Chapter II

Digital Certificates and Public-Key Infrastructures

Diana Berbecaru, Politecnico di Torino, Italy
Corrado Derenale, Politecnico di Torino, Italy
Antonio Lioy, Politecnico di Torino, Italy

ABSTRACT

The technical solutions and organizational procedures used to manage certificates are collectively named Public Key Infrastructure (PKI). The overall goal of a PKI is to provide support for usage of public-key certificates within – and also outside – its constituency. To this aim, several functions are needed, such as user registration, key generation, certificate revocation and many others. It is the aim of this paper to describe issues related to digital certificates and PKIs, both from the technical and management viewpoint.

INTRODUCTION

In 1976, Diffie & Hellman introduced the concept of public-key (or asymmetric) cryptography in their paper “New Directions in Cryptography”. This kind of cryptography uses a pair of mathematically related keys to perform the encryption and decryption operations. One key is named the “private key” and is known only to its owner, while the other key is named “public key” and must be publicly known. Public-key cryptography is a quantum leap in the field of security because it offers a better solution to several old problems: data and party authentication, privacy without a shared secret and key distribution.
The full range of benefits of public-key cryptography can be obtained only when there is assurance about the entity associated to the public key being used; that is the entity that controls the corresponding private key. To this purpose, members of small groups of communicating parties can meet face-to-face and directly exchange their public keys, for example on labelled floppy disks, and then ensure that these keys are securely stored on each user’s local system. This is usually known as manual key distribution (Ford & Baum, 1997), but it is seldom used outside small closed groups because it is highly impractical. Another approach is to aggregate the keys into a so-called “public file” (i.e., the list of keys and associated entities), managed by a trusted entity that makes it publicly available. This solution has its own problems too: the file is insecure and can be manipulated, the trusted entity is a single point of failure (the whole system fails if it gets compromised or access to it is denied) and the whole approach doesn’t scale well.

A better solution would be to bind the public key to the controlling entity on an individual basis and protect this binding with some cryptographic measure. To this aim, Loren Kohnfelder, in his MIT Bachelor thesis (1978), proposed to use a signed data structure named public-key certificate (PKC). Webster’s Dictionary defines a certificate as a “document containing a certified statement, especially as to the truth of something” (Webster’s New Collegiate Dictionary, 1980).

The Kohnfelder’s approach leaves open the issue about the signer of the certificate. This could be a user Alice that would digitally sign Bob’s public key along with Bob’s name and other accessory information. The result would be Bob’s certificate, which could convince anyone who trusts Alice that Bob’s public key really belongs to him. This is the approach taken by some certification systems, such as PGP (Garfinkel, 1995) in which a certificate is signed by all the users that vouch for the data contained in the certificate. However this approach is unpractical, relies on personal judgement and doesn’t scale well. Thus, usually the role of certificate signer is taken by a specialized entity named Certification Authority (CA) that handles the certificates on behalf of its constituency and takes some sort of liability for having performed the necessary trust and security checks. When no privacy issue exists, the certificates are published in appropriate repositories (such as a web server or a LDAP directory) to make them widely available. Since a certificate is digitally signed information, it is intrinsically secure and no other specific security measure is needed when it is stored or downloaded from the repository.

When a third party accepts a certificate as part of a security measure to protect a data exchange with a PKI user, he plays the role of a relying party (RP) because he relies on the issuer to have provided accurate data inside the certificate.

In the remainder of the chapter we deal with certificate formats, standards, and certificate management principles.
The Contribution of Serious Games for the Success of Students in Entrepreneurship
www.igi-global.com/chapter/the-contribution-of-serious-games-for-the-success-of-students-in-entrepreneurship/237668?camid=4v1a