Distributed Identity Management in the PGP Web of Trust

Daniel Margolis
Faculty Advisor: Professor Matt Blaze

Abstract

The aim of this project is to allow users to exchange keys in a reliable manner, without the use of a certifying trusted third party, by use of extended trust paths and automated trust metrics.

Procedure

Key Storage is accomplished by way of a central keyserver, just as in the existing PGP system.

Key signatures include not just an endorsement but two numerical representations of trust, both in the range [0, 1]: key trust, the signer’s estimation of the key’s validity, and principal trust, the signer’s estimation of the key holder’s trustworthiness.

Clients retrieve trust paths from the server, verify their certificate signatures offline, and calculate the total trust for a given key using their chosen trust metric, avoiding imposters and (hopefully) choosing the correct key.

Implemented trust metrics:

- **Strongest path** (product of edge weights)
  - trust = 0.504

- **Disjoint paths** (sum of disjoint path weights)
  - trust = 0.554

- **Network flow** (flow capacity from start to sink)
  - trust = 0.8

Analysis shows us which desired properties each algorithm satisfies.

Desired properties:

1. Longer paths are weaker
2. Paths passing through weak edges are weaker
3. Disjoint paths add value
4. Constraint on amount of damage a single false trust can inflict

<table>
<thead>
<tr>
<th>Property</th>
<th>#1</th>
<th>#2</th>
<th>#3</th>
<th>#4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strongest path</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Disjoint paths</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Network flow</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Testing was conducted in a simulated web of trust derived from the actual PGP strongly connected set, with artificial edge weights assigned in a random normal distribution. High standard deviations and even distributions of trust are preferred. We can also see the correlation between trust strength and path length and the number of disjoint paths between the start key and end key.