Disaster coverable PKI model based on Majority Trust principle

Vesselin Tzvetkov

Arcor AG&Co, KG
Alfred-Herrhausen-Allee 1, D-65760 Eschborn, GERMANY
vesselin.tzvetkov@arcor.net

Abstract

The Public Key Infrastructure(PKI) is an important part of almost all security implementations from secure portals for banks and e-shops to vpn devices. In spite of its strengths there is a critical design issue causing a single point of failure for the PKI infrastructure. Once a CA (Certification Authority) key has been stolen, the integrity of the entire system can be exposed to bogus certificates, compromising the validity of all digital identities issued under this CA.. In this paper we introduce the problem and propose a solution to distribute the trust responsibility to accredited agents. The major advantage of the proposed solution is its compatibility to classical PKI based on x509 certificates.

I. Introduction

The PKI is an evolutional step in cryptography because of the asymmetric encryption algorithms as DSA/RSA and the hierarchical scalability. The use of Digital Signature is a reliable and reasonable alternative to the classical hand signature. This is reflected in the legislation of many countries, that principally Digital Signature is as authentic as classical signature.

An Achilles' heel or the crux of the PKI is its hierarchy, which results in blind trust of the credibility and authenticity of the CA. When the CA key is compromised, the whole PKI structure collapses and the structure should be initialized from the very beginning. This horror scenario can not be treated and principally solved by the current concept of PKI. This is even a difficult task to determine, if the key is destroyed or stolen, which is decisive for further actions.

As a fact there are worldwide only few examples of implementing a PKI structure in official government structures; we believe that it is also due to this single point of failure

The proposed model, called Majority Trust, extends the PKI with reliable and resistant mechanism against lost or abuse of the CA's key. There are two major basic design conditions: first it should be compatible with the well spread existing x509v3 PKI. The Hosts, supporting Majority Trust, can act according to its principles. Other hosts, which don't support it, can proceed in the classical PKI way. This co-existing of both models is a key feature for the successful practical implementation. The second design task considers the vulnerability of the CA and distributes the responsibility for the structure between multiple trusted authorities, called *Accredited CAs.*

II. Relation to other PKI Trust Model

Cross Certification and Certificate Trust List

Cross Certification [6] and Certificate Trust List are standards defining the possibility for integration of different PKI structures without changing the trust authority. Cross Certification and CTL does not change the responsibility domains of the single CA.

Decentralization Methods based on Threshold Cryptography

Solutions for distributing the CA responsibility were proposed based on threshold cryptography [1], since the problem was treated in *Ad-Hoc* network [3]. These solutions assume building new PKI structure with new CAs servers and clients. Majority Trust is based on the existing PKI Model.

Models based on forward-secure signature scheme (FSS)

Some proposals make use of FSS algorithm [4], which also requires new PKI clients and CA servers, which complicates the practical implementation.

III. Majority Trust

First of all a relation between an odd number of authorities should be settled. There should be an *Issuer CA* and even number of *Accelerated CAs*. All authorities should regularly authenticate each other in *authentication periods*. The authentication should be based on non PKI methods, for example biometrics. After the authentication the Accredited CAs sign the user public key provided

from the Issuer CA.

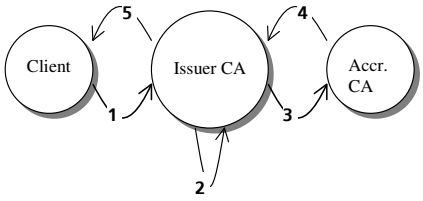
IV. Certificate Revocation Lists

All authorities issue new CRLs every authentication period, where they can revoke Issuer/Accredited CA and user certificates. All user should download the CRLs in order to verify the validity of the certificate. A new CRL extension called **RevokedAccreditedCA** is defined.

V. Issuing the user certificate

The user generates a certificate request and provides it to the Issuer CA, which authenticates the user with his credential (Step 1 on Diagram 1). The Issuer CA adds the request to its *issuing queue* (Step 2). During the next CA's authentication the Issuer CA sends the user request in its queue to every Accredited CA (Step 3). If the Issuer CA and Accredited CA have successfully authenticated themselves, the Accredited CA signs the hash of the user's public key and returns it to Issuer CA as certificate attribute **SignedUserKeyIden** (Step 4). If the authentication fails, a zero attribute **SignedUserKeyIden** (value null) is used. The attribute **SignedUserKeyIden** is set in extension **AccreditedAuthKeyId** and the user certificate is issued and distributed to the user (Step 5).

Diagram 1: Issuing a user certificate



Steps 3 and 4 are repeated for every Accredited CA and **AccreditedAuthKeyId** extensions are added to user certificate. The steps 3 and 4 are proceeded only during the CAs authentication in every authentication period.

VI. User Policy

Every authentication period the user downloads the latest *n* CRLs from every CA. To validate the certificates the clients implement the quorum principle: if one CA (Accredited or Issuer) is revoked in more then *n/2* CRLs, the CA is not trusted - revoked. The CRLs from revoked CA are no more considered.

If the Issuer CA is revoked from the quorum of CAs, the PKI is in state *Capsulated.* – no more new certificates are accepted. All user certificate issued after the revoking date (Capsulation Date) of Issuer CA are not trusted, since they will have all zero value **SignedUserKeyIden** in all **AccreditedAuthKeyId** extensions. Already issued certificates are further valid, because they have valid extensions signed from the Accredited CAs. The user certificate can also be revoked on the quorum principle.

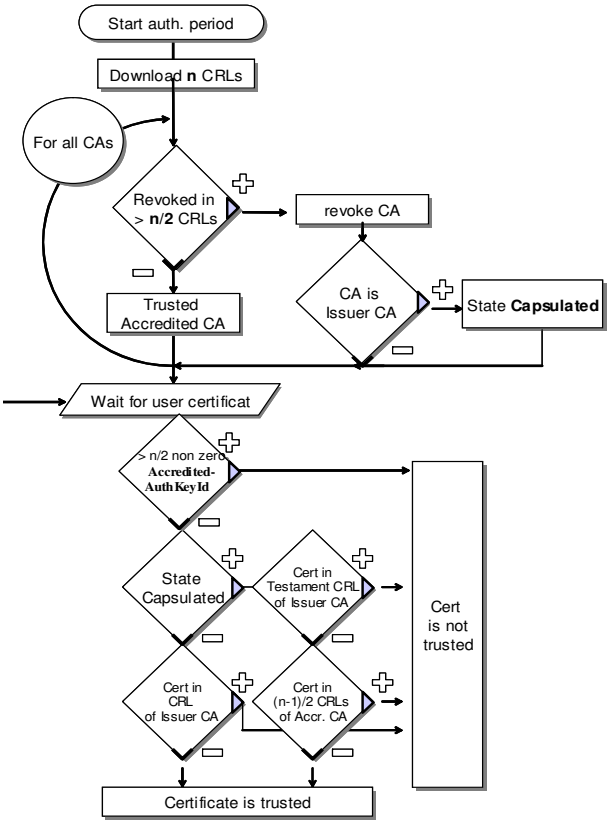


Diagram 2: User policy

VII. Conclusion

CA key compromising was not treated enough deeply in the current PKI, which makes the current PKI unattractive for official structures. The Majority Trust enhances the current PKI to resist against CA attacks PKI.

VIII. Acknowledgement

The author would like to thank Prof. C. Eckert for the helpful comments.

IX. References

[1] "Some Recent Research Aspects of Threshold Cryptography." In E. Okamoto, G. Davida at. al Springer-Verlag, 1997.
[2] "Internet x.509 Public Key Infrastructure. Certificate and CRL (Profile)" Housley, et.al., RFC 3280 April 2002
[3] "Key Management for Heterogeneous Ad Hoc Wireless Networks", Seung Yi Robin Kravets 2002
[4] "Decentralization Methods of Certification Authority Using the Digital Signature Schemes", S.Koga, K.Sakurai 2003
[5] "How to Share a Secret". A. Shamir. ACM, 1979.
[6] "Cross-Certification and PKI Policy Networking", J. Turnbull, 2000