A public key infrastructre based on the SPKI/SDSI certificate system with peer to peer storage

Henry Mortimer

May 2017

Contents

1 Introduction

1.1 Problem

One of the major problems with public key cryptography is one of trust. If you want to encrypt a message to someone or receive a signed message from someone and want to verify the signature you need their public key. If you know the person in real life it is trivial to aquire their public key as you simply meet up and exchange the key file via a USB stick or something and you can be certain the public key belongs to the other person.
If you have never met the person you wish to communicate securely with it is much harder to establish this trust. It is fairly easy to aquire other peoples public keys over the internet. For example many people have their public keys available for download from their personal websites but you still cannot be sure the key belongs to the owner of the site as their server could have been compromised and configured to serve the wrong key or if the site is served over an insecure connection an attacker could intercept the key download and insert their own key instead.
Another way of distributing keys is via key servers. Various organiastions run key servers that allow people to upload their PGP public key to the server and possible associatig it with a name and email address. Others can then search for keys using the name, email address or key hash. Many of these key servers perform no verification that the key is actually associated with the name and email provided. Also should the server become compromised the attacker they would be able to replace keys on the server with their own keys.
The main solution to the problem is to distribute the keys with certificates. The certificates are issued by a third party and attest that a key is associated with a name, email address, domain etc.
A system that can create, mamage, distribute and authorise keys and certificates and known as a public key infrastructre (PKI). There are currently two widely used paradigms: A hierarchical sytem using certificate authorities (CA) and a decentralized web of trust.

Certificate Authorities A certificate authority based system uses hierarchical approach where certain trusted entities are designated as certificate authorities (CA) who can verify the identity of a user (Alice) then issue a certificate attesting to this. A separate user (Bob) can then verify the identity of Alice if the certificate is signed by a CA Bob trusts or a CA Bob trusts has delegated authority to the CA who signed Alice's certificate.
This system is most commonly used when accessing a web server over HTTPS. The server presents.

With certificate authorities there is a single point of failure in the system. If a certificate authorities private key is compromised by an attacker then they are able to issue certificates as if they are the certificate authority enabling them to impersonate the identity of anyone to people who trust the compromised CA.

Web of Trust A web of trust opts for a more decentralized approach. Any user in the system can create certificates for any other user in the system. If a user Alice wants to verify the identity of a user Bob and Alice has a certificate for Bob signed by Charlie if Alice trusts Charlie to identify users then Alice trusts the identity of Bob.
In a web of trust users can be faced with the problem of new users to the system to be able to get enough other users to endorse their identity as authentic. This leaves them unable to participate in the system as no other users will trust their public key.