Trust in Distributed Systems

- Tyrone W. A. Grandison

Supervisors: Prof Morris Sloman and Dr Naranker Dulay

Outline

- Definition
- Motivation
- Properties of trust and trust relationships
- Trust classification
- Trust management solutions
- Future work
Definition

- The contemporary approach

My Definition

“The firm belief in the reliability, truth and competence of an entity and its transmissions”

- Reliable, dependable, honest, secure, competent and timely

Attributes that relate to trust:

- What are trustors and trustees?

Motivation

- The need for a universal way to specify and monitor trust.
- Domain Navigation.
- Remove trust complexity from application layer.
- Enable E-Commerce.
- Risk.
Properties

- Constraints on trusted actions.

  *I believe that you will find a way to bridge this gap*

Properties

- Trust levels.

  *I have to admit that I do trust the manual system more*
The issue of transitivity.
Not symmetrical.
A trust relationship can be:

Properties

- One-to-One
- Many-to-One
- One-to-Many
- Many-to-Many

Trust Classification

Access to Trustor Resources

“The trustor trusts a trustee to use resources that he owns or controls”

- Resource Access Trust can be refined into authorisation policies.
- Resources may be anything from trustor’s services to trustor software environment.
Trust Classification

Provision of Service by the Trustee

“The trustor trusts the trustee to provide a service that does not involve access to the trustor’s resources”

Forms of Service Provision Trust: Confidence, Competence & Reliability

Certification

“The trustor trusts the trustee based on certification from a third party about the trustee’s trustworthiness”

Certification is actually a special form of service provision trust.
Trust Classification

Delegation

“The trustor trusts the trustee to make decision(s) on its behalf, with respect to a resource or service that the trustor owns or controls”

Micky delegates all decisions concerning his investments to his financial advisor.

Delegation is also a special form of service provision trust - a trust decision-making service.

Trust Classification

Infrastructure Trust

“The trustor’s trust in its infrastructure”

I hope this tight rope holds.
Trust Management Solutions

Current Solutions include:
- Public Key Certificates
- PICS (Platform for Internet Content Selection)
- IBM Trust Establishment Framework
- PolicyMaker and KeyNote
- REFEREE

The problem with current solutions
- N-Time Solutions - i.e. run once or at the coder’s discretion, do not learn, believe calling applications unconditionally, suggestion-oriented, no monitoring.

Trust Management Solutions

Public Key Certificates
- “Who is the owner of this public key?”
- A third party vouches for key-name validity.
# Trust Management Solutions

## Public Key Certificates

- Address authentication (public-key-to-name binding), but leaves determination of access rights to application.
- Two more popular certificate frameworks: PGP and X.509
- PGP’s informality is good for email, but not E-Commerce, X.509 may lead to unnatural alliances.
- Both suffer from expiry problems.

## PICS

- A solution to the problem of protecting children from pornography, without compromising freedom of speech.
- Developed by MIT WWW Consortium. PICS defines standards for format and distribution of labels.
- PICS doesn’t stipulate a label vocabulary nor state which labels are important. It merely defines standards for stating ratings services and rating systems.
- There is an associated policy language, PICSRules.
A Very Simple PICS Rules Statement

(PicsRule-1.1)
(Policy (RejectByURL ( "http://@*www.doc.ic.ac.uk/*/" ))
(Policy (AcceptIf "otherwise")
)

A PICS Label

(PICS-version 1.1)
(rating-system "http://www.doc.worldwide.com/ratings")
nlabels on "1998.11.05T08:15-0500" until "1999.09.30T23:34-0000"
for "http://www-dse.doc.ic.ac.uk/~per/index.html"
by "Tom Green"
ratings (rc "a lot")
)

A PICS Rating Service

(PICS-version 1.1)
(rating-service "http://www.doc.worldwide.com/descrip.html")
(icon "icons/good.gif")
(name "The Computing Department Rating System")
description "All about the rating of the pages offered by
computing departments all over the world")
)

PolicyMaker

Seek to solve a problem with public key certificates.

“What is a public key authorised to do?”

PolicyMaker is a query engine. It accepts local policy,
a set of credentials and an action string from a calling
application.

Policies and credentials are assertions.

An assertion is of the form:

Source ASSERTS AuthorityStruct WHERE Filter
Examples of assertions:

<table>
<thead>
<tr>
<th>Policy</th>
<th>BMA_key</th>
</tr>
</thead>
<tbody>
<tr>
<td>policy ASSERTS doctor_key WHERE filter that allows check-up if the field is not plastic surgery</td>
<td>BMA_key ASSERTS “0x12345” WHERE filter that returns “not a plastic surgeon”, if the field is not plastic surgery</td>
</tr>
</tbody>
</table>

- Policymaker has no standard assertion language.
- Filters are interpreted programs.
- Filter language is external to PolicyMaker.

The format of a PolicyMaker query is:

\[
key_1, key_2, key_3, \ldots \quad \text{REQUESTS} \quad \text{ActionString}
\]

- Action strings are application-specific.
- Example of a query:
  
  “0x12345” REQUESTS “do check-up”

- PolicyMaker tries to prove that the credentials contain a proof that the requested actions(s) compiles with the policy.
## Future Work

- Composing Trust Classes
- Conflict Detection and Resolution resulting from Trust Class Composition
- Formulation of a generic trust establishment framework
- Trust Enforcement, Monitoring and Management
- Implementing a Trust Specification Language
- Implementing a Trust Management System