Certificate Chains

Somesh Jha

Imagine that an employee `Bob` works for a company `MSFT`. The following question arises in *public-key infrastructures (PKIs)*.

How does `Bob` prove to `Alice` that his public-key is pk_B?

Consider the following *certificates* or *certs*:

- $c_{V \to M}$: this is a signed statement by `Verisign` that "`MSFT`'s public-key is pk_M". Recall the for signing a statement you need the secret key, so only `Verisign` can sign this statement.
- $c_{M \to B}$: this is a signed statement by `MSFT`) that "`Bob`'s public-key is pk_B".

Now `Bob` presents $\langle c_{V \to M} c_{M \to B} \rangle$ (called *cert-chain*) to `Alice`, who verifies it as follows:

1. Uses the public key pk_V of `Verisign` to verify $c_{V \to M}$ and extract `MSFT`'s public key pk_M. We assume that everybody (including `Alice`) *trusts* that `Verisign`'s public key is pk_V.
2. Uses pk_M to verify $c_{M \to B}$ and extract `Bob`'s public key pk_B.

X.509 is a standard for certs and has a lot more information than what was described before (e.g., expiration date). Details can be found here: `https://en.wikipedia.org/wiki/X.509`
CRLs : *Ceritifcate Revocation Lists (CRLs)* are essentially a "databases" of certificates that have been revoked for some reason (e.g., they were misused). If the cert is in a CRL, it should *not be accepted*.