Trustability of certificates

Alexandre Kervadec

***Abstract*—This paper is inspired from E.Gerck "Overview of Certification systems: X.509, CA, PGP and SKIP" [1]**

I. SKIP, X.509, CAs and PGP

A. SKIP (Simple Key-Management for Internet Protocol)

[...]

B. X.509 and CAs

Description of the different entities

1. CA : can be public (like banks with clients), commercial (like Verisign) or private (like internal departement of a compagny, to log user) 2. Subscriber : sends some infos to the CA to add it to his certificate 3. User : ask infos to CA(s), it's central to the process, since the user party is relying on the informations and is thus at risk

Concerns about the authentification services provided by CAs

1. The content of a certificate needs to be discussed, as well as certificate revocation 2. Issues about DN (Distinguished Name) and CA : a user can possess one or more DN, and use one or more DN on one or more DN 3. Validation of the user, using an ID, which is easily subject to fraud

Going deeper with user validation : DN scheme based on X.500 Recomendation, but it is not completly defined, and will (in 1998) probably not be. Also, X509 certification depends on many others such as ISO, ANSI, ITU and IETF. Thus lead to a lack of harmonization. Plus, there is a big problem with CPS (Certification Practice Statements), that also can be seen such as flexibility (for pros), because each CA answer specific needs, so no harmonization again.

Some kind of conclusion about harmonization (lack of), in a world wide vision.

C. PGP

PGP [1], created thanks to Phil Zimmermann researches.

[Schema] It is based on the *web-of-trust*, if the client doesn't know a CA which gave him a certificate, he ask to the PGP ring. In that ring, even if the client doesn't know everyone, someone will know him, thus the web-of-trust principle. Each member of the ring have a trust evaluation of CAs. If the client knows someone he trust that trust the CA he doesn't know, then he accept the certificate and trust the CA. But if the client trust someone who doesn't trust the CA, he reject the CA. The big point is when nobody knows the CA, and when trusted friends of the client have a medium evaluation of the CA : when to trust, when to reject, at which level of trust?

Tutor : A.Guermouche

[1] Pretty Good Privacy

References

[1] E.Gerck, Overview of Certification Systems: X. 509, CA, PGP and SKIP, 1998, http://www.blackhat.com/presentations/bh-usa-99/EdGerck/certover.pdf

[2] Oracle, SunScreen SKIP User's Guide, Release 1.1, 2010, http://docs.oracle.com/cd/E19957-01/805-5743/6j5dvnrfs/index.html