Towards Provenance and Risk-Awareness in Social Computing

Yuan Cheng, Dang Nguyen, Khalid Bijon, Ram Krishnan, Jaehong Park and Ravi Sandhu
Institute for Cyber Security
University of Texas at San Antonio

September 19, 2012
SRAS 2012, Minneapolis, MN

Access Control in Social Computing

- Content is almost contributed by users
- Access control policies are specified by users rather than the system alone
  - Policies are expressed in terms of attributes
  - In terms of relationships in online social networks
- BUT, all of them are pre-defined static policies that always give the same outcome
  - Unfortunately, social computing environment is dynamically changing over time

Motivating Example

A user starts an **event** to discuss on the upcoming US election outcome. Anyone registered in the social network can **join** the discussion group. However, joining the group requires to **vote** on an election **poll**. In order to vote, one must demonstrate his knowledge of the candidate through an action such as to **like** the candidate's **fan page**. Furthermore, each candidate might want users to **share** their page before liking.

How to place control on the dependency of these actions?
How to place control on the occurrence and frequency of these actions?

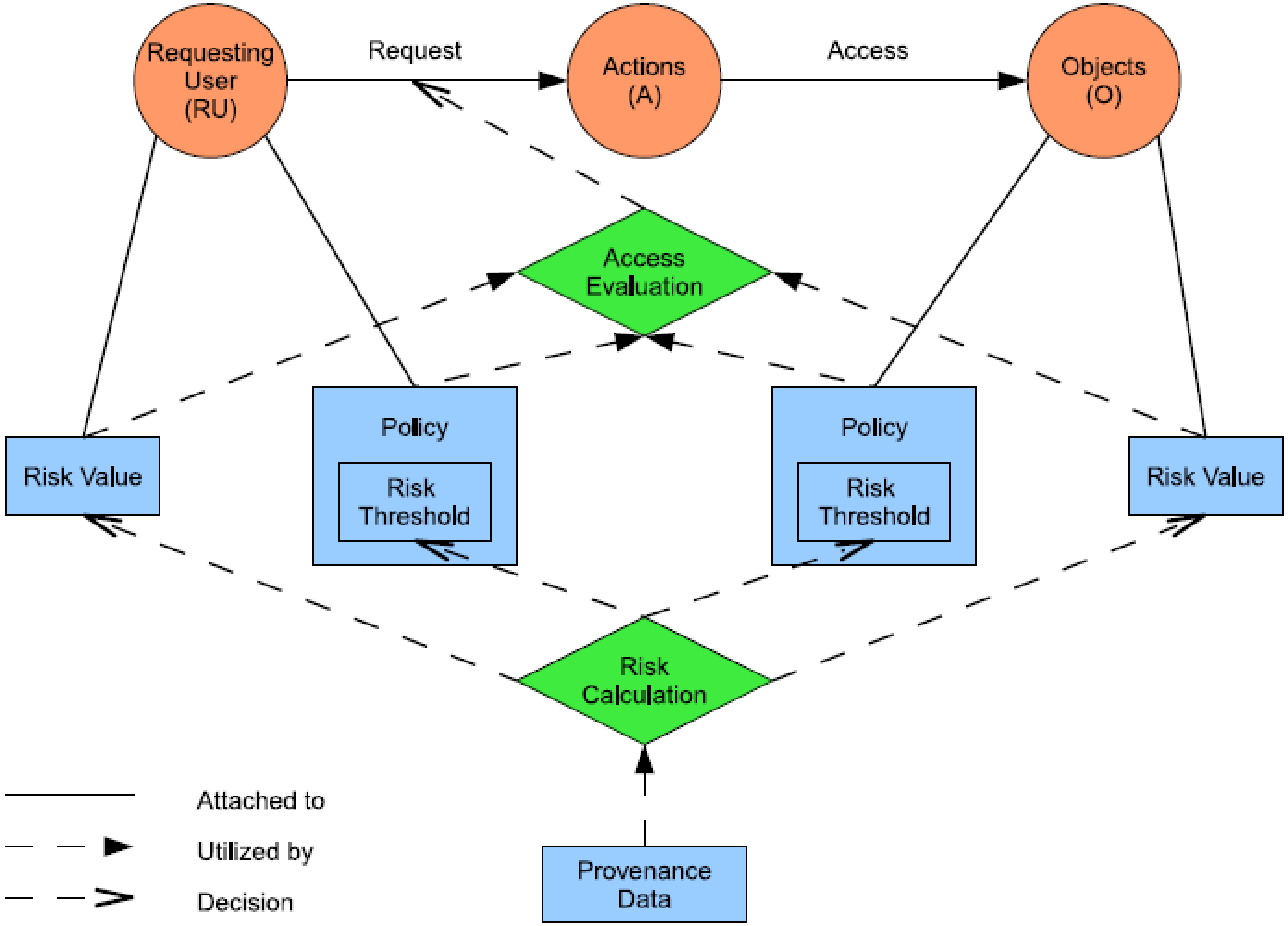
Risk-Aware Access Control

- **Risk** is *the possibility of future loss or damage*
  - Future needs and user behaviors are essentially unpredictable by static access control policies
- Risk-aware Access Control grants or denies an access dynamically based on estimated risk instead of some predefined policies
- Two key issues to assess risk:
  - Estimate the cost of permission being misused (**sensitivity**)
  - Determine the likelihood of misusing permissions (**trustworthiness**)

Provenance-Aware System

- **Provenance** of a digital data object is defined as the documentation of its origin and all the processes that influence and lead to its current state.
- In a provenance-aware system, related provenance information of system transactions/events are captured, stored, and maintained.
- Provenance potentially provides many enhanced benefits: usage tracking, workflow control, versioning, trustworthiness, repeatability, access control, etc..
- Can we use provenance for dynamic risk assessment?

Risk Aware Access Control for SC



Risk Aware Access Control for SC (cont.)

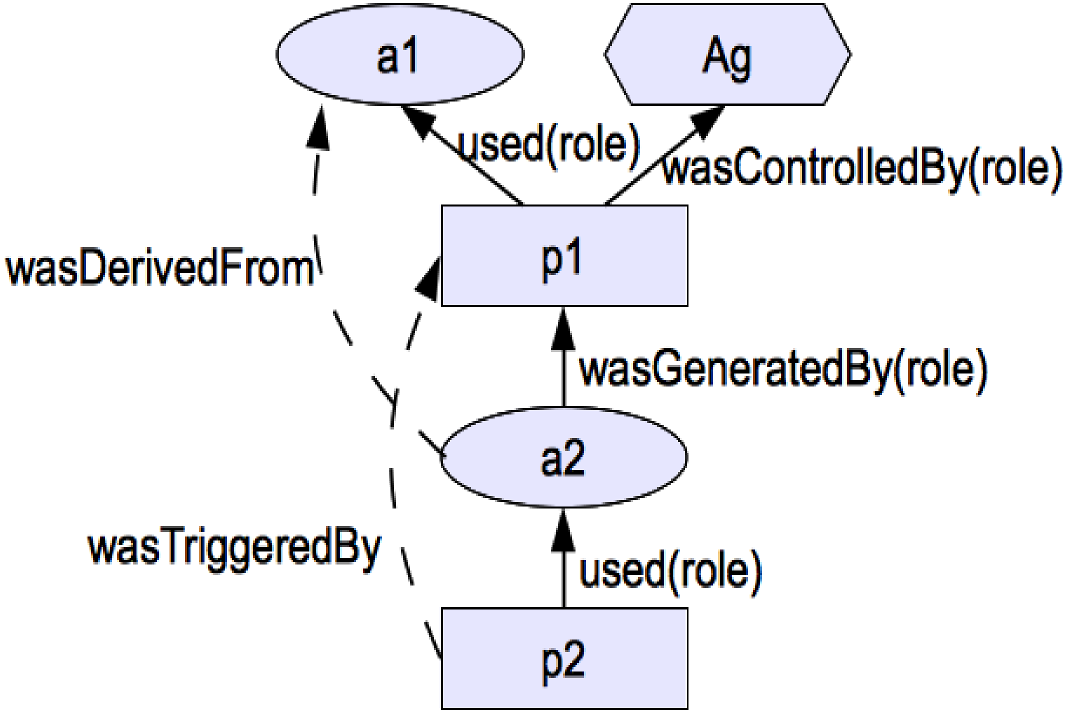
- **Risk value** represents the level of misuse granting requester access would result in
- **Risk threshold** denotes the level of sensitivity of performing the permission
- **Fluctuation of risk** serves as the basis for dynamic access control
  - User's risk value may increase or decrease as a result of her activities and behavior in the system.
  - Similarly, risk value of a resource may change depending on the past interactions on the resource.
- Requester user and resource owner can specify a risk threshold associated with each permission

Modeling Provenance Data in SC

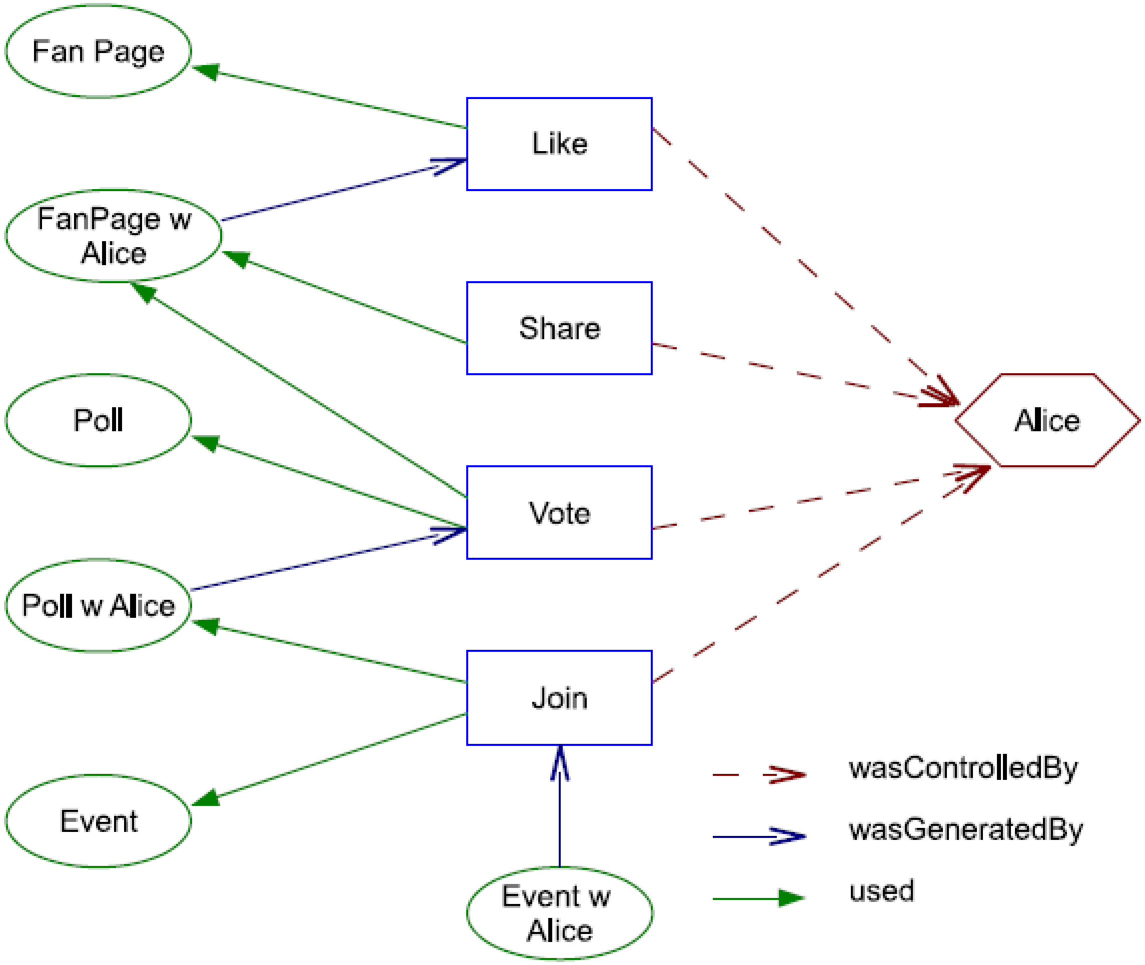
- Open Provenance Model (OPM) as the data model for provenance information
  - Captures information associated with a transaction and expresses the relations between them in causality dependencies

- 3 Nodes
  - Artifact (ellipse)
  - Process (Rectangle)
  - Agent (Octagon)

- 5 Causality dependency edges (not dataflow)



OPM Scenario



Modeling Provenance Data in SC (cont.)

- Alice requests to join an event:
  - *request(Alice, join, accountOf(Alice), event)*
- Associated transaction:
  - *(Alice, join, accountOf(Alice), event, eventWithAcountOfAliceAdded)*
- The corresponding provenance information:
  - *(join, wasControlledBy, Alice)*
  - *(join, used, event)*
  - *(join, used, accountOf(Alice))*
  - *(eventWithAccountOfAliceAdded, wasGeneratedBy, join)*

CONCLUSION

- Identify the necessity of incorporating Risk awareness and Provenance awareness in SC.
- Demonstrate through an example scenario.
- Present an approach for Provenance-based Risk Assessment.
- Present the initial effort towards a conceptual model for Risk-based Access Control.

- Questions or comments?

Thank You ☺