Creating Virtual Hierarchy in Peer-to-Peer PKI to Simplify Certificate Path Discovery

Abstract

Peer-to-Peer Public Key Infrastructure (also called Mesh PKI) architecture is one of the most popular PKI trust models that is widely used in Mobile Ad-hoc networks (MANETs), but certificate path verification is very complex since there are multiple paths between users and the certification path is bidirectional. Unlike a Hierarchical PKI, in Mesh PKI, building a certificate path from a user’s certificate to a trust point is nondeterministic. Certificate Path verification in Hierarchical PKI is simple and straightforward. In this paper, a novel method to establish a virtual hierarchy in Mesh PKI to simplify the certificate path discovery is proposed.

References

Creating Virtual Hierarchy in Peer-to-Peer PKI to Simplify Certificate Path Discovery

org/rfc/rfc2459. txt
- Jordi Fornà, Jose L. Munoz et. al, Certificate Status Validation in Mobile Ad Hoc Networks, Technical University of Catalonia and University of the Balearic Islands, 2009.
- Cristina Satizbal, Rafael Pez, Jordi Fornà, Building a Virtual Hierarchy for Managing Trust Relationships in a Hybrid Architecture, Journal of Computers, VOL. 1, NO. 7, October/November 2006.
- M. Cooper et. al., Internet X. 509 Public Key Infrastructure : Certification Path Building, Network working group, RFC 4158, September, 2005.

Index Terms
Computer Science 
Networks

Keywords
Hierarchical Pki 
Manet 
Certification Authority (ca) 
Web Of Trust 
Certificate Graph