may occur for several reasons and to deny the unauthorized access. The revoked certificate is no longer trusted by the end – entities. The investigation on Certificate Validation Mechanisms is done to identify the drawbacks in validation mechanisms and to enhance such validation mechanisms in such a way that it is in more efficient and suitable to the latest computing infrastructures.

Key words: Certificate Authority, Certificate Revocation List, Online Certificate Status Protocol, Public Key Infrastructure, Revoked Certificate.

1. INTRODUCTION

Public Key Infrastructure (PKI) is a popular authentication approach used by governments, small business and enterprise with the intent of improving security by maintaining the confidentiality and integrity. It is a system that is required to provide public – key encryption and digital signature services to all PKI enabled Protocols and Applications. Digital certificate is the heart of PKI which confirm the identity of the certificate subject. It enables management of keys and certificates to enhance the performance metrics and thereby increase the efficiency by deploying large scale PKI.

1.1 Components of Public Key Infrastructure

1. **Certificate Authority (CA)** acts as root of trust and issuer of the corresponding certificate and CRL. It supports wide variety of administrative functions. Normally, a CA checks with a Registration Authority (RA) to verify the details provided by the requestor of a digital certificate. If the Registration Authority verifies the requestor information, then the CA can issue a certificate. [12]

2. **Registration Authority (RA)** often called as a Subordinate. It is a trusted system that runs services to verify the validity of certificates that has been issued by a root CA. It issues certificates to particularly identified and authenticated individuals permitted by the CA. The services provided by RA can be either physically separate or combined with a CA. [12]

3. **CRL Issuer** is an interface between the CA and Certificate Repository. It collects the CRL from the corresponding CA which is a trusted party in PKI, after a formal registration.

4. **Certificate Repository** is a database of PKI, saves certificate requests of issued and revoked certificates from the RA or CA. The commonly used repository service for certificate storage is a Lightweight Directory Access Protocol (LDAP) server. The CA will store certificates to the repository and the clients retrieve the certificates from the repository using an LDAP based user application access.

5. **Certificate Store** saves issued certificates. It also accounts the pending or revoked certificate requests from the local computer.

6. **Key Archival Server** saves encrypted private keys in a certificate database in case of any failure for recovery purposes i.e., Certificate Database is lost.

1.2 Drawbacks of PKI

The scalability of Public Key Infrastructure (PKI) could be significantly limited by the certificate revocation mechanism. This is evidenced by MITRE report [7] on the PKI Federal Government and Corestreet report on certificate validation in PKI [18]. These reports focused on analysis of cost and time in certificate revocation when CRL is used to periodically circulate revocation information to the end entities via certificate repositories.

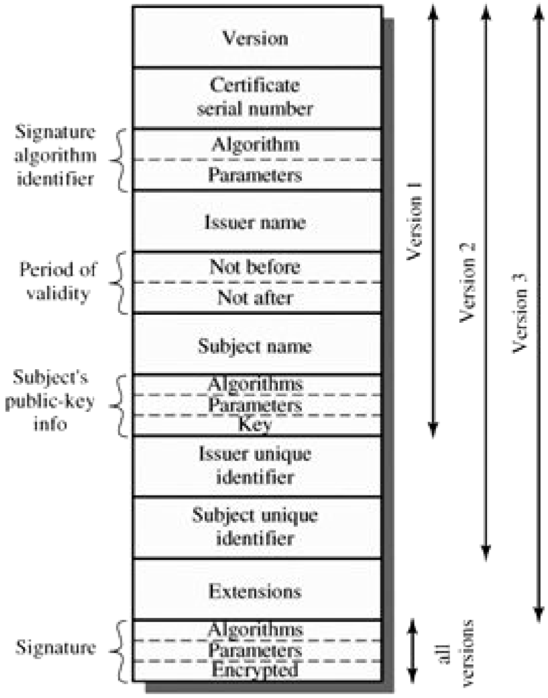

Figure 1: Structure of Certificate [10]

The Figure 1 is the structure of certificate for three different versions of certificate standards. The version 1 is considered as the default, the version 2 is used in most case and the version 3 has the extensions. It contains the certificate serial number, public – key info, signature algorithm and period of validity.

2. CERTIFICATE VALIDATION MECHANISMS

The Certificate Validation in PKI is processed in two ways such as CRL and OCSP. In certificate validation, when any certificate is issued, it has a validity period that is defined by the CA. Usually the validity period is one or two years. If the certificate has past that period or expired, then the authentication should fail. The brief description about the two validation approaches are discussed in detail.

2.1 Certificate Revocation List

The Certificate Revocation List (CRL) is a list which holds the serial numbers for certificates that had been revoked for various reasons. It is that the entities of the certificates present in the CRL should not be trusted. The CRL is issued by the trusted CA and it is stored in certificate repository via CRL issuer. The CRL issuer generates and publishes the certificate in defined intervals.

For example, if the private key associated with a certificate is lost, then any authentication using that certificate should be denied. This is done by adding the serial number of a particular certificate to the CRL. Similarly, the certificate of a user or organization is included in the CRL for various reasons. When their certificates are replaced, the expired certificates have to be marked as "untrustworthy".

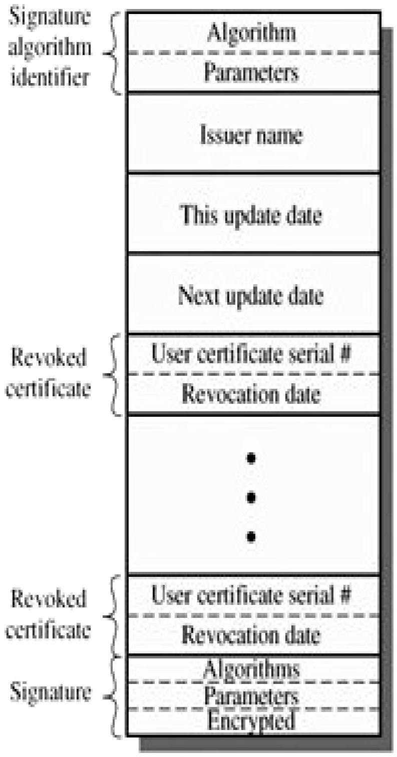

Figure 2: Structure of CRL [10]

The Figure 2 is the structure of CRL which has the signature algorithm, issuer name of the particular certificate and the revoked certificates. The 'This update' is a date on which the list is created. The 'next update' is a date on which the CRL will be issued.

Advantages:

- In CRL, certificates are validated in offline.
- It prevents spoofing or denial-of-services attack.

Disadvantages:

- CRL's are not updated frequently i.e., at defined interval of time.
- The CRL list grows to unmanageable sizes

Use of CRL File:

- During the validation process, the browser will choose a way to check for revocation; if a CRL is preferred, it will download the CRL file from an URL specified by the certificate, and does further verification.
- If a CA indicates that a server's particular certificate was revoked, the user will be stopped from accessing the unauthorised sites.

2.2 Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) allows a PKI-enabled application to contact an OCSP server (also called an *OCSP responder*) to check for revocation status in real time. [11]

In OCSP the client approach a web service running at the specified URL via browser and asks the service whether the requested certificate has been revoked. The response is signed back to prevent tampering. OCSP has the primary benefit of requiring minimum network bandwidth, enabling near real-time status checks for high - volume operations [9]. It is not an effective technique to alleviate against HTTPS server private key.

Advantage:

- In OCSP, the certificates are validated in online.
- It solves the size problem in the CRL approach
- The certificates are verified without consuming more memory and computation resource.
- OCSP is networks friendly compared to CRL.

Disadvantage:

- It requires always online to connect with the server thereby the server may get overloaded during peak hours.
- The OCSP Responder creates bottleneck when the requests are processed in queue.
- There is possibility of single point failure in OSCP responder.

The below Figure 3 is the architecture of OCSP, here the relying parties request for the status of the certificate to back – end PKI by OCSP request, the OCSP services get the result from the back – end PKI and return it to the concern parties via OCSP response

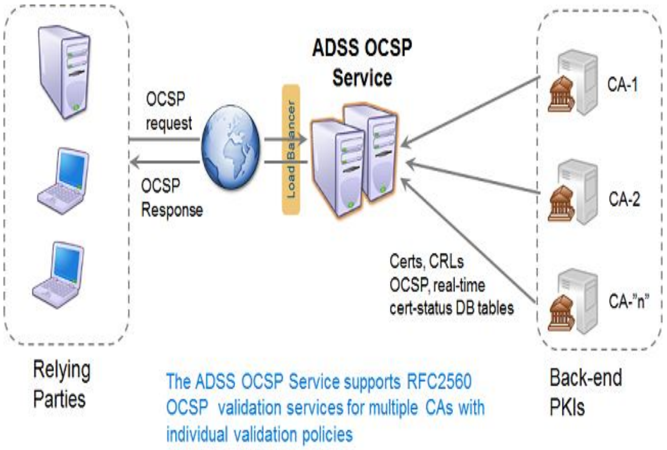
Relying Parties
OCSP request
OCSP Response
Load Balancer
ADSS OCSP Service
CA-1
CA-2
CA-"n"
Certs, CRLs OCSP, real-time cert-status DB tables
Back-end PKIs
The ADSS OCSP Service supports RFC2560 OCSP validation services for multiple CAs with individual validation policies

Figure 3: OCSP Architecture [16]

3. Extended Validation

An Extended Validation (EV) certificate is known as a public key certificate that will be issued after additional identity details has been verified. Usually HTTPS websites have a public key certificate, which is an electronic document proving ownership of a public key. It is used to decrypt information being stored in the certificate. [13]

When the concern client tries to connect to an HTTPS website with an EV certificate, the browser will provides some additional information to the address bar. The Figure 4 shows an Extended Validation certificate for five major browsers.

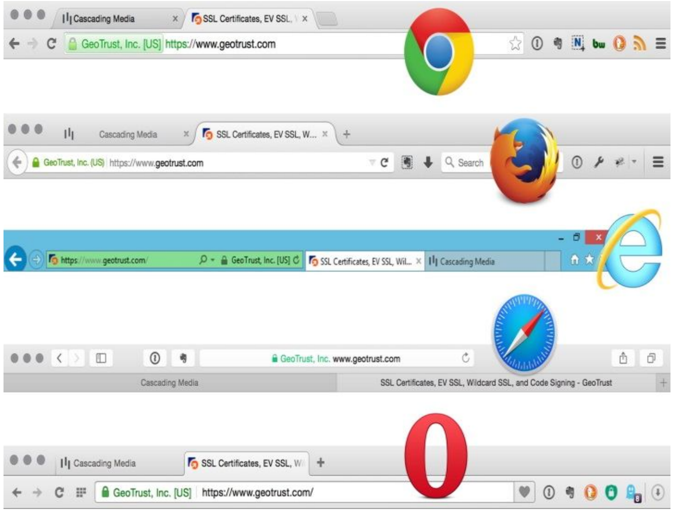
Cascading Media
SSL Certificates, EV SSL
GeoTrust, Inc. [US] https://www.geotrust.com
Search
https://www.geotrust.com/
GeoTrust, Inc. www.geotrust.com
SSL Certificates, EV SSL, Wildcard SSL, and Code Signing - GeoTrust
https://www.geotrust.com/

Figure 4: Five major browsers with extended validation [13]

3.1 CRLs and Revoked Certificates

The Clients can verify the PKI Certificates, so that they can warn users about trusting a website. [14] CA's are required to keep track of the SSL Certificates are revoked. After the CA revokes an SSL Certificate, the CA takes the serial number of the certificate and adds it to their CRL. The URL to the CA's Certificate Revocation List is contained in each SSL Certificate in the CRL Distribution Points field. [14]

To check the revocation status of an SSL Certificate, the client connects to the URLs and downloads the recent CRLs from the Issuer. Then, the client searches throughout the CRL for the serial number of the certificate to make sure that it hasn't been revoked. [14]

4. ANALYSIS OF THE EXISTING SYSTEM

In the analysis of the Certificate validation mechanism, we have refered the Websense ThreatSeeker Intelligence Cloud, Who had made a complete successful survey on the CRL file data. They had reported that CRLs are accessed about 200,000 times within a day Websense ThreatSeeker Intelligence Cloud and they managed to gather about 10,000 access records in the course of one hour from which interesting data are found. [9]

The total URLs which requested a CRL file is 9066. From those 9066 request for URLs only 819 are unique URLs, which mean that certain URLs are accessed numerous times.

4.1 Size of CRL File

Each CRL file has its own size depending upon number of revoked certificate in it. From the report given by the WebSeeker, it is shown that the maximum file size in megabytes and the minimum file size are in few bytes.

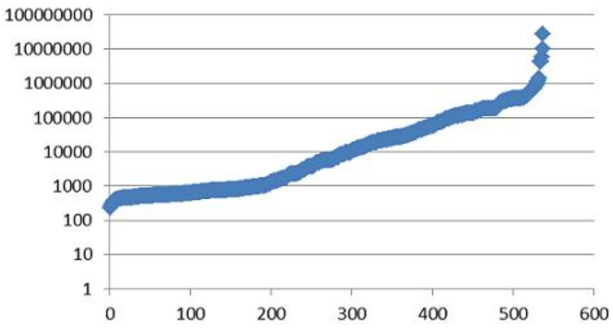

Figure 5: Growth in CRL File size [9]

The above Figure 5 shows that among the considered 600 CRL files, only 200 files are below 1000 bytes, which clearly indicates that most CRL file is large in size. [9]

4.2 Certificate Record in CRL

The number of records in CRL depends on the list of revoked certificates. Each CRL file is issued by a CA. A single CA server can issue many CRLs as it is not limited. Sometimes we may notice that, most of the issued CRL files are from the same CA.

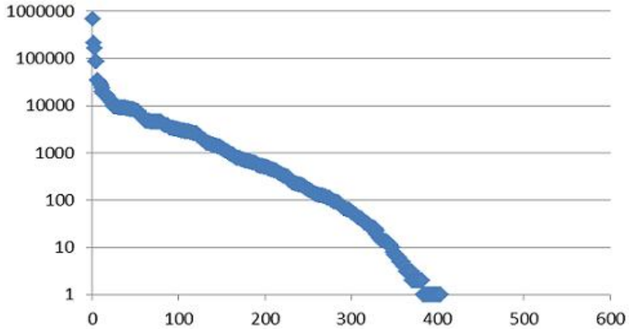

Figure 6: Increase in record in CRL File [9]

The Figure 6 shows that the number of revoked i.e., untrusted certificate will increase the CRL records to billions.

4.3 Signature Algorithm used in CRL

Each CRL file must select its own algorithm for hash and encryption. The different types of algorithms are:

- sha1 With RSA encryption
- sha256 With RSA encryption
- sha512 With RSA encryption
- md5 With RSA encryption

From these algorithm the most commonly used is "sha1WithRSAencryption".

4.4 Reason for Certificate Revocation

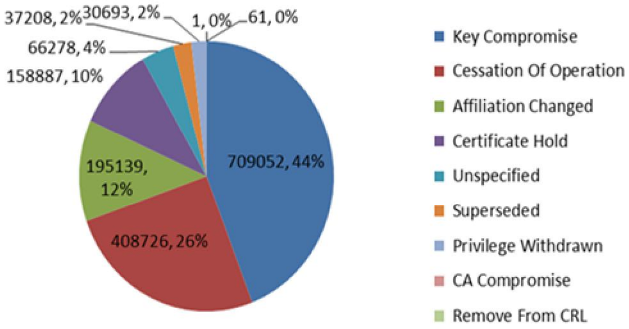

Figure 7: Reasons for Certificate Revocations [9]

From Figure 7, it clearly shows that the reason for the majority of certificates (44%) is revoked due to the fact of "key compromise" which is considered as quite serious problem in this method.

1. **Key Compromise:** When a user's private key is lost or stolen for any other illegal purpose has to be compromised
2. **Cessation of Operation:** When the certificate subject no longer need the certificate further.
3. **Affiliation Changed:** When the certificate subject does not belong the specified organization or changes to other organization.
4. **Certificate Hold:** When the certificate subject temporarily wants to revoke the current certificate.
5. **Unspecified:** When the certificate subject has no reason for the certificate to be revoked then it is unspecified.
6. **Superseded:** When a new certificate is replacing the existing certificate.
7. **CA Compromise:** When a CA's private key is stolen for some illegal access then the certificate of CA itself has to be compromised

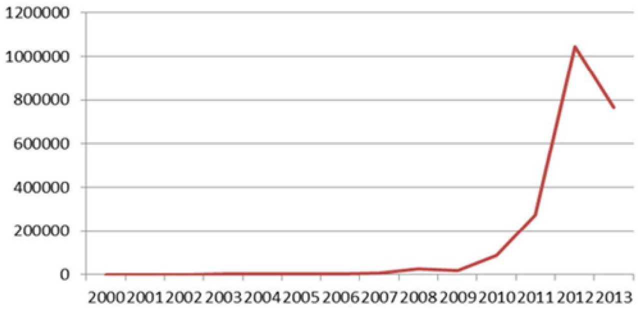

Figure 8: Increasing no. of. Revoked Certificate [9]

From Figure 8, a guess can be made that the number of revoked certificate will be growing enormously in the upcoming years.

Each revoked certificate record specifies the validity date. From the specified date, we could know the recent problem in certificate revocation, and the predictions are to be done for the certificate security issues.

5. CONCLUSION

Worldwide, governments and industries are deploying large-scale, public key infrastructure with the intent of improving security and increasing efficiency. The overall PKI performance has an impact on significant certificate validation mechanism. The two validation approaches CRL and OCSP has its own method to verify the validity of the certificate. But the problem is that to manage the growing size of the revoked list and the cost deployment during the mechanism. Thus the secure Certificate Verification provides the flexibility required to achieve high availability without incurring the significant cost and time in the traditional approach.

REFERENCES

1. Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, **"Identity-Based Encryption with Outsourced Revocation in Cloud Computing",** *IEEE Transactions on Computers***,** VOL. 64, NO. 2, February 2015, pp. 425-437.
2. Devendra Dahiphale, Rutvik Karve, Athanasios V. Vasilakos, Huan Liu, Zhiwei Yu, Amit Chhajer, Jianmin Wang, and Chaokun Wang, **"An Advanced MapReduce: Cloud MapReduce, Enhancements and Applications",** *IEEE Transactions On Network and Service Management***,** VOL. 11, NO. 1, March 2014, pp. 101-115.
3. FAN Yuanquan, WU Weiguo, XU Yunlong, CHEN Heng, **"Improving MapReduce Performance by Balancing Skewed Loads",** *IEEE Transactions on Network Technology and Applications***,** August 2014, pp. 85-108.
4. Tansel Dokeroglu, Serkan Ozal, Murat Ali Bayir, Muhammet Serkan Cinar and Ahmet Cosar, **"Improving the performance of Hadoop Hive by sharing scan and computation tasks",** *Journal of Cloud Computing: Advances, Systems and Applications (Springer),* 3:12, 2014.
5. Qi Zhang, Student Member, Mohamed Faten Zhani, Member, Yuke Yang, Raouf Boutaba, Fellow, and Bernard Wong, **" PRISM: Fine-Grained Resource-Aware Scheduling for MapReduc"**, *IEEE Transactions On Cloud Computing*, Vol. 3, No. 2, April/June 2015, pp.182-194.
6. [6] Jong Hyuk Choi, Sang Seok Lim, and Kurt D. Zeilenga, **"A New On-line Certificate Validation Method using LDAP Component Matching Technology"**, *IEEE Workshop on Information Assurance and Security*, 2005.
7. MITRE Corporation, **"Public key infrastructure final report."** http://csrc.nist.gov/pki/documents/mitre.ps, 1994.
8. Jong Hyuk Choi, Sang Seok Lim, and Kurt D. Zeilenga, **"A New On-line Certificate Validation Method using LDAP Component Matching Technology",** IEEE Workshop on Information Assurance and Security, 2005
9. http://community.websense.com/blogs/securitylabs/archive/2013/07/11/digging-into-certificate-revocation-lists.aspx
10. http://flylib.com/books/en/3.190.1.121/1/
11. http://windowsitpro.com/security/ways-check-revocation-status-certificates
12. http://tutorials.section6.net/home/digital-certificates-and-pki
13. https://cascadingmedia.com/insites/2015/01/https-fundamentals.html
14. https://www.digicert.com/util/utility-test-ocsp-and-crl-access-from-a-server.htm
15. https://www.thales-esecurity.com/solutions/by-technology-focus/pki-and-digital-certificates
16. https://www.grc.com/revocation/ocsp-must-staple.htm
17. https://msdn.microsoft.com/enus/library/windows/desktop/bb427432(v=vs.85).aspx
18. http://www.hotfrog.in/business/actividentity/pki-digital-certificate-validation-corestreet-software-268187
19. http://www.manjrasoft.com/products.html