Trustability of certification systems

Alexandre Kervadec

***Abstract*—This paper is a synthesis of a E.Gerck's paper : *"Overview of Certification systems: X.509, CA, PGP and SKIP"*[1], but not only. It first gives an overview of (the mains) certification systems which are X.509 and CAs, PGP, SKIP, DANE and the Certificate transparency by Google, with thoughts on pros and cons of each system, on a technical point of view and about the government's stranglehold on data exchanges.**

I. Overview of certification systems

First sections talk about existing (sections I-A and I-B) or extinguished (section I-C) certification systems. Then, further sections (I-D and I-E) deals with new, not implemented yet, technologies of certification that may answer to current issues.

A. X.509 and CAs

X.509 and CAs[6] infrastructure is based on a directory method. With this kind of certification system, there are three different entities, which are :

1) **CA : Certification Authority**, an entity at controls the authentication services and the management of certificates. It can be public (like banks with their clients), commercial (like Verisign which sells its services) or private (like a compagny department, for an internal purpose).
2) **Subscriber :** the entity which sends informations to the CA to add it to his certificate. The entity is one that need to be trusted by the next entity (*user*).
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.

The main concerns about authentification services provided by CAs are :

- The content of a certificate needs to be discussed, as well as certificate revocation
- 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
- 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.

Tutor : A.Guermouche

B. PGP (Pretty Good Privacy)

PGP, created thanks to Phil Zimmermann researches.
[TODO : 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?

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

D. DANE (DNS-Based Authentication of Named Entities)

DANE is not implemented yet, but a IETF team is working on the standard.

E. Cetificate Transparency

Because of a case of Google CA's usurpation, Google is working on a new system that can improve certification systems.

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] Ashar Aziz, Tom Markson, Hemma Prafullchandra, Sun Microsystems, Inc., v.06, 1995. https://tools.ietf.org/html/draft-ietf-ipsec-skip-06
[3] Oracle, SunScreen SKIP User's Guide, Release 1.1, 2010. http://docs.oracle.com/cd/E19957-01/805-5743/6j5dvnrfs/index.html
[4] P Hoffman, J Schlyter, The DNS-based authentication of named entities (DANE) transport layer security (TLS) protocol: TLSA, 2012. https://www.rfc-editor.org/rfc/pdfrfc/rfc6698.txt.pdf
[5] Laurie, B., Langley, A., & Kasper, E. (2013). Certificate transparency (No. RFC 6962). https://www.rfc-editor.org/rfc/pdfrfc/rfc6962.txt.pdf
[6] Solo, D., Housley, R., & Ford, W. (1999). Internet X. 509 public key infrastructure certificate and CRL profile. http://tools.ietf.org/html/rfc2459