What's Hot in R&D

Overview

The anonymity and privacy of users are important issues in information system design. We developed a method for formalizing and verifying anonymity and privacy based on the view that they are information hiding properties concerning the link between people and actions. In this view, anonymity and privacy are symmetric to each other, which can be considered a kind of duality in mathematics. This symmetry gives us a clear perspective for requirement formulation and is beneficial for verification efficiency.

Features

- Mathematical formalization and rigorous verification of anonymity and privacy
- Flexibility in describing anonymity and privacy requirements through the use of Epistemic logic
- Efficient verification exploiting the symmetry (duality) between anonymity and privacy
- Formal anonymity and privacy verification of the FOO (Fujioka-Okamoto-Ohta) electronic voting protocol

Application scenarios

- Safe and secure e-commerce and e-government systems
  - Flexible requirement descriptions of individual systems using Epistemic logic
  - Meets the ISO Evaluation Criteria for Information Technology Security
  - Formal methods are needed for evaluation assurance levels higher than EAL 4
- Clarifying the correspondence between legal and engineering requirements concerning privacy invasion
  - Bridging legal and engineering arguments by using a logical representation

Verification flow of our method

Verification flow of our method involves the following steps:

1. **Formal behavior description**
   - **State transition**: Describing the formal behavior of the system.
   - **Formal specification (anonymity, privacy)**: Formulating the anonymity and privacy requirements.

2. **Simulation of state transition**
   - **Proving that the behavior satisfies the specification**: Verifying that the behavior meets the specified requirements.
   - **Epistemic formula**: Using Epistemic logic for formal specification.

3. **General formulation in Epistemic logic**
   - **Anonymity**: Concealing the agent's identity.
     - Alice donated 2 million dollars to the nursing institution.
   - **Privacy**: Concealing the action.
     - I withdrew $10,000.
     - At the bank, I withdrew $1,000,000.

4. **Verification via role interchangeability**
   - **Dual (exchanging I and A)**:
     - \(\bigwedge_{i \in I} P[\theta(i, a)]\) for anonymity
     - \(\bigwedge_{a \in A} P[\theta(i, a)]\) for privacy
   - \(i\) can perform any action in \(A\).
   - \(\text{Anyone in } I \text{ can perform action } a\).

Verification via role interchangeability

- **Anonymity**: Derive
- **Privacy**: Derive
- **Additional cond.**: Role interchange-ability

Duality enables share of the verification process between anonymity and privacy.