Chapter 27

CERTIFICATE AUTHORITIES

INTRODUCTION

Have you ever used a credit card to buy something on the Internet? Then you've probably used both a CA and PKI, without even knowing it. The PKI comes in because you really need somebody to confirm that the site you're on is the site you think it is. That is, say the site claims to be amazon.com. How do you know it really is the one and only amazon.com? Otherwise you might be on a phishing site typing your card info in for the convenience of somebody who'd like nothing better than spending your hard-earned money. You trust the CA to verify that the site is who it claims to be (see sidebar, "What Are Certificate Authorities?"). Ah, but how do you know to trust the CA? Well, your browser knows to trust it because it has a copy of its public key installed with the browser. How can you trust your browser? Well, you did get it from a reputable source, didn't you? This may seem a bit paranoid, but that's the first rule in thinking about security and trust [1].

What Are Certificate Authorities?

In cryptography, a certificate authority or certification authority (CA) is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CA's are characteristic of many public key infrastructure (PKI) schemes.

There are many commercial CAs that charge for their services. Institutions and governments may have their own CAs, and there are free CAs.

Issuing A Certificate

A CA will issue a public key certificate which states that the CA attests that the public key contained in the certificate belongs to the person, enterprise, server, or other entity noted in the certificate. A CA's obligation in such schemes is to verify

an applicant's credentials, so that users (relying parties) can trust the information in the CA's certificates. The usual idea is that if the user trusts the CA and can verify the CA's signature, then they can also verify that a certain public key does indeed belong to whoever is identified in the certificate.

If the CA can be subverted, then the security of the system breaks down. For example, suppose an attacker, Mallory, manages to get a certificate authority to issue a false certificate tying Alice to the wrong public key, which corresponding private key is known to Mallory. If Bob subsequently obtains and uses the public key in this certificate, the security of his communications could be compromised by Mallory – for example, his messages could be decrypted, or he could be tricked into accepting forged signatures.

Security

The problem of assuring correctness of match between data and entity when the data are presented to the CA (perhaps over an electronic network), and when the credentials of the person/company/program asking for a certificate is likewise presented, is difficult. This is why commercial CAs often use a combination of authentication techniques including leveraging government bureaus, the payment infrastructure, third parties databases and services, and custom heuristics. In some enterprise systems, local forms of authentication such as Kerberos can be used to obtain a certificate which can in turn be used by external relying parties. Notaries are required in some cases to personally know the party whose signature is being notarized; this is a higher standard than can be reached for many CA's. According to the American Bar Association outline on Online Transaction Management, the primary points of federal and state statutes that have been enacted regarding digital signatures, has been to "prevent conflicting and overly burdensome local regulation and to establish that electronic writings satisfy the traditional requirements associated with paper documents." Further the E-Sign and UETA code help ensure that:

1. A signature, contract or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form.
2. A contract relating to such transaction may not be denied legal effect, validity or enforceability solely because an electronic signature or electronic record was used in its formation.

In large-scale deployments Alice may not be familiar with Bob's certificate authority (perhaps they each have a different CA), so Bob's certificate may also include his CA's public key signed by a different CA_2, which is presumably recognizable by Alice. This process typically leads to a hierarchy or mesh of CAs and CA certificates [2].