Advances in Computer Science and Information Technology (ACSIT)
p-ISSN: 2393-9907; e-ISSN: 2393-9915; Volume 4, Issue 2; January-March, 2017, pp. 130-132
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

Trust Models in Public Key Infrastructure

Sarvesh Tanwar[1] and Prema K.V[2]

[1,2]*Department of Computer Science & Engineering, Mody Institute of Technology & Science, (MITS) Laxmangarh-332311, Rajasthan, India*
E-mail: sy_kanu@rediffmail.com

Abstract—*Today more and more companies are using Internet as a platform to operate their business systems. With transaction over the Internet, E-commerce is different from traditional face-to-face business model, merchants and customers cannot identify each other directly. Therefore, additional privacy and integrity mechanisms become necessary. Public Key Infrastructure (PKI) provides the secure communication over the unsecure network. PKI is proposed to ensure trust relationships being established and facilitate communication with confidentiality, integrity, and non-repudiation among the entities. It is very important to support secure global electronic commerce and digital communications on networks that depend on the trust among them. Trust is a well-established concept, and there are many examples of conventional trust relationships such as a bank and its account holders, between an employer and its employees, between a government and its citizens, between the media and its subscribers, between an industry association and its members and so on. For maintaining the trust we need different trust models. In this paper we describe the various trust models used in PKI.*

Keywords*: - E-commerce, Public key infrastructure, non-repudiation, Trust.*

1. INTRODUCTION

PKI is a framework for creating a secure method for exchanging information based on public key cryptography. The foundation of a PKI is the certificate authority (CA), which issues digital certificates that authenticate the identity of organizations and individuals over a public system such as the Internet. The certificates are also used to sign messages, which ensure that messages have not been tampered with [1].

Over insecure networks, PKI is responsible to issue, maintain, and revoke public key certificates. A PKI permits users to exchange data through the use of a public and private key pair that is obtained and shared through a trusted authority (CA). A Certification Authority (CA) is a trusted entity whose central responsibility is certifying the authenticity of users or end-entities. To establish trust in the binding between an end-entity's public key and other information (e.g. name) in a certificate, the CA digitally signs the certificate information using its signing private key. End entity is a certificate subject that uses its private key for purposes other than signing certificates. An entity's "electronic identity", issued to it by a CA, is the entity's proof that it is trusted by the CA; therefore, through third- party trust, any entities trusting the CA should also trust it and thus authenticate its public key [3].

2. PKI TRUST MODELS

A trust Model is collection of rules that informs application on how to decide the legitimacy of a Digital Certificate. Architecture of a PKI is composed of operations and security policies, security services and protocols that support interoperability using public key encryption and key management certificates. In PKI a digital certificate issued by CA and applications are usually processed by the Registration Authorities (RA). The responsibility of an RA is to analyze individual user who examines each application and notifies the CA, which is closer to the level of confidence of the applicant by checking the level of confidence, CA issue the certificate. The architecture of a PKI system describes the organization of its CAs and the trust relationship among them [2].

2.1 Peer to Peer trust model

In this model, there is no starting point as a trusted root CA. Certificate users typically rely on their own local CA, and as a starting point of trust. The two CA are now isolated. They are different trust domains; domain users can verify the domain user. This trust model is the most prominent feature is its flexibility, making the trust domain extension is very convenient. But it is this flexibility, so that the manageability of the whole system worse off. With the increasing number of CA, the certification path building is a very difficult task, may appear multiple certification paths, there may be an infinite loop, thus making it difficult to verify the certificate, thereby increasing the burden on users. Therefore, such model is applicable to small, small number of groups of coequal status of the implementation of the organizational PKI. In the peer-to-peer model, the two CAs will certify the public key for each other, which creates a bidirectional trust. This is referred to as cross certification, since the CAs do not receive their certificates and public keys from a superior CA, but instead they create them for each other.

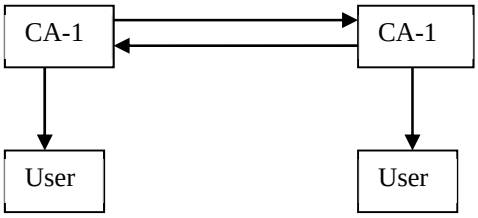

Fig. 2.1: Peer to Peer Trust Model

2.2 Bridge CA

The "Bridge PKI" [6] model is designed to support PKI applications across enterprises and avoid the situation where the user has to maintain information of a large number of trust points or an organization needs to establish crosslink to a large number of other organizations.

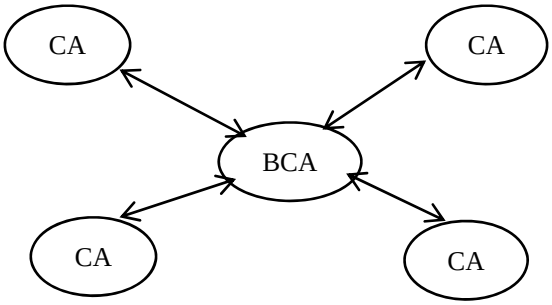

Fig. 2.2: Bridge Trust Model

Using BCAs (in place of bilateral arrangements between separate PKIs) can decrease the total number of cross certificates required to join the PKIs. The BCA does not become a trust anchor for any of the PKIs as it is not directly trusted by any of the PKI entities. Rather trust is referenced from internal PKI trust anchors. The United States federal PKI (FPKI) project is attempting to join together multiple PKIs set up under separate federal agency programs using bridge CAs [4].

2.3 Hierarchical trust model

Hierarchical trust model is like an inverted tree structure, in which root is the starting point of trust, that we all trusted root CA, the top-down parts of the branches have a CA, the leaf node is the user (As shown in Fig. 2.3). Root CA for the issuance of its certificate of direct descendants of the node; intermediate nodes as its direct descendant CA. CA issued certificates node; intermediate nodes that the end-user CA can issue certificates, but for the end-user certificates issued under the CA cannot have a CA.

All nodes of the model have to trust the root CA, and keep a root CA's public key certificate. Communication between any two users, in order to validate each other's public key certificate, must be achieved through the root CA.

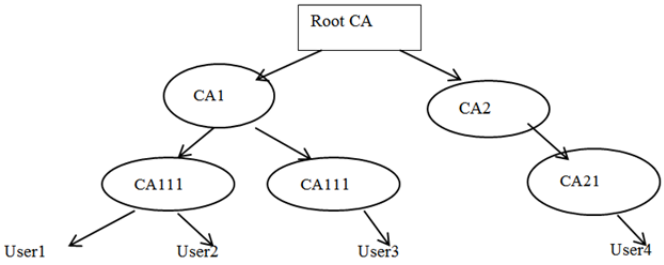

Fig. 2.3: Hierarchical Trust Model

It can be seen in the hierarchical model, the root CA is the trust center for all users, if root CA trust crisis occurs, there is a crisis of confidence throughout the PKI system, and thus in the chaotic Internet environment is very practical.

This model is not suitable for such an open environment in the Internet use, of course, not suitable for e-commerce systems, but it is suitable as the military, government or within the industry so that the upper and lower hierarchical departments.

2.4 Hybrid Trust Model

In practice, the general use of hybrid model is a combination of several models. As shown in the Fig. 2.4 Root CA1 and CA to form a trust domain, the root CA CA2 and its children constitute another trusted domain. They are hierarchical trust model. Then, the root of the root CA1 and CA2 for cross-certification, which constitute the two other models. Thus, the two domain users can verify each other. This model has the advantage of easy to operate, widely used.

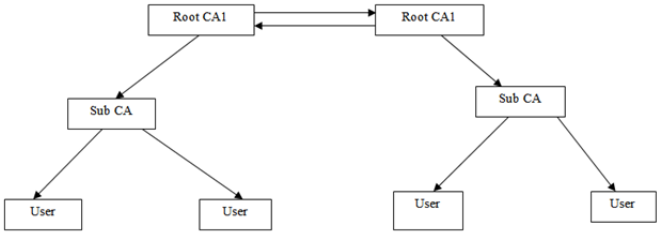

Fig. 2.4: Hybrid Trust Model

2.5 Web-of-trust model

Web of trust is a term used in cryptography to describe decentralized security models in which participants authenticate the identities of other users. Web of trust is a concept used in PGP, GnuPG, and other OpenPGP-compatible systems to establish the authenticity of the binding between a public key and its owner [3]. Its decentralized trust model is an alternative to the centralized trust model of a public key infrastructure (PKI), which relies exclusively on a certificate authority (or a hierarchy of such). In this type of system each user creates and signs certificates for the people he or she knows. Therefore, no central infrastructure needs to be developed.

The web-of-trust model differs greatly from the hierarchical model. The hierarchical model is easily represented with computers as an inverted tree, but the web-of-trust more closely relates to how people determine trust in their own lives. The system allows users to specify how much trust to place in a signature by indicating how many independent signatures must be placed on a certificate for it to be considered valid [5].

This model works very well for small groups who have pre-existing relationships, but it doesn't scale well for large groups or where consistency of assurance (e.g. level of authentication required before a certificate is issued) is important.

3. CONCLUSION

Basically trust models provide the environment whether to trust on one organization or not depending upon the certificate issued by the certification authority. Different trust models are suited to different business organizations. If size of the organization is small and uniform, then implementing a Peer to Peer seems to be most appropriate choice. It is easier to implement mesh or peer to peer architecture as there is no well-defined organization structure and in it certificate path discovery and validation is complex because there are multiple path between the CAs.. However, when organization has a well-defined and formalized organization structure, we can implement hierarchical PKI architecture. In hierarchical architecture Root CA is the most trusted CA and has the highest authority. And in hierarchical architecture certificate path is unidirectional, so certificate path development and validation is simple. If cross certification is required to establish the trust, Bridge PKI architecture is the best suited to link PKIs that implement different architectures.

REFERENCES

[1] PC Magazine Encyclopedia, www.pcmag. com, Accessed on 25th April, 2009.

[2] Chen Jie “Design Alternatives and Implementation of PKI Functionality for VoIP”, Master Thesis, KTH, Stockholm, June 2006.

[3] Haibo Yu, Chunzhao Jin, Haiyan Che, “A Description Logic for PKI Trust Domain Modeling”, Proceedings of the Third International Conference on Information Technology and Applications (ICITA’05) 0-7695-23161/05 $20.00 © 2005 IEEE.

[4] **S. Garfinkel, G. Spafford. Web Security, Privacy & Commerce. O’Reilly, Cambridge, 2002.**

[5] SPKI/SDSI and the Web of Trust. http://theworld.com/~cme/html/web.html.

[6] John Linn, Trust Models Management in Public Key Infrastructures”, Nov. 2000.