
This version is available at https://strathprints.strath.ac.uk/2588/

Strathprints is designed to allow users to access the research output of the University of Strathclyde. Unless otherwise explicitly stated on the manuscript, Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Please check the manuscript for details of any other licences that may have been applied. You may not engage in further distribution of the material for any profitmaking activities or any commercial gain. You may freely distribute both the url (https://strathprints.strath.ac.uk/) and the content of this paper for research or private study, educational, or not-for-profit purposes without prior permission or charge.

Any correspondence concerning this service should be sent to the Strathprints administrator: strathprints@strath.ac.uk

http://eprints.cdlr.strath.ac.uk/2588/

This is an author-produced version of a paper from the Second UK-UbiNet Workshop.

Strathprints is designed to allow users to access the research output of the University of Strathclyde. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. Users may download and/or print one copy of any article(s) in Strathprints to facilitate their private study or for non-commercial research. You may not engage in further distribution of the material or use it for any profitmaking activities or any commercial gain. You may freely distribute the url (http://eprints.cdlr.strath.ac.uk) of the Strathprints website.

Any correspondence concerning this service should be sent to The Strathprints Administrator: eprints@cis.strath.ac.uk
Trust Lifecycle Management in Ad-hoc Collaborations

Sotirios Terzis

Sotirios.Terzis@cis.strath.ac.uk
University of Strathclyde
A Ubiquitous Computing Environment

- **The characteristics of the environment**
  - A plethora of computational entities with a need for collaboration
  - Significant variation in the supporting infrastructure
  - A highly changeable set of potential collaborators

- **Ad-hoc collaborations become the norm**
  - Entities cannot rely on the availability of particular infrastructure
  - Entities need to collaborate with little known or even unknown entities

- **Entities need to decided who to collaborate with**
  - Collaborations are unavoidable and can be dangerous
    - Collaborations may have both costs and benefits
  - Decisions need to be taken autonomously and despite the lack of complete information about potential collaborators
Trust in Ad-hoc Collaborations (1)

- The human notion of trust seems appealing as a basis for entity decision making
  - Despite the difficulty in defining trust, certain characteristics are apparent and appealing
    - Trust is subjective in nature - disposition
    - Trust is situation specific
    - Trust evolves over time in the light of experience
  - Trust propagation is a desirable property

- The goal is to use trust as the mechanism for managing the dangers/ risks of collaboration
  - Trust conveys information about likely behaviour
  - Virtual anonymity: identity conveys little information about likely behaviour
  - Entity recognition as a superset of authentication
Trust in Ad-hoc Collaborations (2)

- **Entity recognition versus authentication**

<table>
<thead>
<tr>
<th>Authentication Process (AP)</th>
<th>Entity Recognition (ER)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1. Enrollment: generally involves an administrator or human intervention</td>
<td>E.1. Triggering (passive and active sense): mainly triggering (as in A.2), with the idea that the recognizing entity can trigger itself</td>
</tr>
<tr>
<td>A.2. Triggering: e.g. someone clicks on a Web link to a resource that requires authentication to be downloaded</td>
<td>E.2. Detective work: to recognize the entity to-be recognized using the negotiated and available recognition scheme(s)</td>
</tr>
<tr>
<td>A.3. Detective work: the main task is to verify that the principal’s claimed identity is the peer’s</td>
<td>E.3. Retention (optional): “preservation of the after effects of experience and learning that makes recall or recognition possible” [30]</td>
</tr>
<tr>
<td>A.4. Action: the identification is subsequently used in some ways. Actually, the claim of the identity may be done in steps 2 or 3 depending on the authentication solution (loop to A.2)</td>
<td>E.4. Action (optional): the outcome of the recognition is subsequently used in some ways (loop to E.1)</td>
</tr>
</tbody>
</table>
Trust in Ad-hoc Collaborations (3)

- Credential-based versus evidence-based trust management
  - Implicit view of trust as delegation of privileges to trusted entities
    - Avoid the issues of what trust is made of, how it is formed
    - Very restricted view of trust evolution – certificate revocation
  - Explicit view of trust as likely entity behaviour on the basis of the history of past interactions

- Trust lifecycle management is key to a trust-based model for ad-hoc collaborations
  - Need for explicit modelling of risk
  - Need for a trust model supporting trust formation, evolution and propagation
  - Need for a decision making process that relates the trust and risk models and incorporates entity recognition
The SECURE Collaboration Model (1)

- **A trust model**
  - A trust domain with a trustworthiness and an information ordering
    - An “unknown” trust value representing lack of information
    - A local trust policy that assigns trust to principals and may reference other principals

- **A risk model**
  - Trust mediated actions with a set of possible outcomes
  - Each outcome with an associated cost/benefit
  - Risk as the likelihood of an outcome occurring combined with its associated cost

- **The relationship between trust and risk**
  - Trust determines the likelihood of the outcomes
  - Trustworthy principals make beneficial outcomes more likely
  - Access right-based versus behaviour-based trust models
The SECURE Collaboration Model (2)

- **Collaboration decision making**
  - Collaboration request → Entity recognition → Entity trust assignment → Collaboration risk assessment → Collaboration policy application → Decision

- **Trust evaluation**
  - The result of multiple interactions with the same entity
  - Monitoring of collaboration → Production of evidence about entity’s behaviour → Evidence processing → Update entity’s trust value

- **Risk evaluation**
  - The result of multiple instances of similar interactions with different entities
  - Monitoring of collaborations → Production of evidence about outcome costs → Evidence processing → Update outcome costs/benefits
The SECURE Collaboration Model (3)

- Evidence of entities’ past behaviour
  - Direct evidence results from a personal interaction with an entity - observations
    - Unquestionable in nature, treated as fact
  - Indirect evidence results from entities communicating their experiences from personal interactions with a particular entity to other entities – recommendations (trust values)
    - Subjective in nature, its value depends on the source
    - Trust in the recommender & recommendation adjustment

- Evidence processing
  - Evaluate evidence with respect to the current trust value → Evolve the current trust value in accordance to the evidence evaluation
The SECURE Collaboration Model (4)

- **Evidence evaluation in terms of Attraction**
  - Attraction is a measure of the effect evidence has to the current trust value
  - The trust domain determines the direction of the attraction
    - In terms of trustworthiness can either be positive or negative
    - In terms of information can either be reinforcing or contradicting
  - The risk domain determines the measure of the attraction
    - The more different the associated profiles of likely behaviour the stronger the attraction

- **Trust value evolution**
  - In the form of a trust evolution or trust update function
  - Encodes dispositional characteristics: trusting disposition & trust dynamics

Evidence evaluation in terms of

www.smartlab.cis.strath.ac.uk
The SECURE Collaboration Model (5)

- **Operational issues**
  - An architecture with the following component
    - Trust Lifecycle Manager
    - Collaboration Monitor
    - Evidence Gatherer
    - Evidence Store

- **Trust Information Structure**

  \[
  \begin{array}{c|c|c}
  \hline
  & T_{ov} & \\
  \hline
  (Stored or combined from the layer below) & & \\
  \hline
  T_{obs} & T_{rec} & \\
  \hline
  \text{Evidence Layer} & \text{Evidence Layer} & \\
  (Lists of all observations and received recommendations) & & \\
  \hline
  \end{array}
  \]
The SECURE Collaboration Model (6)

- **The formation of trust**
  - The “unknown” trust value
    - We always have an initial trust value
  - References in local trust policies
  - Recommendations
    - When using recommendations formation is the same to evolution with “unknown” as the current trust value
    - Approaches to evidence gathering
      - Initial list of recommenders, authorisation hints, ask neighbours for good recommenders, recommender brokers, broadcast
Food for Thought

- **Context as a situational modifier of trust**
  - Who and what are already elements of the decision making process
  - Explicit modelling of relationships between contexts are crucial
  - Different aspects of trust
    - Keep in mind the need for trust propagation

- **System trust**
  - Trust in the underlying infrastructure (e.g. recognition mechanism)
  - Taking into account available (security) infrastructure

- **The role of the user**
  - Introducing user into the trust loop

- **Trust and obscurity**
  - Security by obscurity should be avoided
  - Openness of trust policies opens the possibility of trust scams
Final Word

- SECURE is an EU FET project (IST-2001-32486)
  http://secure.dsg.cs.tcd.ie

- iTrust is an EU FET working group on Trust Management in Dynamic Open Systems (IST-2001-34810)
  http://www.itrust.uoc.gr
The e-purse scenario (1)

- The focus is on the bus company – passenger interaction
- The trust values are intervals \((d_1, d_2)\)
- The risk analysis
The e-purse scenario (2)

- **Trust evolution in the light of observations**
  - Observation – validity of e-cash
  - Observations adjust the boundaries of the intervals
    - Valid e-cash ⇒ positive attraction
    - Invalid e-cash ⇒ negative attraction
    - Expected outcome (i.e. probability > 50%) ⇒ reinforcing
    - Unexpected outcome ⇒ contradicting

<table>
<thead>
<tr>
<th>attraction direction</th>
<th>direction of boundary movement</th>
<th>interval size</th>
</tr>
</thead>
<tbody>
<tr>
<td>positive, reinforcing</td>
<td>→</td>
<td>$m_1 &gt; m_2$</td>
</tr>
<tr>
<td>positive, contradicting</td>
<td>→</td>
<td>$m_1 &lt; m_2$</td>
</tr>
<tr>
<td>negative, reinforcing</td>
<td>←</td>
<td>$m_1 &gt; m_2$</td>
</tr>
<tr>
<td>negative, contradicting</td>
<td>←</td>
<td>$m_1 &lt; m_2$</td>
</tr>
</tbody>
</table>

- If the amount of money is less than $d_1$ and the e-cash is valid we don’t really change the trust value
- We consider the level of positive and negative adjustment as dispositional parameters