PKI (part 1) summary

zondag 8 januari 2023 10:23

Hybrid encryption entails the use of asymmetric cryptography to securely exchange a symmetric session key.

PKI tasks:

- Key availability
- Key authenticity
- Key validity

Public key certificates bind public keys to subjects. The binding is asserted using the signature of a trusted CA. Usually, certificates have a (time) validity constraint and can be revoked.

Direct trust either verifies keys directly with the owner or obtains the keys directly from the owner. Its main downside is that it scales very poorly. However, it can be used to obtain keys for initial trusted parties (i.e. CAs)

PGP

Key validity: is the key owner's identity correct?
Owner trust: is the key owner reliable (i.e. trusted to sign other keys correctly)?

Key validity is computed from the trust in corresponding signers, ***only considering*** signers with key validity *complete* (or better).

Complete is assigned when the key is signed by at least one user with owner trust complete, or by at least x users with owner trust marginal.
Marginal is assigned when the key is signed, but by less than x users with owner trust marginal.
Unknown is assigned when the key is signed by no one with owner trust at least marginal.

Owner trust is computed from the owner trust of signers, where only *ultimate* valid keys are considered.

Issues in PGP

- People often do not upload signatures
- Key servers leak your email address and information about your network

Revocation in PGP

Revocation is done by uploading a key revocation certificate, which can be generated using the private key.

X.509

Trust models for multiple hierarchies

1. Trusted list: every participant has a list of trusted CAs.
2. Common root: there is one root which signs all trusted CAs.
3. Cross-certification: root (or intermediate) CAs sign each other's certificates.
4. Bridge CA: a bridge CA is trusted by CAs in the system and then further delegates trust to other parties

Certificate path validation

Shell model: all signatures (leading up to the root certificate) must be valid at verification time.
Modified/hybrid model: all signatures must have been valid at the point where the signature closest to the verifier in the chain was made
Chain model: all signatures must have been valid at the point where they were made.

X.509 critical extensions

	Critical	**Non-Critical**
Known	valid	valid
Unknown	invalid	valid

Key usage and extended key usage

"*If a certificate contains both a key usage extension and an extended key usage extension, then both extensions MUST be processed independently and the certificate MUST only be used for a purpose consistent with both extensions. If there is no purpose consistent with both extensions, then the certificate MUST NOT be used for any purpose.*"

Certificate policy (CP) states what policy should be complied with.
Certificate practice statement (CPS) states how to comply.