PUBLIC KEY INFRASTRUCTURE (PKI)

Purpose, Methods, Revocation, PKIX

Purpose of PKI

- To distribute public keys securely
- Requires
  - *Certificates* and *Certification Authorities*
  - Method for *retrieving certificates*
  - Method for *revoking certificates*
  - Method for evaluating certificates from *trust anchors*

Chain of Certificates

- A needs D's public key
- A trusts B
- A receives C's certificate from B and signed by B
- C signs D's certificate
- A accepts D's certificate signed by C since its trust anchor B has vouched for C

Terminology in PKIs

- A is the *subject* of its own certificate
- If A's certificate is signed by B, then B is the *issuer*
- A chain of certificates is evaluated by the *verifier* or *relying party*
- Any owner of a public key is a *principal*
- A *verifier* trusts a *trust anchor* to sign certificates

PKI Trust Models

- Monopoly
- Monopoly plus registration authorities
- Delegated Certification Authorities
- Oligarchy
- Anarchy
- Name Constraints
- Bottom-up with Name Constraints
- Name Constraints in Certificates
- Policies in Certificates

Monopoly

- One CA acts as trust anchor for all principals
- Public key of CA embedded in all principal hardware
- Problem of finding single object of trust
- Secure registration problematic
- CA private key compromise presents severe security problem

Monopoly plus Registration Authorities

- Single CA signs all certificates but registration authorities verify registration details
- Like monopoly model requires single object of trust
- CA private key compromise presents severe security problem

Delegated CAs

- Single trusted CA issues certificates for delegates
- Certificates confirm delegate keys and their suitability to act as delegated CAs
- Still requires a single object of trust
- Similar security issues to monopoly model

Oligarchy

- Principals are configured with many potential trust anchors
- Any certificates issued by configured trust anchors would be accepted
- Less secure than monopoly model since total security compromised if any configured trust anchor is compromised
- Exposure to rogue trust anchors
- Used by web browsers

Anarchy

- Each principal configures own trust anchors
- To find path to distant party search database for links
- Problem with scale
- Problem of trust in loose chain
- Used in Pretty Good Privacy (PGP)

Name Constraints

- CA trusted for subset of users
- e.g. Imperial CA would be trusted for name@imperial.ac.uk but not for name@eng.oxon.ac.uk
- User might have several names but one public key confirmed by each CA
- May be configured top-down like monopoly with delegates with each delegate with own namespace

Name Constraints (Bottom-Up)

- Use common ancestor or cross-links
- e.g. name@imperial.ac.uk to name@eng.oxon.ac.uk could use common ancestor (.ac.uk) or a crosslink from imperial to oxon
- Proposed by Digital (Compaq) and similar to that used by Lotus Notes
- A root service may be used to link organisations in absence of cross-links

Name Constraints and Policies in Certificates

- Name Constraints – PKIX allows issuer to specify what names subject can be trusted to certify
- Policies in Certificates –used by Privacy Enhanced Mail (PEM) in which single root CA issued certificates to multiple hierarchies each with its own security policy

Revocation

- Revocation of certificate required if
  - private key compromised
  - principal no longer in position of trust
- Certificates have expiration times so that certificate revocation list (CRL) is manageable

Revocation Mechanisms

- Delta CRLs – publish latest revocations and not complete list
- On-line Revocation Server (OLRS) for complete list of revocations
- OLRS could issue “not revoked at time” certificate to ease congestion at server

PKIX and X.509

- X.500 is ITU-T Directory Service
- PKIX specifies options in X.509
- IETF based certificate format on X.509
- S/MIME and SSL use X.509 certificates

X.509 and PKIX Certificates

- Version – 3 versions defined
- Serial number – integer and CA name is unique ID
- Signature – specifies algorithm
- Issuer – X.500 name of CA
- Validity – start-time and end-time
- Subject – X.500 name of subject
- Subject Public Key – algorithm used and public key
- Encrypted (PKIX Signature Value) – signature on above fields

X.509 and PKIX CRLs

- Signature – as in certificate
- Issuer – as in certificate
- This Update – time CRL was issued
- UserCertificate –serial no. of revoked certificate
- RevocationDate – time certificate was revoked
- Encrypted – the signature on above fields