Case study on public key infrastructure

Sociology, Identity

Public Key Infrastructure is a system that allows the integration of a number of carrying services that are in one way or the other related to cryptography. PKI ensures integrity, provides confidentiality, access control, a system of authentication and also non-repudiation - in which both parties, the sender and receiver cannot deny either sending the message or receiving it in future. (Srinivasan, 2008)

Basically, PKI is an aggregation of processes, technologies and policy of organizations that facilitate the use of public key cryptography in ways as to enhance the verification of the authenticity of public keys (BCS, 2013)

The primary functions of PKI include digital key exchange, Encryption and decryption and digital signature. (Srinivasan, 2008).

The encryption technology used in PKI is known as Public Key Encryption. The system uses asymmetric cryptography which involves a " pair of keys" (Srinivasan, 2008). Each pair of key includes a private key and the other one is called a public key. There is a key repository in which the public key is stored. The public key is accessible to everyone. The private key, on the other hand, is never revealed to anyone and is kept secret, as the name implies, by the owner of the key.

The key can either function to encrypt or decrypt a message. Moreover, a message which has been encrypted with a private key can be decrypted only with the public key which corresponds to it. On the other hand, a message encrypted by use of a public key can be decrypted only with the private key which corresponds to it.

In order to ensure the security of the data sent between two individuals and also in order to ensure that there is no alteration of the data during the process of transmitting the document, the sender of the document encrypts the document with the public key of the recipient. This ensures that the data can only be decrypted with the private key of the recipient.

In order to ensure that the content of the transmitted message is not altered during the process of transmission, the sender of performs a hash function. The hash value is called the message digest. This value is sent along with the document. The receiver of the data compares this value to the message digest sent by the sender. This process ensures that the data sent has not been compromised in its integrity.

The sender applies a digital signature to the document. The digital signature is the sender's private key. The data sent can only be decrypted with the use of the sender's public key.

A digital certificate is used in PKI to authenticate the identity of an entity. The digital certificate serves as a form of electronic identity for the entity. The digital certificate is the public key.

The advantage of a public certificate is that it ensures a high standard in the verification of the identity of the user. This type of certificate is desired if verification of the identity of the user is a high priority. However, it is important to examine the cost implications especially if the organization uses a large number of systems. Using a public certificate on all the systems might lead to accumulation of huge costs (IBM, 2013).

The advantage of having private certificates is that there is better internal control over the specific users who can hold the privilege of having the certificate and as such, access to sensitive information within the organization can be easily controlled.

In view of the structure of the organization, I would strongly suggest that a private certificate be issued to sensitive systems so as to facilitate the flow of information among sensitive computer systems.

REFERENCES

Srinivasan (2008). Public Key Infrastructure (PKI) and other Concepts in Cryptography for CISSP Exam. PACKT Publishing. Retrieved on 11th August, 2013 from http://www. packtpub. com/article/public-key-infrastructure-pki-other-concepts-cryptography-cissp

IBM (2013). Public Certificates versus Private certificates. IBM. retrieved on 11th August, 2013 from

BCS (2013). PKI -what is it and do i need one?. THe Cjartered Institute for IT. retrieved on 11th August, 2013 from