Presented by Joshua Schiffman & Archana Viswanath

Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure – By Carl Ellison and Bruce Schneier
Trust Models

Rooted Trust Model
- In a rooted trust model, the root CA is the trust anchor and has a self-signed certificate.
- The root CA issues a certificate to all direct subordinate CAs, if needed, which, in turn issue certificates to their subordinate CAs. A subordinate CA is trusted cryptographically, based on the signature of its parent.

Network Trust Model
- In a network trust model, all CAs are self-signed and trust relationships between CAs are based on cross-certificates. Cross-certificates establish trust between unrelated CAs.

Hybrid Trust Model
- It is a combination of the above two models.
- Certain CAs are cross certified and certain others are rooted trust models.
Keys

Risk – “Who is using my key?”
- Safety of Private Key at user end
  - Is the key encrypted?
  - Is the user computer protected?
  - Is the computer virus-free?
- Basis of PKI – Non – Repudiation
  - The user is held responsible for all transactions executed with his key.
Keys

Risk – “Which John Robinson is he?”
Certificates associate name with a public key

- May end up getting the public key of somebody you don’t want to correspond with.
- Principal recognition through names is not a good approach.
- In cryptography, X.509 is an ITU-T standard for public key Infrastructure (PKI).
- X.509 specifies standard formats for public key certificates.
# Keys

## Structure of a certificate

The structure of a X.509 v3 is as digital certificate is as follows:

Certificate:

- **Version** – Version of the certificate in X.509
- **Serial Number** – This along with the Issuer name forms the primary key of the certificate.
- **Algorithm ID (Signature)** – This specifies the algorithm used to compute the signature.
- **Issuer** – The name of the issuing CA.
- **Validity**
  - Not Before – The time the certificate becomes valid.
  - Not After – The time until when the certificate is valid.
- **Subject** – The entity who is being certified.

**Subject Public Key Info**

- Public Key Algorithm
- Subject Public Key

**Issuer Unique Identifier** (Optional) – Uniquely identifies the issuer of this certificate.

**Subject Unique Identifier** (Optional) - Uniquely identifies the subject of this certificate

Extensions (Optional) ...(AuthorityKeyIdentifier, SubjectKeyIdentifier(hash of subject’s public key), PrivateKeyUsagePeriod, etc.)
Certificate Revocation Lists

Certificate Revocation List (CRL) is a list of all the unexpired, revoked certificates.

- **Revocation Mechanisms**
  - Delta CRLs – The latest additions to the revoked CRLs
  - First Valid Certificate (Issued with Serial numbers)
    - These have no expiration date.
    - They have a field called FIRST VALID CERTIFICATE field which differentiates valid from invalid certificates.
  - Online Revocation Server – It is a system that can be queried over the net about the revocation status of individual certificates.
  - Good Lists vs Bad Lists
Risk – “How Secure are the certificate practices?”
- How is key lifetime computed?
  - Cryptographic lifetime – The lifetime during which the key can be used for encryption.
  - Theft lifetime – a function of the system’s vulnerability, the rate of physical and network exposure, attractiveness of the key to an attacker, etc.
- Are Certificate Revocation Lists supported?
  - How is compromise of a key detected in order to trigger revocation?
  - Are the signatures made by the user dated in order to distinguish between good and bad ones in the event of compromise.
  - User’s responsibility – To check that he is communicating with the right principal as indicated by the certificate.
Risk – “Is the User part of the security design?”
- Does the application using the certificates take the user into account or does it concern itself only with cryptography?
  • It is the onus of the user to decide whether to shop on an SSL-protected web page.
  • The certificate that is issued is for the URL and not for the content the URL hosts.
Users

“Why are we using the CA process anyway?”
• Usability Issues – Limitations – Single Sign On
• CA authenticity issues.
• Mapping principal to public key issues
• Certificate validity issues

CONCLUSION :
• PKI is a commercial money making venture used for communication between unknown principals.