Abstract

Information security and trust are the most important factors to be considered in e-commerce and e-business transactions. The protection and distribution of valuable information that is needed in a widely pervasive environment is the main goal of modern security architectures. The users, resources and the information are spread across different places. The users need information at different times. Even though there are many solutions to improve the quality of security services, there is a significant opportunity to improve those services in e-commerce and e-business applications. The emerging approach to address the security needs makes use of the scalable and distributed characteristics of Public Key Infrastructure.

Public Key Infrastructure (PKI) is one of the solutions to use the security services in a useful way. PKI is a framework on which the security services are established. A PKI binds user’s Public Key with a data structure called Public Key Certificate or Digital Certificate. It can provide various secure services in e-commerce and e-business transactions. A number of security related services like end entity authentication, data integrity etc. are supported by PKI and this needs a proper utilization of the key pairs generally used in PKI i.e., public or private key pairs.

Each company willing to transmit its critical data safely over the internet has to deploy a PKI. X.509 PKI systems are the most popular PKI systems deployed in enterprises. The systems have evolved from simple single CA(Certification Authority) PKIs, to complex enterprise PKIs, to cross-certified PKIs, and now to bridge technology. There are different types of PKI models which are also called trust models. One of the popular and most commonly used trust models is the Hierarchical PKI model. Since each company deploys its own security infrastructure, there arise interoperability problems during communication with other companies.

During merger and acquisition of companies, the multiple PKIs deployed by them must be interoperated. Interoperability is viewed both by customers and industry analysts as a critically important issue for PKI. PKI interoperability offers greater
flexibility and freedom of choice between products of different vendors in deploying a PKI based solution. Hence, design and implementation of interoperable trust models is a major thrust area in Network security. To date, there have been several solutions to improve interoperability between enterprise PKIs. Much research work has been carried out to develop trust models that facilitate interoperability. In this research work, algorithms are developed for faster and cost effective interoperable PKI architectures that are suitable for merger and acquisition of companies and their efficiency is compared with other PKI merging solutions. The situations considered are: i) Merging Hierarchical PKIs without using cross-certification that can be used when companies dynamically change their collaborators and the merging is temporary, and ii) Merging Hierarchical PKIs without using cross-certification during acquisition of companies.

The interoperable PKIs can be designed either by using cross-certification between PKIs or without using cross-certification. But in both the cases, consideration of the issues related to Certificate Policy (CP) and Certificate Practice Statement (CPS) is very important. A certificate policy describes the following parameters:

- Allowable encryption and signature algorithms
- Minimum key sizes
- Certificate validity period
- Maximum period between Certificate Revocation List updates
- Allowable mechanisms for verifying the identity of the entity prior to certification

A policy will be named by an object identifier (OID), and the policy’s OID will be contained within all certificates issued under the policy. The automation of merging PKIs is not yet achieved properly mainly because of the inadequate
standardization of the CPs. The CPs define the PKI certificates’ profile and, thus, form the basic comparison parameter for the mutual acceptance of CAs. The cross-certification is not yet technically provided in an automated way largely due to the inadequate standardization of the certificate policies. In other words, although the CP structure is defined in some of the existing standards, there is still a significant gap in the standardization of the CP content (e.g., roles of the involved subjects, certification and registration requirements, etc). There is no systemized way for the development and the comparison of CPs, thus making their comparative analysis a difficult task. In addition, lack of adequate CP comparison tools for comparison of CPs is one more problem associated with merging of CPs. The above restrictions together with the lack of the necessary legal/regulatory issues make the automation of CP comparison complex. This affects the automation of the overall merging process with or without cross-certification service, which makes secure electronic co-operation, information exchange and knowledge sharing over the internet a difficult task. While developing PKI merging algorithms, the issues related to Certificate Policy (CP) are also considered in this research. An efficient method for comparison and assessment of Certificate Policies has been developed.

One more nontrivial service provided by PKI is certificate based user authentication. Authentication involves syntactic verification of a certificate chain followed by a semantic look at the policies under which the certificates were issued. Masquerading is the most commonly occurring security threat which is to be addressed properly. Millions of users are participating in e-commerce and e-business transactions over the internet. So, authentication of the users is a challenging task. In Public Key Infrastructures, the authentication of the users can be done by performing verification of their certificates. Essentially it is nothing but verification of user’s public key. One critical process for the public key verification in Hierarchical PKI is certificate path verification. Certificate path verification involves the task of discovering a path and then verifying its validity. The path discovery is a complex task since it involves finding a chain of CAs that trust each other. A
centralized public key management system such as central Certification Authority or a directory is used for doing this process conveniently. In some type of PKI models such as Hierarchical PKI, certificate path is unidirectional, so certificate path development and validation is simple and straightforward. Each Relying Party (the certificate verifier) has an acceptable trust policy for the chain of CAs that it is trying to validate for a given certificate. The certificate policy defines the minimum level of CA practices that it expects from each of the CAs on the path. There are some well-established algorithms for verification of users’ certificates in Hierarchical PKIs, but still there is significant opportunity for optimizing those methods.

Mesh or Peer-to-Peer PKI is another type of trust model which is widely used in MANETs. In peer-to-peer network cross-certification plays a very important role. The term cross-certification is defined as the establishment of a trust relationship between two certificate authorities (CA) through signing of each other’s certificate. Since a Mesh PKI is constructed with peer-to-peer Certification Authority relationships, the path between users is bidirectional. There may be multiple paths between any two users. Thus building a certificate path from a user’s certificate to a trust point is nondeterministic. All the above factors make the certificate based user authentication in Mesh PKI a complex process. Thus there are enough reasons to take up the development of a proper certificate verification technique in Mesh PKI as one of the research problems.

Thus, one more research problem considered in this research work is to develop novel certificate path verification algorithms in Hierarchical and Mesh PKIs.

The merging methods of Hierarchical PKIs is explained in chapter 4 and chapter 5. Chapter 4 presents a merging method of Hierarchical PKIs that can be used when the merging of companies is temporary and companies dynamically change their collaborators. The merging method explained in chapter 5 is applicable when one company acquires one or more other companies. Chapter 6 highlights a method to compare and assess certificate policies during merger and acquisition of
companies. Chapter 7 and chapter 8 explain efficient methods to certificate path verification in Hierarchical PKI and Peer-to-Peer PKI respectively.

The overall contributions of the research include merging Hierarchical PKIs during merger and acquisition of companies, developing an efficient method to compare and assess Certificate Policies while merging PKIs, and developing efficient certificate path verification algorithms in Hierarchical and Mesh PKIs. It is observed that, the efficiency of the methods developed is comparatively better than the solutions suggested for the same purpose by other researchers.