Combining Access Control and Trust Negotiations in an On-line Social Network

Stefano Braghin   Elena Ferrari   Alberto Trombetta

Dipartimento di Informatica e Comunicazione
Università degli Studi dell’Insubria
Varese (Italy)

CollaborateCom2010
October 10th 2010
Overview

1. Problem statement

2. Introduction to On-line Social Network Access Control

3. Goals

4. Introduction to Trust Negotiation
   - Trust-$\chi$ framework

5. Proposed solution
   - Extension to the Access Control Protocol
   - Dynamic relationships
   - Trust Level Adjustment

6. Conclusions and future work
Problem statement

- The extensive use of On-line Social Networks for exchanging information and requesting or offering services requires to rethink the way access control is performed.
- Required to improve the flexibility of the access control conditions.
- The overwhelming number of interacting subjects creates management issues.
- Necessity to delegate the policies enforcement from servers to clients to reduce the load.
OSN $SN$ is a directed labeled graph $(V_{SN}, E_{SN}, RT_{SN}, \phi_{SN})$:

- supported relationship types $RT_{SN}$
- nodes $V_{SN}$
- edges $E_{SN} \subseteq V_{SN} \times V_{SN} \times RT_{SN}$
- $\phi_{SN} : E_{SN} \rightarrow [0, 1]$, a function assigning to each edge $E_{SN}$ a trust level $t \in [0, 1]$. 

**Diagram:**

- A -> B (colleagueOf, 0.8) (friendOf, 0.4)
- A -> D (colleagueOf, 0.5)
- A -> C (friendOf, 0.4)
- B -> C (colleagueOf, 0.3) (friendOf, 0.4)
- C -> D (colleagueOf, 0.3)
- C -> E (colleagueOf, 0.6) (friendOf, 0.4)
- C -> F (colleagueOf, 0.7) (friendOf, 0.4)
- D -> F (colleagueOf, 0.3)
- F -> A (friendOf, 0.8) (friendOf, 0.2)
Introduction to On-line Social Network Access Control

Model definition [Carminati, Ferrari and Perego]

OSN $SN$ is a directed labeled graph $(V_{SN}, E_{SN}, RT_{SN}, \phi_{SN})$:

- supported relationship types $RT_{SN}$
- nodes $V_{SN}$
- edges $E_{SN} \subseteq V_{SN} \times V_{SN} \times RT_{SN}$
- $\phi_{SN} : E_{SN} \rightarrow [0, 1]$, a function assigning to each edge $E_{SN}$ a trust level $t \in [0, 1]$. 

Braghin et al. (DICOM) Combining AC and TN in an OSN CollaborateCom2010 4 / 19
Access control is performed expressing constraints on OSN users graph

(A, colleagueOf, 2, *)

The resources owned by the nodes are protected by access control rule

(rid, \{(A, colleagueOf, 2, *), (D, colleagueOf, 1, 0.2)\})

Several access control rules can be associated with the same resource.
Access control is performed expressing constraints on OSN users graph

\[(A, colleagueOf, 2, *)\]

The resources owned by the nodes are protected by access control rule

\[(rid, \{(A, colleagueOf, 2, *), (D, colleagueOf, 1, 0.2)\})\]

Several access control rules can be associated with the same resource
Access control is performed expressing constraints on OSN users graph

\[(A, \text{colleagueOf}, 2, *)\]

The resources owned by the nodes are protected by access control rule

\[(\text{rid}, \{(A, \text{colleagueOf}, 2, *), (D, \text{colleagueOf}, 1, 0.2)\})\]

Several access control rules can be associated with the same resource
Access control is performed expressing constraints on OSN users graph

\[(A, \textit{colleagueOf}, 2, \ast)\]

The resources owned by the nodes are protected by access control rule

\[(\textit{rid}, \{(A, \textit{colleagueOf}, 2, \ast), (D, \textit{colleagueOf}, 1, 0.2)\})\]

Several access control rules can be associated with the same resource
Access control rules definition language

- Access control is performed expressing constraints on OSN users graph
  
  $(A, \text{colleagueOf}, 2, \star)$

- The resources owned by the nodes are protected by access control rule
  
  $\text{rid}, \{(A, \text{colleagueOf}, 2, \star), (D, \text{colleagueOf}, 1, 0.2)\}$

- Several access control rules can be associated with the same resource
Introduction to On-line Social Network Access Control

Access control protocol: a brief overview

1. \( R \) submits to \( O \) a request for \( rsc \)
2. \( O \) returns to \( R \) the set of access rules \( AR = \{AR_1, \ldots, AR_n\} \)
3. \( R \) chooses \( ar \in AR \) and sends \( AC(ar) \) to \( CS \).
4. \( CS \) returns \( R \) the set \( CP \) of shortest certificate paths related to \( AC(ar) \)
5. Based on \( CP \), \( R \) generates \( \pi \) and sends it to \( O \)
6. If the proof \( \pi \) is valid then \( O \) sends \( rsc \) to \( R \)
Goals

- Extension of the access control policy definition language to use resources as requirements
- Extension of the access control protocol using Trust Negotiations techniques
- Extension of the On-line Social Network model to support dynamic relationships
- Definition of a procedure for computing trust
In conventional systems access is managed via the identification of the subjects.

This is difficult in an environment in which many unknown subjects communicate among themselves.

A more flexible access control mechanism is required.
The idea is to provide a multicentric access control system
Based on:
- the attributes of the subjects and
- distributed policy statements
An explicit identification is not required
Challenges of the approach:
- Defining security credentials
- Policy language expressiveness
- Policy enforcement
Introduction to Trust Negotiation

Trust Negotiation

- Automated trust establishment
- Consists in an interactive process
- Trust is established gradually and **mutually**

- Subjects have their own credentials and policies
- They interact in order to determine whether there is a set of policies on which they agree
- Trust is established without involving trusted third parties other than credential issuers
Introduction to Trust Negotiation

A simple example of Trust Negotiation

P₁ \rightarrow P₂

Time

Braghin et al. (DICOM)
Combining AC and TN in an OSN
CollaborateCom2010
Introduction to Trust Negotiation

A simple example of Trust Negotiation

\[ P_1 \rightarrow R \rightarrow P_2 \]

\[ R \leftarrow C_1 \]

Braghin et al. (DICOM) Combining AC and TN in an OSN

CollaborateCom2010
Introduction to Trust Negotiation

A simple example of Trust Negotiation

\[ P_1 \xrightarrow{R} P_2 \]

\[ P_1 \xleftarrow{C_1} P_2 \]

\[ C_1 \leftarrow C_2 \land C_3 \]

\[ \text{Time} \]

Braghin et al. (DICOM) Combining AC and TN in an OSN CollaborateCom2010
Introduction to Trust Negotiation

A simple example of Trust Negotiation

P₁

Time

P₁

P₂

P₂

P₁

C₁ ← C₂ ∧ C₃

R ← C₁

C₂, C₃

C₁ ← C₁

?R

Braghin et al. (DICOM)

Combining AC and TN in an OSN

CollaborateCom2010
Introduction to Trust Negotiation

A simple example of Trust Negotiation
Introduction to Trust Negotiation

A simple example of Trust Negotiation
Introduction to Trust Negotiation

Trust-X

- A comprehensive XML-based system for TNs
- Initially developed at the University of Milano by Ferrari, Squicciarini and Bertino
- Further enhanced at University of Insubria
- Specifically designed for a P2P environment:
  - both parties are equally responsible for negotiation management
  - both can drive the negotiation process
  - each party is equipped with the same functional modules
  - can alternatively act as a requester or a resource controller
Introduction to Trust Negotiation

Trust-\( \mathcal{X} \): features

\( \mathcal{X} \)-TNL: policies and credentials specification language

\[
\text{AccessCred}(\text{Place} = "\text{Home}") \leftarrow \text{ID}(N = "\text{John}", S = "\text{Doe}") \land \text{Passwd}()
\]
\[
\text{BookOrder} \leftarrow \text{StudID}(\text{Inst} = "\text{Insubria}") \lor \text{WorkCred}(\text{Empl} = "\text{Insubria}")
\]

Trust-\( \mathcal{X} \) TN protocol

Three distinct phases:

- introductory
- policies evaluation
- credentials exchange
Introduction in the OSN access control language of resources as requirements:

\[ \text{rid}, \{(rsc', \{(att_1, =, 5), (att_2, <, 3))\}), (rsc'', \emptyset)\}] \]

Negotiation of required resource by means of parallel TN

TN does not replace the original access control protocol but extends it when dealing with resource requirements.
Extension of the Access Control Protocol

Introduction in the OSN access control language of resources as requirements

\( (\text{rid}, \{(rsc', \{(\text{att}_1, =, 5), \\( (\text{att}_2, <, 3)\}\}), (rsc'', \emptyset)\}) \)

Negotiation of required resource by means of parallel TN

TN does not replace the original access control protocol but extends it when dealing with resource requirements
Extension of the Access Control Protocol

- Introduction in the OSN access control language of resources as requirements $(rid, \{(rsc', \{(att_1, =, 5),
(\text{att}_2, <, 3)\}), (rsc'', \emptyset)\}))$

- Negotiation of required resource by means of parallel TN

- TN does not replace the original access control protocol but extends it when dealing with resource requirements
Dynamic relationships

- The access control procedure **locally** modifies the relationships between nodes.
- History of terminated interactions.
- For both interacting nodes for keeping track of:
  - who is willing to disclose a certain resource
  - who is safe to disclose to a certain resource
- Note that dynamic relationships expire over time.
The access control procedure **locally** modifies the relationships between nodes.

History of terminated interactions

For both interacting nodes for keeping track of

- who is willing to disclose a certain resource
- who is safe to disclose to a certain resource

Note that dynamic relationships expire over time.
Dynamic relationships

- The access control procedure **locally** modifies the relationships between nodes.
- History of terminated interactions.
- For both interacting nodes for keeping track of:
  - who is willing to disclose a certain resource
  - who is safe to disclose to a certain resource
- Note that dynamic relationships expire over time.
Dynamic relationships

- The access control procedure **locally** modifies the relationships between nodes
- History of terminated interactions
- For both interacting nodes for keeping track of
  - who is willing to disclose a certain resource
  - who is safe to disclose to a certain resource
- Note that dynamic relationships expire over time
Dynamic relationships

- The access control procedure **locally** modifies the relationships between nodes
- History of terminated interactions
- For both interacting nodes for keeping track of
  - who is willing to disclose a certain resource
  - who is safe to disclose to a certain resource
- Note that dynamic relationships expire over time
Takes advantage of the TN
- Each user assigns values to unprotected resources
- Policies structure further defines the value of the protecting resource
- The trust level is set to the aggregate value of the exchanged resources
- If the relationship exists the trust level is adjusted depending on the outcome of the TN
Trust level adjustment

- Takes advantage of the TN
- Each user assigns values to unprotected resources
- Policies structure further defines the value of the protecting resource
- The trust level is set to the aggregate value of the exchanged resources
- If the relationship exists the trust level is adjusted depending on the outcome of the TN
Trust level adjustment

- Takes advantage of the TN
  - Each user assigns values to unprotected resources
  - Policies structure further defines the value of the protecting resource
  - The trust level is set to the aggregate value of the exchanged resources
  - If the relationship exists the trust level is adjusted depending on the outcome of the TN
Trust level adjustment

- Takes advantage of the TN
- Each user assigns values to unprotected resources
- Policies structure further defines the value of the protecting resource
- The trust level is set to the aggregate value of the exchanged resources
- If the relationship exists the trust level is adjusted depending on the outcome of the TN
Trust level adjustment

- Takes advantage of the TN
- Each user assigns values to unprotected resources
- Policies structure further defines the value of the protecting resource
- The trust level is set to the aggregate value of the exchanged resources
- If the relationship exists the trust level is adjusted depending on the outcome of the TN
Trust level adjustment

- Takes advantage of the TN
- Each user assigns values to unprotected resources
- Policies structure further defines the value of the protecting resource
- The trust level is set to the aggregate value of the exchanged resources
- If the relationship exists the trust level is adjusted depending on the outcome of the TN
Conclusions

- Extension of an OSN access control framework integrating TN
- Extension of the language for expressing access control policies
- Feedback mechanism that takes into account the outcome of a TN between two nodes to dynamically set their trust levels
Future work

- Further development of the prototype
- Identification of methods to automatically set the lifetime of dynamic relationships
- Methods for computing the relevance of a resource
- Evaluate the impact of trust propagation among neighbours
- Further extensions to the policy definition language
Questions?

stefano.braghin@uninsubria.it