Incorporating revocation of certification into a PKI model

ABSTRACT

Public key infrastructures (PKIs) are complex distributed systems that are responsible for giving users enough information to make reasonable trust judgments about one another. PKI is a prerequisite for security in distributed systems and for electronic commerce. The validation of public keys is hence of paramount importance. This is achieved by public-key certificates. Several researches have done to evaluate the confidence afforded; one of them is Maurer's model. The problem of assigning and evaluating confidence values numerically (Maurer model) is non-trivial, in particular when certification paths intersect. A restriction in this model is that certificate revocation is not included, but usually revocation happens. While Maurer consider only positive evidence, in this paper has been considered negative evidence as well as revocation. Moreover a few of authors incorporate negative values in inference rules on deterministic part. In this paper we have used a tailored form of that and consider revocation on inference rules. After that negative evidence to exert in probabilistic part, with to take in to a suitable value for this evidence omits the path of trust include the revoked certification.

Keyword: Certification; PKI; Revocation; Trust model