A Model of Trust Evaluation for X.509 Certificate

Abu Shohel Ahmed
NordSecMob, University of Tartu
How to identify an anonymous persons in online or virtual world?

Whom to Trust
Overview

- Digital Certificate & Public Key Infrastructure
- X.509 Certificate Fields
- Trust in Certificate Authority policy
- Proposed Trust Evaluation Technique
Digital Certificate

- "A digital certificate is an electronic document which uses a digital signature to bind together a public key with an identity" — wiki
PKI allows us to know that a given key belongs to a given user.
<table>
<thead>
<tr>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Create a public/private key pair</td>
</tr>
<tr>
<td>2. Send a Certificate Signing Request.</td>
</tr>
<tr>
<td>3. Provide your identity</td>
</tr>
<tr>
<td>4. Get the signed certificate from CA</td>
</tr>
<tr>
<td>5. Publish certificate</td>
</tr>
</tbody>
</table>
How Validation Works

- Certificate validation chain
- Checking against OCSP or CRL
X.509 Certificate

Certificate format defined by IETF

Some important fields:

- Key Usage
- Certificate Policy
- Name Constraint

  Policy Identifier=2.16.840.1.113733.1.7.23.6
  [1,1]Policy Qualifier Info:
    Policy Qualifier Id=CPS
    Qualifier: https://www.verisign.com/rpa
Extended Validated Certificate

- A special type of X.509 certificate that requires more extensive investigation of the requesting entity
- Based on certificate policy mapping field.
Certificate Authorities

- A set of trusted entities known as Certificate Authorities (CAs) are established to sign certificates.
- X.509 certificate delegates trust in certificate to CA.
Where is Trust in Certificate

- Certificate is granted based on two documents
  1. Certificate policy
  2. Certification practice statement

But who will evaluate these policy and actual CA practice?
How to automate trust evaluation process from this document?
Trust evaluation in CA policy

Some previous research:
- Criteriata for certificate trust requirements
- Certificate practice statement formalization or semi-formalization.
- Platform for Internet Content Selection rating service
Introduction of a trust level in certificate fields. (currently defined in CP)

Semi-formalization of CPS document
## Comparison

<table>
<thead>
<tr>
<th>Solution</th>
<th>Advantage</th>
<th>Disadvantage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPS semi formalization</td>
<td>Processing is performed using local knowledge which means applications can independently evaluate a certificate.</td>
<td>Trust evaluation is based on weak assumptions (e.g., counting MUST). Requires online request to get CPS file.</td>
</tr>
<tr>
<td>CPS formalization</td>
<td>Provides more accurate information about the CPS file.</td>
<td>CPS has no common standard. Requires an online request for CPS file.</td>
</tr>
<tr>
<td>Ratings service</td>
<td>Flexible and easy to find rating for a certificate. Provides a clear direction about a certificate.</td>
<td>Trust depends on the independent auditing authority. Requires an online request to get rating information.</td>
</tr>
</tbody>
</table>
Proposed Evaluation Model

- Based on all the best known Trust solution for certificate.
- Rating based system.
- Stepwise – Modular
- Incorporate online and offline evaluation
Discussion

- Model can be used for trust evaluation in most of the cases.
- Model is extendable with other rating feature.
- Mapped with VirtualLife identification strategy.
Questions
References

- Gabriel A, Weaver, Scott Rea, Sean W, and Smith. A computational framework for certificate policy operations. In Dartmouth College Hanover, NH03755, USA