Foundations of Computer Security

Lecture 55: Certificates II

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Certificates and Trust

Certificates address the need for constructing a *web of trust* in computer systems: *How do mutually suspicious entities establish a relationship of trust?*

One way is to rely on a known third party to "vouch for" one or both of the parties.

In a digital context, this typically means certifying the binding between identity and public key.

Chains of Trust

Suppose Y has a certificate signed by X, but Y now needs to certify W. He might produce a certificate for W and append X's certificate to it.

This creates a chain of trust from W to Y to X.

Ideally, the chain is rooted at some unimpeachable authority.

Certification Authorities

An entity may gain authority to certify by virtue of position, rather than familiarity.

In off-line transactions this might be a notary public, personnel officer, security officer in a company, etc.

On the Internet, several groups serve as "root certification authorities": Verisign, SecureNet, Baltimore Technologies, Deutsche Telecom, Certiposte, and several others.

X.509 Certificates

X.509 is a widely followed standard for digital certificates. An X.509v3 certificate has the following components:

1. *Version:* version of X.509 used;
2. *Serial number:* unique among certificates issued by this issuer;
3. *Signature algorithm identifier:* identifies the algorithm and params used to sign the certificate;
4. *Issuer's distinguished name:* with serial number, makes all certificates unique;
5. *Validity interval:* start and end times for validity;
6. *Subject's distinguished name:* identifies the party being "vouched for";
7. *Subject's public key info:* identifies algorithm, params, and public key;

X.509 Certificates (Cont.)

8. *Issuer's unique id:* used if an Issuer's distinguished name is ever reused;
9. *Subject's unique id:* same as field 8, but for the subject;
10. *Extensions:* version specific information;
11. *Signature:* identifies the algorithm and params, and the signature (encrypted hash of fields 1 to 10).

To validate the certificate, the user:

- obtains the issuer's public key for the algorithm (3);
- verifies the signature (11);
- recompute the hash and compare with the received value;
- check the validity interval.

Lessons

- Certificates can be combined to produce a chain of trust.
- To be useful the chain must be rooted in a trusted authority.
- X.509 is a widely followed international standard for certificates.

Next lecture: Cryptographic Protocols