Trust Management and Theory Revision

Ji Ma

School of Computer and Information Science
University of South Australia

24th September 2004, presented at SKM

Outline

- Motivation (background, aims etc)
- A brief introduction to the logic TML
- Theories of trust
- Modeling the dynamics of trust
- A methodology for theory revision
- Conclusion and future work

Trust and Belief

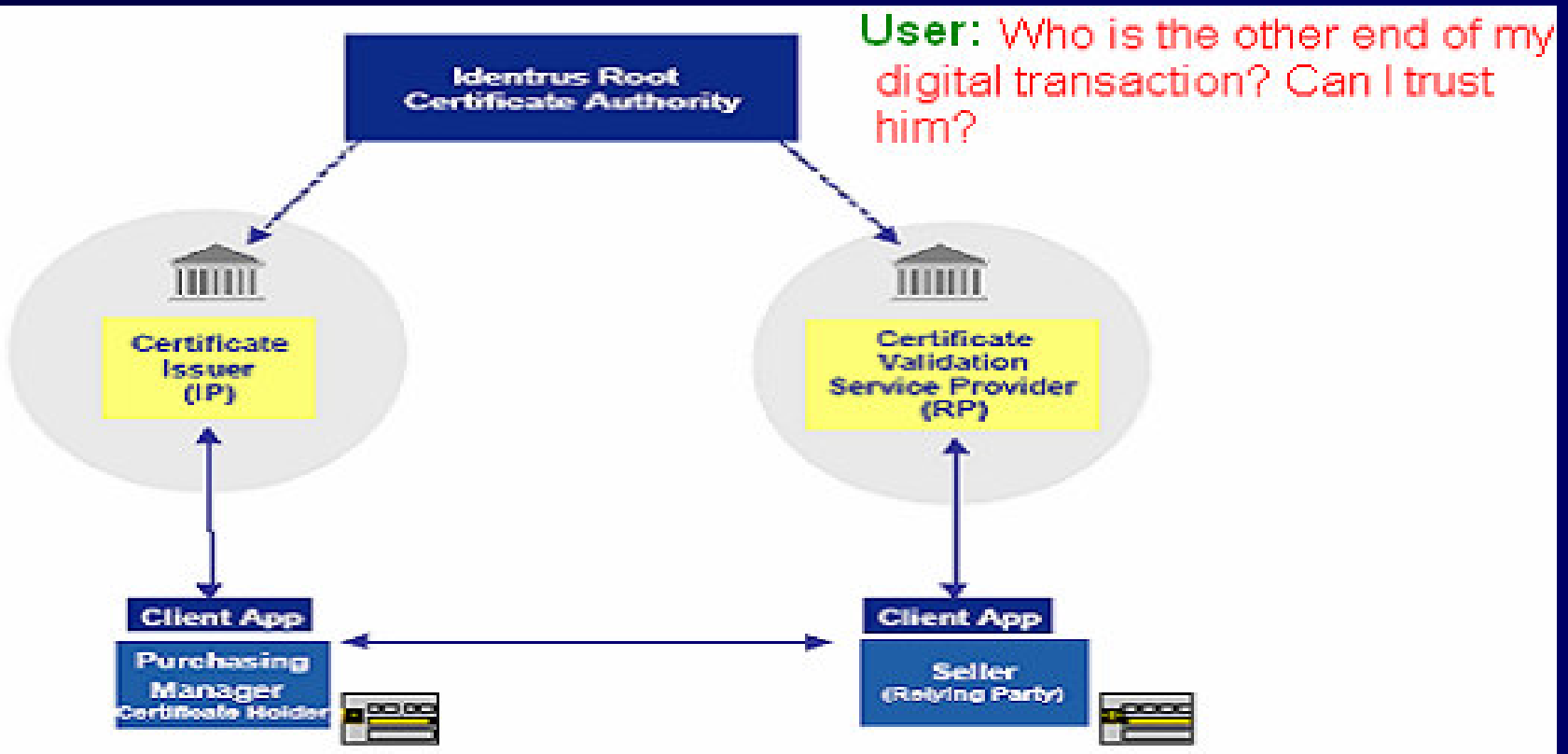
Trust and trust management are important issues for digital communication systems.

Some general questions regarding trust and agent belief such as:

- Can I trust the system?
- Is the message received through the system reliable?

Trust and Belief (con't)

- Every security system depends on trust



Recently Research Work on Trust

Most of the work focus on:

- Trust concept: What is trust?
  (Dimitrakos 2001, Kini & Choobineh 98)
- Specification of trust and reasoning
  (Liu 2001, Liu & Ozols 2002, etc)
- Trust management
  (Blaze 93, Yahalom *et al*. 93, Josang 2000)

But not many papers focused on a dynamic theory of trust

Trust Theories

- The concept of trust theory is proposed for the specification of trust (Liu 2001) .
- A trust theory is a set of rules describing trust of agents in a system, and
- established based on the initial trust of agents in a system.

Need to revise a trust theory?

- Trust changes dynamically
- A theory is constructed based on the initial trust of agents in the system, therefore,
- When agents lose their trust in dynamic environment, the theory need to be revised, otherwise it can no longer be used for any security purpose

Aims of Our Work

- Investigate factors that influence trust
- Provide methods and techniques for modeling the dynamics of trust
- Obtain a general approach to revising and managing a theory of trust for an agent-based system

Contributions of this Paper

In this paper, we propose

- A method for modeling trust changes and an algorithm to compute the trust state
- A method for modeling theory changes
- A technique for computing the new theory based on trust changes
- A framework for managing a theory of trust

TML logic - What is it?

- TML is an extension of the first-order logic with
  - typed variables, and
  - multiple belief operators

- Belief operator $\mathbf{B}_i$ stands for "agent *i* believes that".

- Every variable must be typed, i.e., it ranges over a certain domain.

Why TML?

We choose TML, because of

- Its expressive power: TML can express agent beliefs in a natural way.
- any security system depends on agent beliefs.

Example: If we have

$\mathbf{B}_{john}$ Has(bob, key)

$\mathbf{B}_{john}$ (Has(x, key) $\rightarrow$ MayRead(x,doc))

Then, we may derive that

$\mathbf{B}_{john}$ MayRead(bob, doc).

Multi-agent Systems

- Agents can be human beings, machines, a program, a method or any other entities.
- Agents may have their goals, intentions, beliefs, obligations etc.
- They may perform actions (co-operatively sometimes) in a society of other agents.

Trust Model and TrustTheory

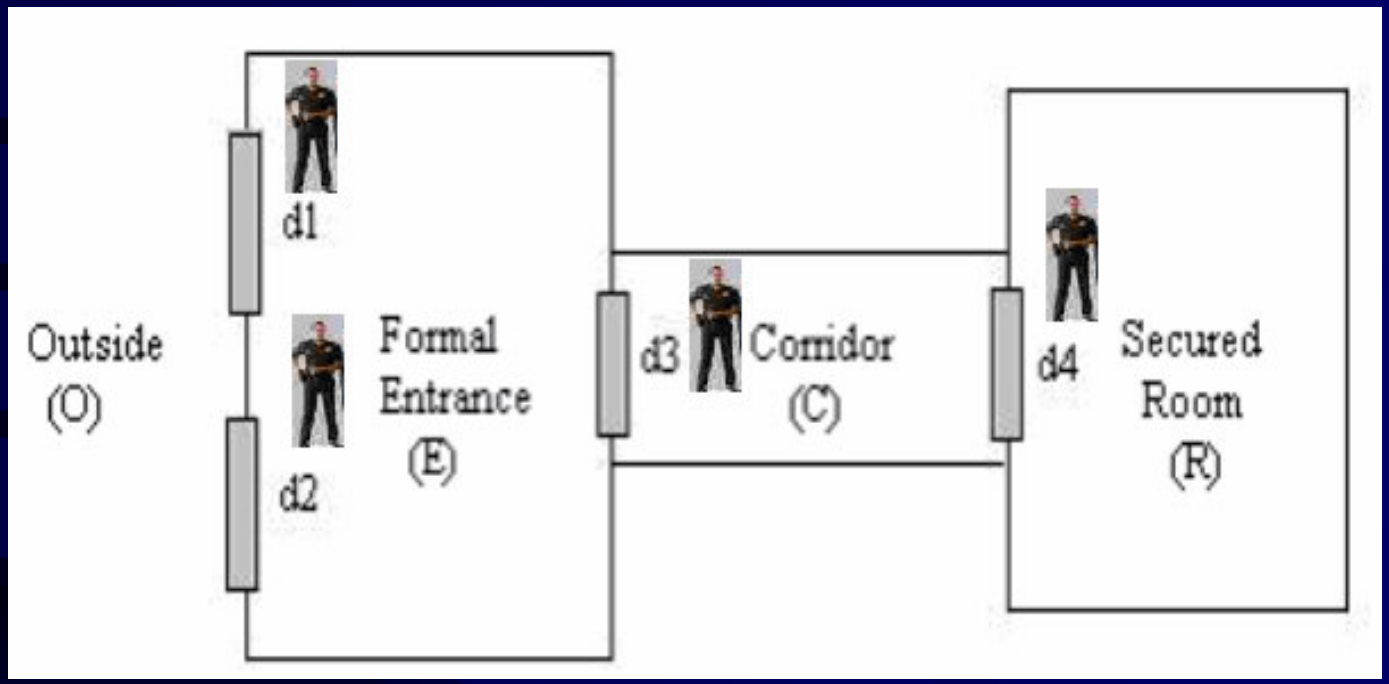
- Simple trust model (Liu & Ozols, 2002):

  An agent does not trust anyone but the security mechanisms (as special agents) of the system.

- For reasoning about beliefs, the key is to obtain rules specifying such trust.

- Those rules form a theory, we called it a *trust theory*.

An example – A secured room
(A multi-agent authentication system)



- Agents: a1, a2, a3, a4 control doors d1,d2,d,3,d4 respectively.
- Authentication methods: m1 (for d1) ,m2 (d2) ,m3 (d3), m4 (d4)

An example – A secured room (con't)

- security mechanisms of the system include:

  1. agents a1, a2 a3 and a4,
  2. the authentication methods m1, m2, m3 and m4
  3. the physical security environment (consisting of doors and walls), denoted as pse.

Thus, agents have an initial trust set:

{a1, a2, a3, a4, m1, m2, m3, m4, pse}.

An example – A secured room (con't)

- Trust of agents includes:

1. trust that a1, a2 a3 and a4 are capable of performing their functions as required;

2. trust that these authentication methods are reliable;

3. trust that there is no problem with pse on the security objective

Building a Theory for the System

Define Predicates:

- At(*x, l, t*) : *x* is at the location *l* at time *t*,
- ReqToEnter(*x,l*) : *x* requests to enter the location *l*.
- AuthBy(*x,m*) : the identity of *x* is authenticated by *m*.

Building a Theory for the System (con't)

- Rules describing the functions of agents a_1, a_2, a_3,, a_4:

(r1) $\mathrm{At}(x,\mathrm{O},t) \wedge \mathrm{ReqToEnter}(x,\mathrm{E},t) \rightarrow (\mathrm{At}(x,\mathrm{E},t+1) \leftrightarrow (\mathbf{B}_{a1}\ \mathrm{AuthBy}(x,\mathrm{m1}) \vee \mathbf{B}_{a2}\ \mathrm{AuthBy}(x,\mathrm{m2})))$.

(r2) $\mathrm{At}(x,\mathrm{E},t) \wedge \mathrm{ReqToEnter}(x,\mathrm{C},t) \rightarrow (\mathrm{At}(x,\mathrm{C},t+1) \leftrightarrow \mathbf{B}_{a3}\ \mathrm{AuthBy}(x,\mathrm{m3}))$.

(r3) $\mathrm{At}(x,\mathrm{C},t) \wedge \mathrm{ReqToEnter}(x,\mathrm{R},t) \rightarrow (\mathrm{At}(x,\mathrm{R},t+1) \leftrightarrow \mathbf{B}_{a4}\ \mathrm{AuthBy}(x,\mathrm{m4}))$.

Building a Theory for the System (con't)

- Rules related to pse are:

(r4) $At(x,O,t) \rightarrow At(x,O,t+1) \vee At(x,E,t+1)$.

(r5) $At(x,E,t) \rightarrow$
$At(x,E,t+1) \vee At(x,O,t+1) \vee At(x,C,t+1)$.

(r6) $At(x,C,t) \rightarrow At(x,C,t+1) \vee At(xE,t+1) \vee At(x,R,t+1)$.

(r7) $At(x,E,t) \wedge At(x,E,t+1) \wedge At(x,E,t+2) \rightarrow At(x,O,t+3)$.

(r8) $At(x,C,t) \wedge At(x,C,t+1) \wedge At(x,C,t+2) \rightarrow At(x,E,t+3)$.

Thus, we have the theory:

T ={r1, r2, r3, r4, r5, r6, r7, r8}

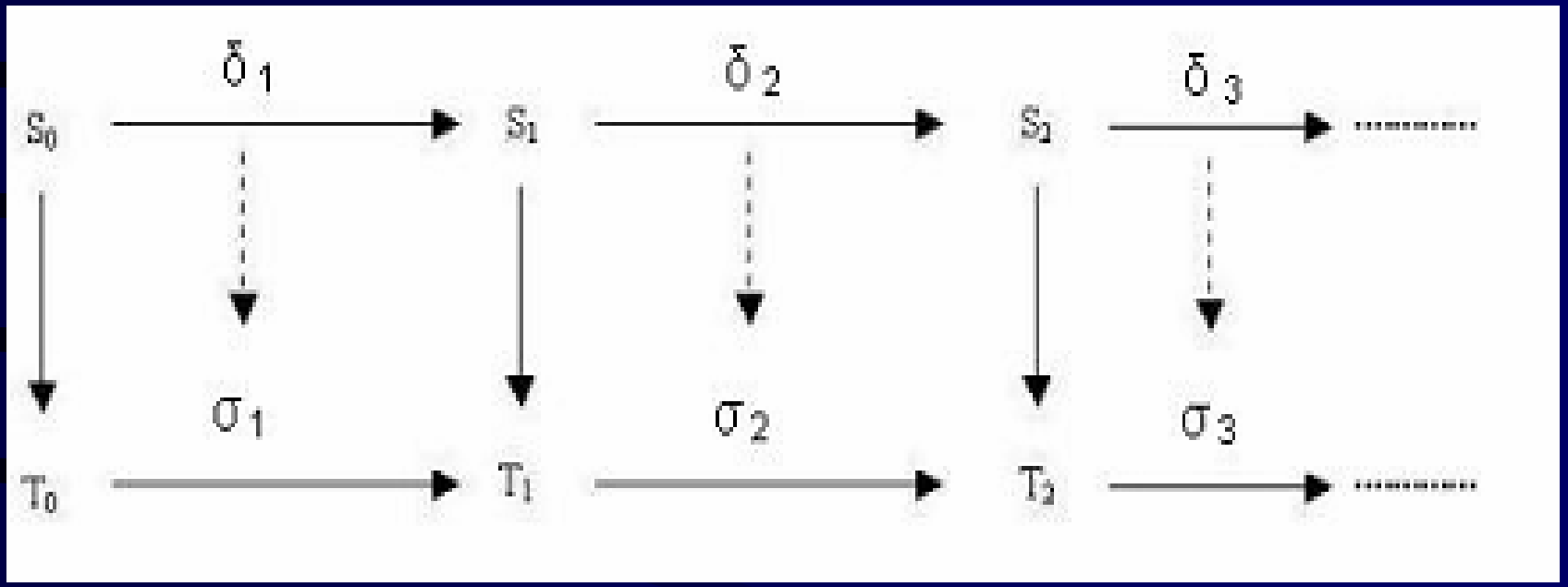
The Dynamics of Trust

Trust changes dynamically. It depends on many factors:

– Modification of the security policy
– Replacement of security mechanisms
– Movement of employees
– Interaction between agents
– accidents

……

Trust Change Vs Theory Change



Questions:

- How to model trust change?
- How to express a theory change?
- How to obtain the new theory?
- How to find the theory change based on trust changes?

Modeling Trust Changes

- Trust state:

  S = **(**Ω,Θ), where
  - Ω is the set of agents involved in the system,
  - Θ is a trust relation over Ω.

- A trust change to the state S includes two classes of operations:
  - deleting a pair (*x*,*y*) from Θ
  - adding a pair (*x*,*y*) to Θ

Modeling Trust Changes (con't)

- We say that $\delta = (IN, OUT)$ is a trust change to the state $S = (\Omega,\Theta)$, if
  - $OUT \subseteq \Theta$
  - $IN \cap \Theta = \varnothing$
- Assume that the set of agents Ω is always static, then the new trust state $S' = (\Omega,\Theta')$, where

$$\Theta' = \Theta + IN - OUT,$$

Theory Revision

- Two types of activities:
  - $\oplus \varphi$: adding a formula φ to a theory
  - $\circledR \varphi$: retracting a formula φ from a theory

- Let T be a theory and $\sigma = <*_1 \varphi_1, \ldots, *_n \varphi_n >$ be a theory change to T, where $*_i$ is $\oplus$ or $\circledR$. Then, the new theory is:

$$T' = T \circ \sigma = T *_1 \varphi_1 \cdots *_n \varphi_n .$$

Theory Revision (con't)

Minimal change technique:

- $T \oplus \varphi$ -- is proceeded in two steps: first remove just enough formulas from T to obtain a theory T' such that T' is consistent with φ; then add φ to T'.

- $T \circledR \varphi$ -- is proceeded in this way: take out the formulas from T to get T' such that $T' \nvdash \varphi$ and T' is an exactly the subset of T that cannot be expanded without φ.

Theory Revision (con't)

Example

Suppose $T = \{p \vee q \rightarrow r, r \rightarrow s\}$ and a theory change $\sigma = \langle \oplus p, \circledR(r \rightarrow s), \oplus s \rangle$, then the new theory is

$T' = T \circ \sigma = \{p \vee q \rightarrow r, p, s\}$

Finding Theory Changes

To answer question 4, let H be the set of trusted agents at a state S = (Ω,Θ), and δ =(IN, OUT) the trust change to S. Then the theory change σ to T can be obtained as follows:

- For any $x \in$ H,if there exists a pair $(y,x) \in$ OUT and a rule *r* related to *x*, then ® *r* is added to σ.

- For any agent *x*, x $\notin$ H, but $(y,x) \in$ IN for all $y \in \Omega$, and if *r* is a rule specifying the function of *x*, we will add ⊕ *r* to σ.

An Example

Let T_0 = {r1,r2,r3,r4,r5,r6,r7,r8} at the state S_0. If m1 is not reliable and door d1 is permanently closed. Therefore, we have a theory change σ = <®r1 >.

But, for retracting r1 from T_0, we need to add the following formula to it:

(r9) $At(x,O,t) \wedge ReqToEnter(x,E) \rightarrow$
$(At(x,E,t+1) \leftrightarrow \mathbf{B}_{a2}\ AuthBy(x,m2))$.

Therefore, the new theory
T_1 = {r2,r3,r4,r5,r6,r7,r8,r9}

Conclusion and Future Work

- We have presented a formal approach to revising a theory of trust.
- These methods and techniques could be useful in the specification and management of trust for any systems with communicating agents.

- Future works
  - Case studies, finding more applications.
  - Trust degree refinement in theory revision
  - Investigation of ways to express security properties based on evolving theories of trust.

Thanks

Any Question?

Email:MAYJY005@students.unisa.edu.au