An Agent Subscription-based Model for CRLs Validation

Sekpon Juntapremjitt, Somchart Fugkeaw, and Piyawit Manpanpanich

Abstract— **In the PKI system, digital certificates are used to authenticate entities. The information about the certificate status is necessary by the relying parties for the verification. However, the available revocation mechanisms such as CRL and OCSP have major drawbacks in terms of untimeliness and expensive computation cost respectively. In this paper, we propose a novel CRL verification model driven the immediate CRL enforcement in distributed certificate subscription environment. We introduce the agent subscription based approach to support both "push" model for the relying parties that require immediate CRLs enforcement and "pull" model to support the groups that do not require such an immediate update.. The design offers the flexible scheme for relying parties as well as optimizes the CRLs delivery cost. Besides we also introduce the signature broadcast technique to deliver the up-to-date CRLs information from the CA to relying parities with a small size. At the end, we present the results of a pilot implementation based on the proposed design.**

I. Introduction

Reliability of the PKI systems that issue certificates and keys to the number of users is normally handled by the certificate management system implemented by the certification authority (CA) system. The status of the certificate may be either valid or invalid. A revocation system operated by the CA is employed to control the certificates which are compromised or revocation request by the relying parties. This mechanism is very crucial for the applications that download the certificate status before granting the operation to any transactions.

A. Certificate Revocation Model

CRLs

The most common method is to use the Certificate Revocation List (CRL) issued and signed by the CA. CRL has been standardized by the X.509 standard [2], it is supported by most of PKI systems. The CRL generally contains the list of invalid certificates and are published in the open directory periodically upon the change of CRLs by the CA.

Delta CRLs

A Delta CRL is a special CRL containing a list certificates that have been revoked since the last complete CRL (base CRL) was issued. A Delta CRL is supposed to be much smaller than the corresponding full CRL and thus it can be retrieved more often by the relying parties with less bandwidth consumption. The concept of Delta CRL is part of the X.509 standard.

OCSP

OCSP is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 [3] and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders*[8].

Even though OCSP provides a good degree of timeliness but it is non-scalable since all OCSP queries need to be signed every time by CA when there is a change on certificate status.

We try to overcome the limitations of the traditional CRLs and OCSP mechanisms by minimizing the CRLs size and enabling immediate CRLs enforcement. In this paper, we present an approach of the certificate revocation management system by employing agent subscription and signature broadcasting technique.

At a core, the agent subscription-based service works with the certificate and CRL repository to function as a mediator between the source of certificate and CRL and the relying parties. The agent service consists of push and pull model to support the different need of user's real-time update(Push Agent) and traditional way of CRLs retrieval by other applications (Pull model), the agent service will be a reliable source for ultimate verification as well.

In summary, our contributions are summarized as followings:

1) The proposed certificate revocation management system empowers the efficient CRL update and publication in both performance and freshness of the CRLs.
2) The signature broadcasting is a proven CRLs information delivery to relying parties with a better performance and reliability.
3) The system that supports the certificate and CRLs publication for multiple CAs.

S. Juntapremjitt Whitehat Certified Co.,Ltd. Bangkok, 10310, Thailand (e-mail: sekpon@whitehatpro.com)
S. Fugkeaw Thai Digital ID Co., Ltd. Bangkok, 10500, Thailand (e-mail: somchart@thaidigitalid.com)
P. Manpanpanich Thai Digital ID Co., Ltd. Bangkok, 10500, Thailand(e-mail: piyawit@thaidigitalid.com)

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

II. Related Works

There are several attempts to address the CRL validation scheme. Most works concentrated on the CRLs updating approach since it's the simplest way for certification revocation checking and widely used by many applications. The techniques for minimizing the CRLs size have been proposed e.g., Delta CRLs [1] and Over-issued CRL [4]. Even though those techniques can solve the CRLs optimization and make the CRLs updating process perform more faster, the enforcement of freshest CRLs to relying parties does not be solved.

Recently Datniel Kouril et.al. [5] proposed the approach of CRL Push Delivery for revocation information management in the Grid systems. The push model for CRL distribution is tactically favor for relying parties that do not require to poll for CRLs checking at CA. Rather, the proposed CRL distribution service that collects revocation data from one or more CAs and distributed to the clients. The model offers a flexible scheme for CRLs updating and delivery in nearly real-time fashion. However, the push model requires all relying parties to subscribe in order to receive the information from the dedicated service understandably. This can be done in the Grid since it is more practical in managing the resources in the grid. The real world distributed systems where each party is autonomous and resides on the heterogeneous domains require more scalable scheme. Also, since the push method relies on the notification infrastructure, the huge stream of CRLs update renders high communication cost.

In [6], the authors proposed a certificate revocation model based on certificate space partitioning. The certificate is divided into several partitions; each partition contains the status of a set of certificates. When a certificate contained in a partition changes status (e.g., gets revoked), the current version of that partition is expired and a new version reflecting the new certificate status is created by the CA. The proposed method reduces the CA to directory communication costs significantly. Nevertheless, the approach does not guarantee the real-time validation if the application does not check the partition field in the certificate extension.

In fact, both the OCSP and CRL retrieval is a Pull-based revocation information distribution, where the relying parties are responsible for checking if it is valid or if a new piece of revocation information has been issued [7].

In this paper, we present a new design of CRLs information delivery, based on an immediate enforcement model, which ensures that they are delivered to the end systems instantly after their publishing by the CA. With the design scheme of signature broadcasting, the users always get the fresh CRLs in case that they need the real-time update of the CRLs for the validation

III. A Framework of the Proposed Model

A. Certificate Revocation Model

The proposal intends to propose the desired feature of the certificate revocation management system rendering the efficient CRL delivery mechanism and optimized network cost. Figure 1 illustrates our proposed framework.

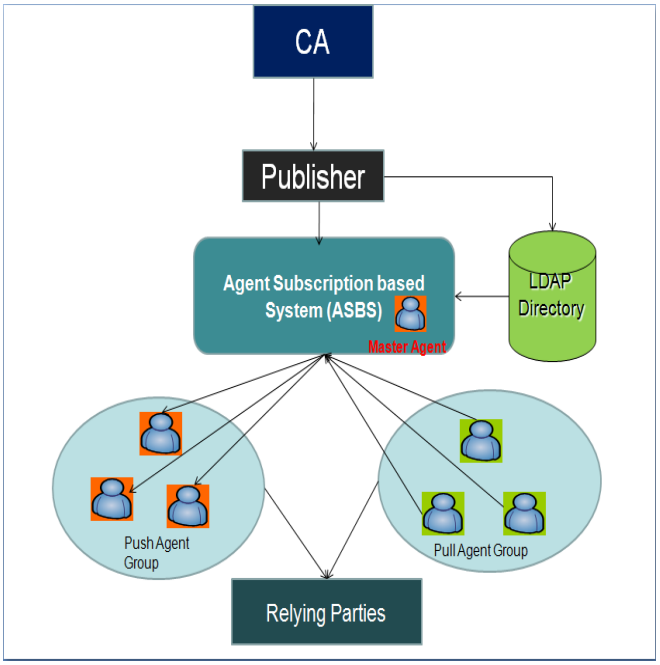

Fig. 1. Proposed ASBS Framework

The core elements consist of:

1) LDAP Directory is a repository used to store the certificate and CRLs issued and published by CA.
2) Publisher is a system component developed to integrate with CA system by invoking all certificates and CRLs issued by CA and publishing to the directory and Agent Subscription-based system.
3) Agent Subscription-based System(ASBS) is a proposed component designed to work with the Publisher and CA repository system. In ASBS, there is a Master Agent to be responsible for (1) monitoring the publishing CRLs information to the relying parties and (2) constructing the signature for broadcasting the CRLs to other agents. All CRLs are signed by the trusted agent service which is authorized by the CA. There are 3 types of agents:
    1. Master Agent
       It is an agent that resides in the ASBS engine and liaises with the other two types of agent by communicating the publishing command and controlling for the concurrent process of CRLs request.
    2. Pull Agent
       It is an agent that is responsible for checking the CRLs and pulling the Delta CRLs in a certain period of time.
    3. Push Agent
       It is an agent supporting real-time update of CRLs from the ASBS. In ASBS, the system

B. Signature-based Broadcast

We use the delta CRLs to be a part of signature which is defined as <time, delta CRL, push agents registered>.This is signed by the CA and compressed. If there is any update on master CRL it will be automatically generate the subscription signature and publish to all registered push

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

agent. Therefore, push agents always get the freshest CRLs for the active use of its own relying party. For the pull agent, we can set the grace period for CRLs publication which is a regular manner done by typical CA software.

C. CRLs Update

As we use the Delta CRL update scheme, only the incremental changes of the base CRL is invoked to the agents and relying parties. Technically, the base CRL is published from the CA and stored in the directory and ASBS. In ASBS, Master agent computes and Delta CRL and propagate to the subscribed agents and those agents retain the sufficient CRLs as a source of CRL validation by the applications or relying parties.

IV. Evaluation

We set up the experiment to evaluate the functionality and performance of our proposed system. We established the CA system by using the Open CA running on Linux platform. The publisher and component in ASBS are developed by java programming. We use MySQL as a repository to store the series of base CRLs and Delta CRLs issued by the CA.

For the functionality test, we compare the publication result of certificates and CRLs generated by our Open CA system including publisher and ASBS and Microsoft CA. In the test scenarios, 50 certificates were issued from both CA systems and CRLs lifetime is set to 3 days and it is updated every 1 hour.

Based on the functional test, the Open CA with our developed publisher can issue and publish certificates and CRLs as correctly as Microsoft CA does. We also tested functional operations of the certificate management e.g., issuance, suspension, and revocation. The results are compared by checking CRLs contents and certificate status in one by one fashion from both CA systems. This confirms that our proposed elements working with Open CA can support the normal certificate management functions including CRLs publication.

For the performance test, we classify applications into two groups: normal CRLs validation and Real-time CRLs validation.

The applications require that traditional CRLs checking is registered and connected to ASBS and the pull agent will be assigned to each application individually to perform pull-based checking. Hench, the CRLs lifetime and update frequency are automatically applied to this group and Pull Agents handle for CRLs delivery to applications.

For the applications requiring real-time CRLs checking, they need to be subscribed and connected to ASBS and push agent will be assigned to this particular group of applications. In this group, whenever there is any update upon the certificate status, CRLs will be published in realtime by the publisher to ASBS and Push Agent will be notified by the Master Agent in ASBS and carry the deltaCRLs to the respective applications.

The reason that we let the application be connected to ASBS rather than to be directly connected to LDAP directory is because we need agent systems to perform the delta CRLs computation and dynamic scheduling.

In this paper, we perform the test between the applications in the pull agent group and compare with the traditional CRLs checking.

We initially use our current ePayment application to work with both our CA environment and Microsoft CA and we observe the time used for CRLs checking.

TABLE I
Comparing CRL update between Open CA with ASBS and Microsoft CA

	CRL Update Period (1-5)				
	1	2	3	4	5
Update time of Open CA with ASBS (seconds)	0.22	0.24	0.28	0.32	0.36
Update time of Microsoft CA (seconds)	0.62	0.65	0.69	0.74	0.78

The result shows that our proposed systems provides less time of CRL update. This is because only delta CRLs is enforced to the application and pull agents conducts the update function with the subscribes entities in a dynamic and

For the realtime CRLs update test, we simulate an secure application called SeCrypt to do sign and encrypt files. This application is subscribed to ASBS and required real-time update of CRLs.

Empirically, the application can validate the CRLs in a real-time manner as Push agent automatically updates the Delta CRLs to application whenever there is an update on certificate status. For this kind of test, we still need to perform a test with more applications with a lot of certificate management operations.

V. Conclusion and Future Works

This paper illustrates the technique for CRLs validation by proposing push and pull validation scheme based on the agents system. The approach focuses on the support of minimizing the size of CRLs for CRL enforcement as well as the real-time CRL checking. We propose a mediator called Publisher to support a flexible scheme of certificate and CRL publication. Delta CRLs update model is applied to provide a better performance of CRL update and Agents concept is employed to provide a dynamic management of CRLs delivery and application subscription. This yields the significant improvement and scalability to work with any PKI-enabled applications.

The test result reveals the potential extension of our

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

approach.

For future work, there are two aspects the proposed system needs to be conducted. First, the detailed analysis of scheduling and Delta CRLs size minimization are very interesting to work on because these systems provide more advanced network monitoring and update performance. We will investigate more advanced techniques for over-issued CRLs and data compress algorithm to improve the performance of ASBS when facing more complexity in terms of number of applications connected, CRLs size, and network traffic.

Another aspect is to perform a full test with real environment including multi-applications and multi-users. The system could be also tested with dynamic scenarios and we will collect the feedback from application users for further improvement.

REFERENCES

[1] D A. Cooper, A More Efficient Use of delta-CRLs, International Symposium on Security and Privacy (S&P) 2000, Berkeley California, USA, May 2000

[2] RFC 2459 Standard: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999

[3] RFC 2560 Standard: Internet X.509 Public Key Infrastructure Online Certificate Status Protocol - OCSP, June 1999

[4] J. Zhao, S. P. Tan, An Improved Over-issued CRLs Method, Second International Conference on Innovative Computing, Information and Control (ICICIC 2007), Kumamoto Japan, September 2007

[5] KOUŘIL, Daniel - MATYSKA, Luděk - PROCHÁZKA, Michal. Using CRL Push Delivery for Efficient Certificate Revocation Information Distribution in Grids. CESNET, 2007. Technical report.

[6] V. Goyal Certificate revocation using fine grained certificate space partitioning, 11th International Conference on Financial cryptography and 1st International conference on Usable Security, Berlin Germany, 2007.

[7] Daniel Kouril, Ludek Matyska, Michal Prochazka, "A Robust and Efficient Mechanism to Distribute Certificate Revocation Information Using the Grid Monitoring Architecture," ainaw, vol. 1, pp.614-619, 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07), 2007

[8] Online Certificate Status Protocol from Wikipedia, available at http://en.wikipedia.org/wiki/Online_Certificate_Status_Protocol

ISBN: 978-988-18210-6-5
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)