

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”

- Attributes that relate to trust:

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

- 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.



Properties



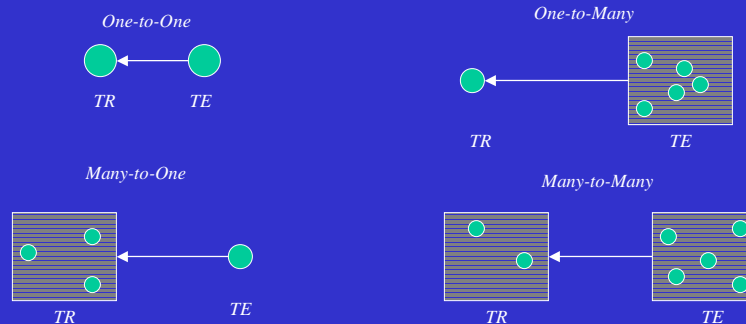
- Trust levels.



Properties



- The issue of transitivity.
- Not symmetrical.
- A trust relationship can be:

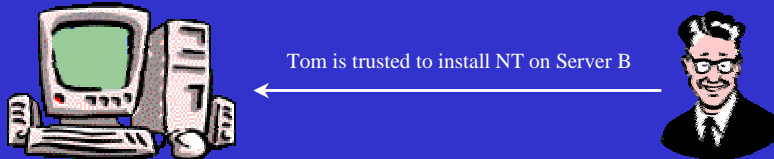


Trust Classification



- Access to Trustor Resources

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



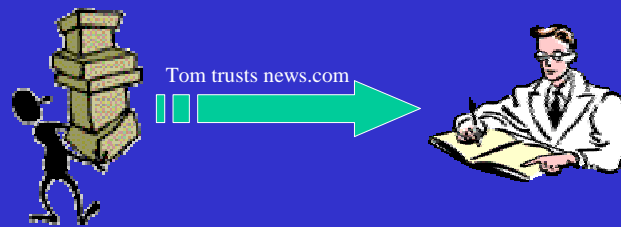
- Resource Access Trust can be refined into authorisation policies.
- Resources may be anything from trustor's services to trustor software environment.

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”



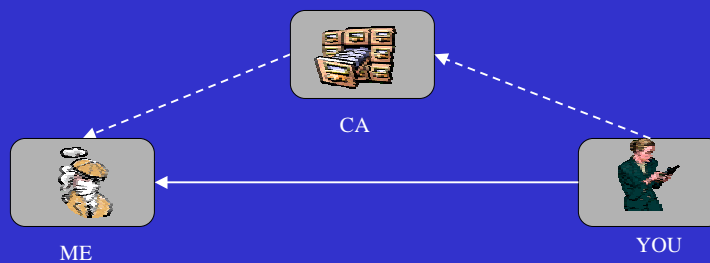
- Forms of Service Provision Trust: Confidence, Competence & Reliability

Trust Classification



● Certification

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



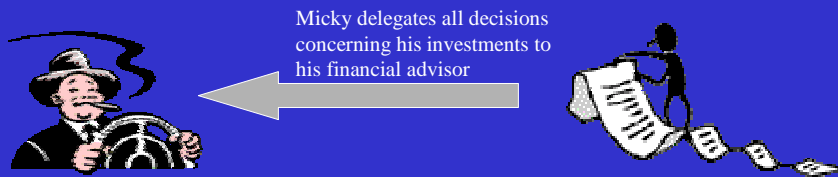
- Certification is actually a special form of service provision trust.

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”



- 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”



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.

Trust Management Solutions



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.

Trust Management Solutions



PICS

A PICS Rating Service

```
( (PICS-version1.1)
(rating-system "http://www.doc.worldwide.com/ratings/")
(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")
( category
(transmit-as rc)
(name "Research Content")
(label (name "very little") (value 0) (icon "icons/little.gif") )
(label (name "a lot") (value 1) (icon "icons/lots.gif") )
)
)
```

A PICS Label

```
( (PICS-version1.1)
"http://www.doc.worldwide.com/descrip.html"
labels 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 Very Simple PICS Rules Statement

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

Trust Management Solutions



PolicyMaker

- Seeks 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

Trust Management Solutions



PolicyMaker

- Examples of assertions:

policy ASSERTS doctor_key WHERE filter that allows check-up if the field is not plastic surgery	BMA_key ASSERTS "0x12345" WHERE filter that returns "not a plastic surgeon", if the field is not plastic surgery
---	---

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

Trust Management Solutions



PolicyMaker

- The format of a PolicyMaker query is:

key₁, key₂, key₃, REQUESTS *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