Global Information Assurance Certification Paper

Public Key Infrastructure – A Brief Overview

The Need for Security

As organizations increase their use of the Internet as a business tool the importance of security also increases. A Public Key Infrastructure, or PKI, enables organizations to securely conduct their business on public networks by providing user authentication, non-repudiation, data confidentiality and data integrity. Without this framework many of today's e-business applications would not be able to function due to the inherent lack of trust between the communicating parties.

Public Key Infrastructure Framework

A Public Key Infrastructure incorporates both hardware as well as software components, which are in turn managed by security polices. The main components include: Public Key Cryptography, a Certificate Authority (CA), a Registration Authority (RA), a Certificate Distribution System, Security Policies, and a PKI enabled application.

Public Key Cryptography – Each user has a key pair, generated during the initial certificate deployment process, that is comprised of a public key, which is shared, and a private key, which is not shared. Data is encrypted with the user's public key and decrypted with their private key. Digital signatures, used for non-repudiation, authentication and data integrity, are also generated using public key cryptography. Most PKI implementations also support a dual key-pair.

Certificate Authority – The CA is the backbone of the framework, which issues user certificates and acts as the chief agent of trust. In certain large scale PKI models there may be multiple CAs configured in a hierarchical layout with a master CA known as the Root CA. The Digital certificates issued by the CA should be X.509 v3 compliant to ensure inter-operability and includes information such as the name of the issuing CA, the validity period, the user's name, e-mail address and public key. When issuing a certificate to a user, the CA signs the certificate with it's private key in order to validate it. During electronic transactions the CA also confirms that certificates are still valid and if they are not the server will revoke them. Certificates may be revoked for various reasons. For example, a user may leave the organization or they may forget their secret passphrase, the certificate may expire or become corrupt. This process is usually accomplished through the use of a Certificate Revocation List (CRL) which is a list of the certificates that have been revoked. Only the certificates that have been revoked appear on this list.

Registration Authority – The RA accepts user requests for certificates and once the user's identity has been authenticated the request is then forwarded to the CA. The authentication of a user can either be an automated process, for example checking the user information against an HR database, or a manual one, for example submitting government documents, such as a passport or a drivers license, in person, depending on the level of trust that will be associated with the certificate required by the user.

Certificate Distribution System – Depending on the size of the PKI deployment, a directory server may be used to distribute and store certificates. This server would use the Lightweight Directory Access Protocol (LDAP) in order to access the user

information stored in an X.500 compliant database when storing and querying certificates.

Security Policies – The PKI runs according to the guidelines that are found within the security policies which outline how the certificates are issued, revoked, renewed and stored. The certificate policy also defines the approved uses of the public keys. Organizations that run commercial CAs, known as trusted third parties, publish a Certificate Practice Statement (CPS) for their clients which contains detailed information such as how the CA is secured and operated, the user verification procedures used, the scope of the certification, certificate lifetime and cross certification.
Due to the importance of a PKI the managing policies need to be developed by a team that include members from management, the IT department and the legal department to ensure that the security objectives are met.

PKI Enabled Applications – Applications that require a high level of security are good candidates for a PKI implementation. They include e-mail, Virtual Private Networks, and Internet based on-line transactions.

PKI Issues
There are many issues that arise from the development, deployment, management, and usage of a PKI implementation. Some important issues or considerations include CA cross certification, private key management, deployment and interoperability.

CA Cross certification – Sometimes the users of a PKI need to communicate with users from another PKI. In this case the Root CAs of each PKI need to 'trust' each other's certificates, which is known as cross certification. The issue here is how is trust established and how are the communicating organizations guaranteed that it is maintained?

Private Key Management – Depending on the PKI deployment users will be required to store their private signing key either on their local computer, or on a diskette or smart card. These storage mediums are inherently insecure since access to the workstation cannot be granted only to authorized individual, floppy diskettes may be lost or stolen, and smart cards are, on average, very weak. Once access to the private signing key has been achieved it is only as secure as it's passphrase. There is no perfect solution, although the development of biometrics will certainly help in the area of user authentication. Until then the users and administrators of a PKI will have to accept some measure of risk.

Deployment – There are many decisions to make when deciding to implement a company wide PKI. Foremost is the question of whether an organization will want to host their own CA and all of it's subordinate components or decide to outsource the solution, PKI is very expensive and in some case difficult to justify.

Interoperability – Interoperability is very important since most organizations have a mixture of systems from web servers running e-commerce applications to legacy systems which supply 'a strong backend to transaction systems. Also various applications will use certificates in different ways and may require different levels of trust. The need may arise to have more than one CA in order to issue more that one

type of certificate. Fully integrating the PKI solution may require the involvement of various vendors, supplying a number of products.

Trust Is Everything

Although there are several issues regarding the implementation, deployment and management of a Public Key Infrastructure, it is thought by many that PKI will finally allow the business community to securely harness the e-commerce potential of the Internet. Public Key Infrastructure may not be the silver bullet that we have been hoping for, but until now it is all we have to ensure e-commerce security.

Bibliography

Baltimore Technologies. "An Introduction to PKI Based e|Security". September 14, 2000. URL: http://www.baltimore.com/solutionsplus/pki/index.html (November 15, 2000)

Bhimani, Anish. "PKI: Be Careful What You Wish For…". May 2000. URL: http://www.infosecuritymag.com/may2000/pki.htm (November 14, 2000)

Entrust Technologies. "Trusted Public-Key Infrastructures", v1.2. August 2000. URL: http://www.entrust.com/resourcecenter/pdf/pki.pdf (November 14, 2000)

McKinley, Barton. "The ABCs of PKI", January 17, 2000. URL: http://www.nwfusion.com/research/2000/0117feat.html (November 14, 2000)

Schneier, Bruce; Ellison, Carl. "Ten Risks of PKI: What You're not Being Told About Public Key Infrastructure". Date N/A. URL: http://www.counterpane.com/pki-risks.pdf (November 14, 2000)