Efficient Certificate Revocation Lists in Public Key Infrastructure

Shalini Vermani

Apeejay School of Management, Dwarka, New Delhi. E.mail: s_vermani_s@yahoo.com

ABSTRACT
In this paper a brief overview of the existing revocation schemes is given and their advantages and disadvantages are also discussed. A new revocation scheme ECRL based on CRL is proposed here. The ECRL scheme overcomes two major drawbacks of the basic CRL scheme.

KEYWORDS
Authentication, Revocation, Public-key Certificate, Certification Authority

INTRODUCTION
In the digital world government, military, financial institutions, private businesses and hospitals store and process a great deal of confidential information about their employees, customers, products, research, and financial status on electronic computers and transmit it across networks to other computers. But information transmitted over the network is not secure. Any one can listen to or modify the information transmitted over the network. During this time when the Internet provides essential communication between tens of millions of people and is increasingly used as a tool for commerce, security becomes a tremendously important issue to deal with. One solution to this problem is to transmit the data in coded form. The art of keeping secrets secret is called cryptography. Traditional method of cryptography is called private key cryptography. In which a single key is used for both encryption and decryption. When two persons have to communicate then how will they establish a secure session key is one of the major drawbacks of private key cryptography. Another method is public key cryptography. In which each user has two keys – private key and public key. Private key is kept secret and known only to the person to whom it belongs and public key is made public. A message encrypted with the public key can only be decrypted with the corresponding private key and vice-versa.

Public Key Infrastructure (PKI) requires the ability to verify the authenticity of the public key of the other party. This is achieved through the use of certificates. A certificate contains user’s public key, identity, validity period and some other information digitally signed by a trusted third party known as Certification Authority(CA). Certificates are unforgeable i.e. only the CA can produce the signature. Certificates are used to prevent the use of a forged key in place of a legitimate key. When a certificate is issued its validity is up to its expiry date. But there are circumstances when a certificate may have to be revoked before its expiry date e.g. a user’s private key has been compromised or the authority that issued the certificate ceases to certify a given user. Therefore existence of certificate is necessary but not sufficient evidence for determining the validity of a certificate. The CA must provide the revocation information in a trustworthy manner to the user that relies on the data in the certificate to make decision. There are a number of available schemes to provide timely information to the user. Each of these has some advantages and disadvantages over the others.

OVERVIEW OF EXISTING SCHEMES

- Off-line revocation schemes
In off-line scheme, the validity information is precomputed by a CA and then distributed to the requester. Some of the off-line revocation schemes are:

A Certificate Revocation List (CRL) [8] is a signed list issued periodically that contains the serial number of all revoked but unexpired certificates. This list is digitally signed by the CRL issuer to avoid tampering. The main advantage of this scheme is its simplicity. CRLs are criticized for its high communication cost as the list becomes too large and not being able to provide timely information.

A delta-CRL [8] is issued between two CRL updates and provides the means for constructing incremental CRLs. It includes only changes since the last issued CRL. In order to obtain the most accurate revocation information, a relying party must retrieve the most recent base CRL and the most recent delta-CRL. Delta-CRLs allow the validity period of base CRLs to be extended, as the delta-CRL is relatively small and therefore can be issued on a much more frequent basis than the base CRL. This both improves latency and reduces the overall network load and hence the communication cost.

In indirect-CRL [1] scheme an authority other than the CA can issue a CRL. In this scheme a CRL contains the revocation information from multiple CAs. Therefore it reduces the overhead of obtaining the multiple CRLs to get the revocation information of certificates of multiple CAs.

In partitioned CRL[8] (also known as CRL distribution points) a single CRL is partitioned into multiple CRLs (segments) possibly issued at different rates. Each segment can be located on different hosts or on directories on the same host and each certificate has a pointer to the location of its CRL distribution point. In this scheme the revocation information is spread across a number of manageable partitions which improves performance by distributing the load. The drawback
of this scheme is that each end entity is likely to require access to multiple partitions. It therefore increases the average request rate. In CRL scheme request rate is maximum when new revocation list is issued. With the traditional method, a new CRL is not issued until the time specified in the nextUpdate field of the previously issued CRL has been reached. As a result, a relying party with a CRL in its cache will not request a new CRL from the repository until the time specified in the nextUpdate field of the cached CRL has been reached. It is possible to reduce the peak request rate by using over-issued CRLs [4] scheme. This scheme can be implemented by issuing a new CRL before the expiry of previous CRL. Then some relying parties will retrieve this new CRL while other relying parties continue to use the previously issued CRL. If each issued CRL is valid for the same length of time, then the relying parties that retrieved the new CRL will still have valid CRLs in their caches when the original CRL expires. Over-issued CRL scheme distributes the peak request rate.

There are a number of other off-line revocation schemes named as Redirect CRL [2], Freshest CRL [2], Certificate Revocation System (CRS) [14], Certificate Revocation Tree (CRT) [9] etc.

- **Online revocation schemes**
  
  In online revocation checking, an end entity can confirm the validity of the certificate by performing an online transaction that returns the current status of the certificate. Online revocation schemes may significantly reduce the latency between revocation of a certificate and the distribution of the information to the relying parties. One of the popularly known online method is **Online Certificate Status Protocol (OCSP)** [11]. In OCSP the client sends a request containing identifiers (serial number and other information) of the certificates queried to the server. The OCSP responder (server) checks the revocation status of the required certificate and issues an OCSP response to the client. The OCSP response must be digitally signed. Since the OCSP responder has to sign each reply it increases significantly processing load at the responder end.

  There are a number of other online certificate revocation schemes like OCSP extensions (OCSP-X) [7], Simple Certificate Verification Protocol (SCVP) [12], Data Certification Server (DCS) [3] etc.

  In off-line CRL based schemes a list is signed once and is distributed to the various dependent entities. But in online schemes the responder has to sign every response of the request made by the end entity. Therefore online schemes increase processing load at the responder end. Using off-line schemes, commonly the time between two updates is long and therefore, the validity cannot be assured exactly. However this is sufficient for the purpose of some applications. Online schemes are more appropriate for the applications where timely information is needed.

**EFFICIENT CERTIFICATE REVOCATION LISTS (ECRL)**

Efficient Certificate Revocation Lists (ECRL) is the proposed off-line certificate revocation scheme based on CRL [8]. The main criticism of the CRL is its poor performance. If the expiry

---

**ECRL Scheme**

<table>
<thead>
<tr>
<th>Certificate Revocation List</th>
<th>Time</th>
<th>Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>First CRL</strong></td>
<td>1 week</td>
<td>$c_1$</td>
</tr>
<tr>
<td></td>
<td>2 week</td>
<td>$c_1, c_2$</td>
</tr>
<tr>
<td></td>
<td>3 week</td>
<td>$c_2, c_3$</td>
</tr>
<tr>
<td></td>
<td>4 week</td>
<td>$c_3, c_4$</td>
</tr>
<tr>
<td></td>
<td>5 week</td>
<td>$c_4, c_5$</td>
</tr>
<tr>
<td><strong>Second CRL</strong></td>
<td></td>
<td>$c_1$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_1, c_2$</td>
</tr>
<tr>
<td></td>
<td></td>
<td>$c_1, c_2, c_3$</td>
</tr>
<tr>
<td><strong>Third CRL</strong></td>
<td></td>
<td>--------------</td>
</tr>
</tbody>
</table>

---

In ECRL scheme instead of issuing a single CRL three different CRLs are issued. Initially when a certificate is revoked its revocation information is kept in the first CRL. After keeping the revocation information in the first CRL for some fixed amount of time it is shifted to the second CRL. Similarly after keeping it in the second CRL for the fixed amount of time it is shifted to the third CRL where it is kept until its expiry date. In this way a single CRL is divided into parts. Suppose a revoked but unexpired certificate is kept in the first CRL for two weeks, in the second CRL for four weeks and in the third CRL for the remaining time. If a certificate expires in between then the corresponding revocation information will be removed from the revocation lists.

Therefore if a certificate is revoked not more than two weeks earlier then its revocation information will be in the first CRL. If a certificate is revoked not more than six weeks earlier then its revocation information will be in the first or the second CRLs. Otherwise to get the revocation information of a certificate one must have all the three CRLs.

Let the certificate revocation list be issued weekly and there be nine certificates numbered $c_1, c_2, c_3, \ldots, c_9$ such that a certificate revokes every week ($c_1$ in first week, $c_2$ in second week, $c_3$ in third week and so on.). Also suppose that none of the certificates expires upto the 9th week. Now how the revocation information of the certificates moves from one CRL to the other is shown below:

---
If Alice wants to communicate with Bob then Bob sends his certificate to Alice. Now Alice has to check the validity of the certificate (to make sure that the certificate has not been revoked so far). If Alice has a certificate of Bob that was issued not more than two weeks earlier, then its sure that if the certificate has been revoked in between then its revocation information will be in the first CRL. So Alice will request only the first CRL. If the certificate was issued not more than six weeks earlier, then its revocation information will be in the first or the second CRL. So Alice will request only the first and the second CRLs. If Alice has a certificate, which was issued more than six weeks earlier, then Alice will request all the three CRLs.

In ECRL scheme most of the time the client will request only first or first and second CRLs. Therefore it reduces the bandwidth requirement and hence the communication cost compared to the existing CRL scheme in which every time the entire revocation list is communicated to the client.

The other disadvantage of CRL is not to provide timely information. To overcome this problem combines the ECRL scheme with delta-CRL. To improve latency, issue the delta-CRLs frequently for all the three revocation lists.

In the ECRL scheme the revocation list is divided into three sublists. However, it can be divided into any number of sublists. Here the time span for which the revocation information of a certificate resides in the first CRL is two weeks, in the second CRL is four weeks and in the third CRL until it expires. Any other time span of equal/unequal lengths can be taken for which the revocation information resides in the lists.

CONCLUSION

In the ECRL scheme, most of the time only few segments of CRL have to be communicated to the dependent entity instead of transmitting the entire CRL. It also provides more timely information as compared to the basic CRL scheme. ECRL scheme is simple and easy to implement.

FUTURE SCOPE

There are a number of revocation schemes that shows benefits over one another. In off-line revocation schemes the receiver does not get the timely information whereas in on-line schemes the processing load at the responding end is very high. So in future researchers have to work to find some intermediates between the two so that the client get the timely information and at the same time the processing load at the responder site is not very high.

REFERENCES