Ontology driven process for Mobile Security

Use Case: Group Detection

May 11 2010
Eun-kyung Kim
Scope

Security + Semantic Web
Scope

Security + Semantic Web

Mobility
Introduction: Mobile

• Mobile?
  - Mobile computing devices (e.g., mobile phones) are getting increasingly ubiquitous
  - Nodes can enter or leave the network spontaneously at any time to form or break links unintentionally

• Security issues related to mobility
  - Authentication
  - Privacy

  - Coordinating these devices has been recognized as a major challenge
    - e.g.
      Nodes entering/leaving the communication range dynamically group
Introduction: Group

- **Group** interaction examples
  - “We often eat in the same restaurant”
  - “We buy books from the same booksellers”
  - “We listen music by same singer”

- **Trust Group**
  - Before interacting with an agent for the first time, we seek the advice of entities we know and trust
    - Family, Friends, Colleagues or fairly stable communities of recommenders
Introduction: Security Issue

**Problem**
- How to decide who to involve in the trust group
- e.g.
  - When an interaction takes place, we have several difficulties,
    - The lack of administrative boundaries
    - The permission of anonymity of individuals interact with
- Collaboration may seriously be blocked
- Mobile devices may prefer to close their connectivity for their security
Problem Description

• Goal
  - To share semantically information with the right people, at the right \textit{time} and at the right access \textit{authority} in order to make the right communication using ontology

• Topic
  - Mobile applications security
    - especially how to decide who to interact within the authorized group dynamically
    - For the group-trust recommendation, the ontology used to encode the context of trust
  - Ontology
    - Conceptualization of mobile security
    - Use ontologies for specifying security policies
Requirement of an Ontology

• Advantages
  - To share common understanding of the structure of information among people or software agents
  - To enable reuse of domain knowledge
  - To separate domain knowledge from the operational knowledge

• Proposed ontology (extension of previous work, focuses on Security)
  - Mark up the concepts of mobile security in a well-understood and consistent manner
  - Formalize the relationships and influence btw the given concepts
Proposed Approach

- Research focus
  - Ontology based *authorization/reputation control issues* in group communication

- Communication Policy
  - Determines whether the prospective partners are able to communicate securely for the desired communication pattern according to their authorization policies
Trust Service-Group Discovery Framework

Requester’s Semantic Requirements

Ontology Repository

Security Policy Ontology

Domain Ontology

Distributed Registry

Trust Negotiation

Trust Negotiator

Authorization Manager

Service sends requester’s authorization info to requester

Discovery

Requester

Requester’s Authorization information
Proposed Ontology

• Mobile users want to maintain all configurations concerning the services they are using, the quality of service agreements and, mainly, the trust and privacy requirements

• Types of Agreements
  - User-Provider Agreements
    - Once the user contracts the provider, user wants to have guarantees that user’s privacy policies will be fully met during the entire session
  - Provider-Provider Agreement
    - The user constantly changes provider, but user’s identity must remain the same.
  - User-User Agreements
    - This type focuses on haggle communications, in which two end-users trust each other to exchange information and to share services and resources.
Security Policy Ontology - sketch

- Resources and Data
- Autonomous Entities (Including Agents)
- Actions and Events
- Relationships among Data and Resources
- Attributes: Characteristics, Metadata
- Mechanisms and Protocols: Sensors, Networking, Cryptography
- Contextual Parameters: Location, Time, etc.
- Constraints: Deontic, Limits, Precedence
Prototype

• **Ontology modeling** by using a Protégé
  - It is possible to model ontology concepts, their attributes/associations, check for inconsistencies, view the concepts’ hierarchy, handle instances, check semantic, etc.
  - -> Result of this modeling process, the ontology is formalized in a language called OWL (Ontology Web Language)

• **Mapping**
  - The concepts of ontology are mapped into Java classes

• **Testing**
  - The proposed ontology aims at allowing users to maintain control levels on their data according to the way they and their contacts trust the requesters
Result: Proposed Ontology

- There are 4 top classes
  - Users
  - Roles
  - Resources
  - Constraints

- If we deal with assets protection, our ontology should be support security services which are in relationship with users, role, resources and constraints
Result: Security Policy Ontology

• Example of the Ontology about “Role” concept
  - for Authorization
Experimentation

• Trust recommendation using ontology
  - each participant incorporates information from others and combines these in order to produce and make new information available

- Mechanism
  - Aggregating complexity to the devices’ operation
  - String trust and reputation information about everyone
  - Performing all the calculations

  - Participants’ opinions about each other are updated in a frequency as intense as the opportunistic encounters
Experimenting Scenario

• 3 users: Yellow, Blue and Red

• 5 trust level
  - Very Unreliable
  - Unreliable
  - No Opinion
  - Reliable
  - Very Reliable

• Goal
  - Make the trust communication depending on each trust level
Experimenting Result 1

- 20 requests from Yellow to Red’s WiFi interface
  - Default trust level

- At the initial state
  - Yellow’s trust value = 1

- After the initial interaction
  - Yellow adds a good experience with Red (Red edge rise)

- Blue’s recommendation
  - No communication
Experimenting Result 2

- 20 requests from Yellow to Red’s WiFi interface
  - Default trust level

- Similar to the test 1

- Charlie is now communicates with Yellow
  - Yellow: Trust level- No Opinion
  - Blue: adds good experiences about Yellow (Yellow increases)
  - Yellow: change the trust level to “Very Reliable”
  - Blue: is denied
  - Red: is decreased
Result Analysis

• The objective in prototyping is to validate the ontology and the trust models
  - It is tested in a desktop, could be used in a mobile device
• Security ontology used by analyzer of the trust level within the group

• (Evaluation/Comparison with related work)
  - Mathematical models were proposed for behavioral quantifying
    - The methods proposed range from weighted average [Yu et al., (2004)]
    - Probabilistic approaches [Yu and Singh (2003)]
    - Iterative approaches [Liu and Issarny, (2004)]
Conclusion

• We conceptualize the semantic relationships btw mobile actors and the associated security services
  - Extending the ontology for security
  - Experimenting the trust capture system using ontology

• Future work
  - Comparison to other similar approaches
  - Generalizing the ontology for security
    - independence of use cases
References

• S Parkin, A van Moorsel, R Coles, An information security ontology incorporating human-behavioural implications, 2009
• S Beji, N El Kadhi, A Knowledge Based Process Proposal for Mobile Security, Developments in eSys-tems Engineering (DESE), 2009
• S Mondal, S Sural, XML-based policy specification framework for spatiotemporal access control, 2009
• A Kostina, N Miloslavskaya, A Tolstoy, Information security incident management process, 2009