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:

- The web of trust is the graph representing key signatures granted by users validating each others’ keys. Each node in the graph represents a principal (i.e. user), and each edge a key signature.

- A key signature is an endorsement by one user indicating that a key belongs to another user, i.e. an assertion that a unique key belongs to a certain non-unique (and forgeable) identity (name, e-mail, etc.).

- A trust path is a sequence of key signatures that leads from a starting, trusted key (the key of the user querying) to an end key (the key the user is trying to validate). Trust paths are comprised of multiple edges from the web of trust.

- A trust metric is an algorithm that can analyze the structure of a given trust path and determine how reliable it is (i.e. how likely it is that the key at the end is valid).

- 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

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.