Runtime Reasoning about Conflicting Norms

Jiaming Jiang
Collaborators: Nirav Ajmeri, Jon Doyle, Munindar Singh, Rada Chirkova
Overall Objective

- **Hard Problem:** Policy Governed Secure Collaboration
- **Goals:**
  - To understand how security properties vary with policies that govern the behavior of collaborators (individuals and organizations)
  - To enable identification of policies that achieve desired tradeoffs between security and user preferences
- **Research Questions:** How to verify whether a set of policies
  - Is consistent through the preferences of the collaborators?
  - Is realizable through the preferences of the collaborators?
  - Achieves specified security properties?
Norms

• Standards of correct and secure behavior in a collaboration, e.g. sociotechnical system
• Example (HIPAA): A covered entity may use or disclose an individual’s PHI for treatment activities of health care providers.
• Sociotechnical system (Singh, 2013):
  • Norm components:
    • Subject & object: individuals or organizations
    • Context: organizations
    • Antecedent & consequent: conditions
  • Norms types: commitment, authorization, prohibition, power, sanction
Differences from Other Approaches

• Other approaches force conflict resolution to be done during the design phase, either by
  • Identifying all needed exceptions, or
  • Providing a total ordering of all norms
• Our approach allows runtime resolution of conflicts using
  • Partial ordering of norms
  • Knowledge of agent abilities and preferences
Reasoning about Norms

• Incorporate domain knowledge to detect conflicts among norms
• Use precedence relations to resolve conflicts at runtime
  • Precedence relation: a binary relation between two conflicting norm instances that decides which one is dominating and which one is dominated
  • Dominated norm instances: cannot be considered as violated
Coco Formalism

• Norm components:
  • Subject & object
  • Antecedent, consequent & deadline conditions
• Norm type: commitment
• Example: discloseCom(Physician, Patient, forTreatment, disclosePHI, empty)
Theoretical and Empirical Results

• Theoretical results on correctness and tractability of Coco’s ability to
  • Determine maximal sets of non-dominated commitment instances, and
  • Determine liveness and safety of a system of commitments.

• Empirical results on the usability of Coco:
  • Participants using Coco produced normative models with higher correctness and more coverage than those using Nomos3 (an existing normative approach).
  • Participants using Coco produced state diagrams with higher correctness and more coverage than those using Nomos3 or a non-normative approach.
Plan for Future Work

• Design and conduct better experiments
  • Reduce bias
  • Ask participants to answer questions with definite answers
• Formalize more norm components and norm types
  • Components: context, expiration condition
  • Types: authorization, prohibition
• Improve treatment of norm precedence via connections with non-monotonic logics
General Plan of Previous Experiment

- 3 Groups (20 participants each):
  - **Coco formalism**: Given tutorials on Coco and state diagrams, construct Coco normative models and draw state diagrams from the models for 3 scenarios.
  - **Nomos3 formalism**: Given tutorials on Nomos and state diagrams, construct Nomos normative models and draw state diagrams from the models for 3 scenarios.
  - **Non formalism**: Given tutorials on state diagrams, draw state diagrams for 3 scenarios.
- Metrics: correctness and coverage of normative models and state models
Problems with Previous Experiment and Solutions

• **Problem:** participants tended to rush work when seeing others leaving
  **Solution:** handout the materials for the next phase only when the previous phase is finished

• **Problem:** participants might start working on the solutions before finishing reading the tutorial
  **Solution:** deliver the tutorial using slides instead of handouts and give them the scenarios only after finishing the tutorial

• **Problem:** the solutions to the deliverables had too many variations, making it hard to create a standard rubrics for grading
  **Solution:** ask participants to answer unambiguous questions instead of constructing the whole model
General Plan of Next Experiment

• 2 groups:
  • **Control**: given an example, answer 20 questions for each set of policies (3 sets in total)
  • **Experimental**: given an example and a tutorial on constructing Coco normative models, answer 20 questions for each set of policies (3 sets in total)

• Metrics: the number of questions answered correctly for each set of policies
Norm Components

- Previous components: subject, object, antecedent, consequent, deadline condition for consequent.
- Add:
  - **Context**: the organization establishing the norm
  - **Expiration condition**: the condition that makes an antecedent false, after the antecedent has taken effective
- Example:
  
  *Norm*: The hospital regulates that for the first three days of a patient being hospitalized, his attending physician is committed to check on him in person at least twice a day.
  
  *Expiration condition*: three days have passed
  
  *Context*: hospital
Norm Types

• Previous formalized norm type: commitment
• Add:
  • **Authorization**: the subject is authorized by the object to bring about the consequent when the antecedent holds.
    • **Example**: A doctor is authorized to disclose a patient’s PHI for treatment purpose.
  • **Prohibition**: the subject is prohibited by the object to bring about the consequent when the antecedent holds.
    • **Example**: A doctor is prohibited to disclose a patient’s PHI without the patient’s or the patient’s representative’s consent.
Norm Precedence

- Previous: a set of dominance relations, but does not handle the situation where norm1 dominates norm2, which dominates norm3 properly.
- Dominance relation is not transitive.
- More problems arise when the dominance relations incur a cyclic ordering among norms.