PKI Risks, Experience
Summary & Lessons Learned

Papers:
- Ten Risks of PKI: What You’re not Being Told about Public Key Infrastructure – Carl Ellison and Bruce Schneier
- PKI: It’s Not Dead, Just Resting - Peter Gutmann
- Deploying and Using Public key Technology: Lessons Learned in Real Life- Guida, et al.

Presenter: Aparna Sharma

CS 6204, Spring 2005
Ten Risks of PKI

- Risk #1: “Who do we trust, and for what?”
- Risk #2: “Who is using my key?”
- Risk #3: “How secure is the verifying computer?”
- Risk #4: “Which John Robinson is he?”
- Risk #5: “Is the CA an authority?”
- Risk #6: “Is the user part of the security design?”
- Risk #7: “Was it one CA or a CA plus a Registration Authority?”
- Risk #8: “How did the CA identify the certificate holder?”
- Risk #9: “How secure are the certificate practices?”
- Risk #10: “Why are we using the CA process anyway?”
The problem with X.509 style PKI:
- generic all-purpose identity certificates issued by third-party CAs.
- Hierarchical directory structures, offline revocation instead of relational databases, non-hierarchical organizations & online validity/authorization checking

The solution:
- Adapt PKI design to real world rather than constraining the real world to match PKI
Identity Certificates

Problems

- “Which directory?” problem
  - Include any certificates that might be needed with the signature.

- “Which John Smith?” problem
  - SPKI – SDSI names as an identifier to provide global uniqueness.
  - PGP – Identifier consisting of email address and user name.
  - X.509 – Local naming scheme crammed with information.

- Revocation
Revocation

♦ CRLs violate the rule of data-driven programming which is once you have emitted a datum you can’t take it back.

♦ **Accuracy** - indicated revocation time should be the time reported by the user (backdated revocations)

♦ **Consistency** - indicated revocation time should be the time of CRL issue.
Problems with CRLs

♦ Fetching a CRL

♦ Time taken to fetch a CRL

♦ How frequently should CRLs be issued?

♦ No real mechanism for charging fees for revocation checking
Workarounds for CRL shortcoming

- Issue CRLs that don’t expire at the same time
- Segment CRLs based on urgency of revocation information
  - E.g. “Key compromised” CRLs issued more frequently than “affiliation change” CRLs.
- Delta CRLs
- SET cardholder certificates
- AADS - ssh key management system
- SPKI- revalidation, representing a positive assertion
- Use of extremely short lived certificates
- Application-specific approach
Online Revocation Authorities

Figure 2: X.509 certificate usage model

Figure 3: Certificate usage model with OCSP responder
OCSP: Problem & Solutions

♦ “Has this been revoked?” vs. “Is this currently valid?”- vagueness in the response

- Simple Certificate Validation Protocol (SCVP) has a full certificate chain validation system

- Data Validation & Certification Server Protocol (DVCS)
  • Third-party data validation
Certificate Chains

♦ Path construction
♦ Trustworthy CAs in the chain
♦ Certificate Revocation-OCSP
♦ “Which directory?”- Path Construction Servers (PCS)

Figure 5: CRL-based revocation checking for a chain of length 3

Figure 6: Offloading the revocation checking process
Bypassing Revocation Checking & Certificates

**Figure 7: Avoiding revocation checking**

**Figure 8: Avoiding certificates altogether**
PKI Design Recommendations

♦ **Identity**- combination of locally meaningful and globally unique identity info.

♦ **Revocation**
  - Avoid revocation
  - Avoid revocation checking
  - Online status query mechanism
  - Use of CRLs when info. is of little or low value

♦ **Application-Specific PKI**
Deploying and Using PKI: Lessons learned

- Shifting user paradigms
  - users need to know how their environment & standard operations would change.
- Helping the help desks
  - Estimating the number of users calling for help
- Anomalous Cryptographic service provider behavior
  - Make the user interface contain unambiguous commands
- CRL
  - Easy to underestimate CRLs projected size
- What to do when you get new certificates
  - Identity credential change have many consequences
- CRL caching behavior
  - Be prepared to deal unexpected behavior
- Language barriers
  - Can’t restrict to English as the information-management language