A location-aware Revocation Approach

Damian Kulikowski, Peter Langendörfer, Krzysztof Piotrowski

IHP,
Im Technologiepark 25,
15236 Frankfurt (Oder),
Germany,
{kulikowski|langendoerfer|piotrowski}@ihp-microelectronics.com

Abstract: We present a new certificate revocation system for both on-line and off-line use, which is targeted to mobile-commerce systems. It allows to use certificates from any certificate issuer and to apply a proprietary revocation strategy. Our approach is well suited especially for location-aware services and mobile devices, because 1) our protocol reduces the amount of online communication, 2) the revocation tree is structured in such a way that certificates of services, which are located in the same region, can be verified using the same revocation proof.

1 Introduction

Mobile devices are actually the most popular terminals at the client side. In order to make e-commerce systems economically successful they need to evolve into mobile-commerce systems. I.e. they have to provide the same level of security for mobile transactions as they provide for wired operations. Due to the scarce resources of the mobile devices mutual authentication as well as verifying certificates should be as lightweight as possible. One potential solution is shifting the tasks to the more powerful infrastructure side and a second one is to reduce the network traffic in the system. The basic assumption in the design of our system is that mobile devices are going to use services in a certain environment, e.g. in an airport or in a shopping mall. In order to reduce communication and computing costs for the mobile device, we designed the system in such a way that retrieving the revocation status of a certain service provides the same information also for the services in its vicinity. This is achieved by clustering the revoked certificates with respect to their real world addresses. In addition the system allows using certificates of any issuer, which are then integrated in the revocation tree of the system.

The rest of this paper is structured as follows. First we give an overview of our system. Thereafter we present some more details concerning the revocation verification. Then we discuss our system in comparison to related work. The paper ends with a short conclusion and an outlook on further research steps.

2 Regional optimised revocation trees

Our system does not aim to provide specialized certificates. It is capable to integrate certificates from any issuer. It allows any m-commerce system to implement a unified interfaced to several independent certificate authorities. This enables end users as well as service providers to co-operate which such an m-commerce system without applying for a new certificate. The only obligation for certificate owners that want to participate in the system is that they have to register at the revocation system. But an m-commerce system, which uses our approach, may apply its own revocation rules, which may be stricter than those of the original issuing authority.

In our system we use revocation trees instead of revocations lists, due to the fact the revocation trees allow smaller transferable proofs. Especially the use of 2-3 trees decreases computational effort with respect to tree update operations (insert/delete operation) [NN98]. We modified the tree construction so that the certificates of services, which are located in the same area are included in the same branch of the tree. The location information that is used during the tree construction can either be retrieved from the distinguished name of the certificate owner or it can be requested when the certificate owner registers at the m-commerce system.

Several certificate authorities may be part of the overall system. They provide the current status of a certain certificate. Our revocation authority retrieves the certificate revocation lists from those third party certificate authorities. Then it updates its own revocation tree. During verification it generates revocation proofs and sends these to the requesting parties.

2.1 Location dependent tree structure

In order to exploit the location of the subjects in such a way that the verification overhead is reduced for mobile devices, the revocation tree has to be constructed in particular way. We use a five steps comparison of the location information given for a certain service, to place revoked certificates as close together as possible. First we compare the name of the country then the name of the city/state. Thereafter the more precise location information (e.g. organisation) is examined. In addition the certificate's issuer name and the unique serial number are taken into account, during the construction of the revocation tree.

2.2 Revocation proofs

The revocation proof consists of one or two paths depending on whether a certain certificate is revoked or not. If the revocation authority claims that a certain certificate is revoked, it responds with one path from the leaf, whose value is equal to the value of queried certificate up to the root node (see Figure 1a). For a valid certificate the revocation authority responds with two paths from two adjacent tree leaves up to the root, where one leaf value is smaller and the second one is greater than one of the certificate for which the proof is

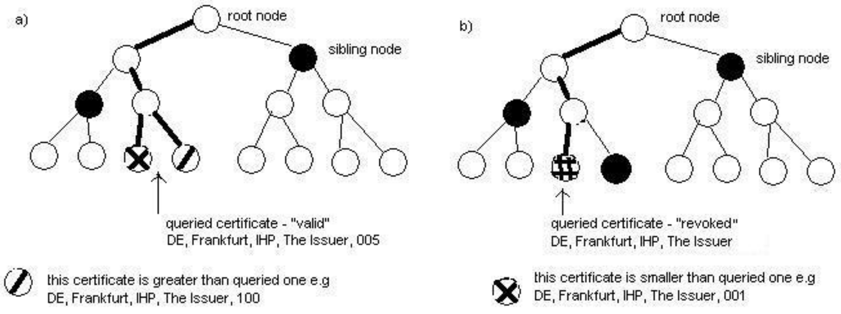
a)
root node
sibling node
queried certificate - "valid"
DE, Frankfurt, IHP, The Issuer, 005
this certificate is greater than queried one e.g
DE, Frankfurt, IHP, The Issuer, 100
b)
root node
sibling node
queried certificate - "revoked"
DE, Frankfurt, IHP, The Issuer
this certificate is smaller than queried one e.g
DE, Frankfurt, IHP, The Issuer, 001

Figure 1: Revocation paths for valid and revoked certificates

provided (see Figure 1b).

Each path is a sequence of hash values. These are calculated in the following way. For each interior node we apply the hash function in such way that the hash value is calculated from the concatenated hash values of its children.

To check the correctness of the proof the verifier has to apply the hash function to the sibling nodes. These are sent from the revocation authority along with the root hash value. Then the verifier has to compare the calculated value with the signed root value. To prove that a certain certificate is valid it is sufficient to have one proof consisting of two paths, which lead to smaller and greater value than the tested certificate value.

3 Our Certificate Verification Protocol

The client and the service authenticate one another by checking their certificates and revocation status. There are two types of verifiers: first one is a client who wants to check service's revocation status, and the second one is a service that checks client's revocation status. For our revocation system we made the assumption that the service is the more powerful party, so the major part of revocation verification should be performed by the service.

3.1 Checking service's revocation status

In our revocation system services are responsible for obtaining and storing their revocation status. They can request their status periodically, what enables them to have a small transferable proof for off-line use.

If the proof consists of two paths (the proof for not revoked certificate) it represents two revoked certificates. Then all certificates that are greater than the first value and smaller than the second value are valid. When the proof has only one path (the proof for revoked certificate) the client stores this value in its list of revoked certificates. It uses these leaf values for the future verification. After establishing a new connection with another service the client searches for revocation information concerning this service in its locally cached proof structure. If the requested information is not available or not fresh enough, the client asks the service about its newest revocation proof. The service responds with a proof unless it does not have it. Then the service has to establish an on-line connection to the revocation authority in order to download its revocation proof, which is then send to the client.

There are many places where mobile users execute electronic transactions one after another with several services which are located near to each other e.g. in a shopping mall or at an airport. Revoked certificates are stored in the same branch of the revocation tree if they belong to neighbouring services. Thus, the revocation proof of a still valid certificate enables the mobile devices to calculate whether the certificate of a service, which is locate near to the first one, is valid or not. Therefore, the client does not need to check the revocation status of each service individually, which reduces the computational effort and the network traffic.

3.2 Checking client's revocation status

The structure of client's revocation proof is the same the one of the service. A client does not have to care about its own revocation status, but after the first executed transaction with a service the client has the opportunity to retrieve its status from that service. If the service cannot extract the client's revocation status from his locally cached proof structures, it requests the revocation proof from the client. In case the client does not have a satisfying proof, the service has to request it from the revocation authority. The service caches the obtained information for future use, and forwards the proof to the client. This improves the revocation verification process of all further transactions performed by that client, at least for the time interval in which the proof is valid.

4 Discussion

The integration of mobile devices in the Internet raise a lot of new problems in the PKI area, which stem from the scares resources of these devices. The standard way to publish revocation state of certificates are certificate revocation list [NI93]. Their major drawback is the size of the revocation proof. This issue was addressed in [X.509] and further improved in [Co00]. A different approach to reduce the size of revocation proofs was proposed in [NN98], this one is applied in our system. [Ru99] discusses potential ways to improve the performance of PKI systems on mobile devices, one of the mentioned points is the reduction of the number of messages send to verify a certain number of certificates. Our system fulfils this requirement by exploiting the locality of verified certificates as well as by the fact that the certificates of several certificate authorities may be used. The benefits of system with such kind of nested PKI were discussed in [LK01]. [PCT03] describes a system, which also exploits locality. This system generates new certificates that are issued by a server, which is responsible for a certain region. The basic assumption here is that he clients stay in a certain area, whereas we assume that the services are tied to a certain place.

5 Conclusions

In this paper we have discussed a new revocation system. Its main features are its capability to integrate certificates from any certificate authority and that its revocation tree is structured using location information. Thus, retrieving a revocation proof for a certain service provides automatically also the revocation proofs for services in its vicinity. So, clients are enabled to verify the revocation state of several services without additional communication and computational effort.

In our next research steps we will verify under which conditions the computational effort on the client side can be reduced further, e.g. by applying a different structure of the revocation proofs. In addition we will quantify the benefits our approach for several usage scenarios.

References

[Co00] Cooper, D. A.: "A More Efficient use of Delta-CRLs". In *Procedings of the 2000 IEEE Symposium on Security and Privacy*. May 2000.

[LK01] Levi, A.; Koc, C. K.: "Reducing Certificate Revocation Cost using NPKI". In Trusted Information, The New Decade Challenge, IFIP TC11 16th International Conference on Information Security, M. Dupuy and P. Paradinas, (editors), Kluwer Academic Publishers, Boston, MA, June 11-13, 2001.

[NI93] U.S. National Institute of Standards and Technology. "A Public Key Infrastructure for U.S. Government Unclassified but Sensitive Applications". Federal Information Processing Standards Publication 180. 1993.

[NN98] Naor, M. und Nissim, K.: "Certificate revocation and certificate update". In: *Procedings 7^{th} USENIX Security Symposium*. pp. 217–228. 1998.

[PCT03] Popescu, B. C.; Crispo, B.; Tanenbaum, A. S.: "A Certificate Revocation Scheme for a Large-Scale Highly Replicated Distributed System". Proc. 8th IEEE International Symposium on Computers and Communications. pp. 225-232. June 2003.

[Ru99] Russell, S.: "Fast Checking of Individual Certificate Revocation on Small Systems". In Proceedings of the ASAC Conference. 1999.

[X.509] ITU-T Recommendation X.509 (1997 E): "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework". June 1997.