Contextual Integrity and its Formalization

Anupam Datta

CMU

Fall 2007-08
Problem Statement

» Is an organization’s business process compliant with privacy regulations and internal policies?

» Examples of organizations
  • Hospitals, financial institutions, other enterprises handling sensitive information

» Examples of privacy regulations
  • HIPAA, GLBA, COPPA, SB1386

Goal: Develop methods and tools to answer this question
Contextual Integrity

◆ Philosophical framework for privacy
◆ Central concept: Context
  • Examples: Healthcare, banking, education
◆ What is a context?
  • Set of interacting agents in roles
    - Roles in healthcare: doctor, patient, ...
  • Norms of transmission
    - Doctors should share patient health information as per the HIPAA rules
  • Purpose
    - Improve health
Outline

1. Motivating Example
2. Framework
   - Model
   - Logic of Privacy and Utility
3. Workflows and Responsibility
4. Algorithmic Results
   - Workflow Design assuming agents responsible
   - Auditing logs when agents irresponsible
5. Conclusions
Now that I have cancer, Should I eat more vegetables?

Yes! except broccoli
Possible Enhancement

◆ Secretary handles every message
  • Privacy
  • Efficiency
  • Robustness

◆ Messages opaque to MyHealth
  • Unable to help secretary route messages
  • Hinders adding features like delegation

◆ Suggestion: add short tags to messages
Now that I have cancer, Should I eat more vegetables?

Yes! except broccoli
Now that I have cancer, should I eat more vegetables?

Yes! except broccoli
Workflow Design Goals

- **Privacy**
  - Secretary does not get sensitive info

- **Utility**
  - Health question eventually answered

- **Robustness**
  - Properties hold even with mistakes
Recommendations

◆ Add short tags to messages
  - Enhances privacy
  - Increases efficiency
  - Scales with added functionality

◆ Assign responsibilities
  - Example: secretary should tag messages with “health question” if needed
Outline

1. Motivating Example
2. Framework
   ◆ Model
   ◆ Logic of Privacy and Utility
3. Workflows and Responsibility
4. Algorithmic Results
   ◆ Workflow Design assuming agents responsible
   ◆ Auditing logs when agents irresponsible
5. Conclusions
Informational Norms

“In a context, the flow of information of a certain type about a subject (acting in a particular capacity/role) from one actor (could be the subject) to another actor (in a particular capacity/role) is governed by a particular transmission principle.”

Contextual Integrity [N2004]
**Model**

- **Communication via send actions:**
  - **Sender:** Bob in role Patient
  - **Recipient:** Alice in role Nurse
  - **Subject of message:** Bob
  - **Tag:** Health Question
  - **Message:** Now that I have cancer, Should I eat more vegetables?

- **Data model & knowledge evolution:**
  - Agents acquire knowledge by:
    - receiving messages
    - deriving additional attributes based on data model
      - Health Question $\leq$ Protected Health Information

**contents(msg) vs. tags (msg)**
Model

- State determined by knowledge of each agent
- Transitions change state
  - Set of concurrent send actions
  - Send(p,q,m) possible only if agent p knows m

Concurrent Game Structure

\[ G = \langle k, Q, \Pi, \pi, d, \delta \rangle \]
Logic of Privacy and Utility

◆ Syntax

\[ \varphi ::= \text{send}(p_1, p_2, m) \]
\[ \quad | \text{contains}(m, q, t) \quad \text{p}_1 \text{ sends p}_2 \text{ message m} \]
\[ \quad | \text{tagged}(m, q, t) \quad \text{m contains attrib t about q} \]
\[ \quad | \text{inrole}(p, r) \quad \text{m tagged attrib t about q} \]
\[ \quad | t \leq t' \quad \text{p is active in role r} \]
\[ \quad | \varphi \land \varphi \quad \text{Attrib t is part of attrib t'} \]
\[ \quad | \neg \varphi \quad \text{Classical operators} \]
\[ \quad | \exists x. \varphi \quad \text{Temporal operators} \]
\[ \quad | \varphi U \varphi \quad \text{Strategy quantifier} \]
\[ \quad | \varphi S \varphi \quad \text{Strategy quantifier} \]
\[ \quad | O \varphi \]
\[ \quad | <<p>> \varphi \]

◆ Semantics

Formulas interpreted over concurrent game structure
Specifying Privacy

- MyHealth@Vanderbilt

In all states, only nurses and doctors receive health questions

\[ G \forall p1, p2, q, m \\]
\[ \text{send}(p1, p2, m) \land \text{contains}(m, q, \text{health-question}) \]
\[ \Rightarrow \text{inrole}(p2, \text{nurse}) \lor \text{inrole}(p2, \text{doctor}) \]

LTL fragment can express HIPAA, GLBA, COPPA [BDMN2006]
Specifying Utility

MyHealth@Vanderbilt

Patients have a strategy to get their health questions answered

\[ \forall p \text{ inrole}(p, \text{patient}) \Rightarrow \]
\[ [p] F \exists q, m. \]
\[ \text{send}(q, p, m) \wedge \text{contains}(m, p, \text{health-answer}) \]
Expressing Privacy

Allow message transmission if:

- at least one positive norm is satisfied; and
- all negative norms are satisfied

Figure 1. Norms of Transmission Represented as a Temporal Formula
• HIPAA consists primarily of positive norms: share phi if some rule explicitly allows it (2), (3), (5), (6)
• Exception: negative norm about psychotherapy notes (4)
COPPA – Children Online Privacy

COPPA consists primarily of negative norms

- Children can share their protected info only if parents consent (7) (condition)

- (8) (obligation – future requirements)
Financial institutions must notify consumers if they share their non-public personal information with non-affiliated companies, but the notification may occur either before or after the information sharing occurs.

\[
\text{inrole}(p_1, \text{institution}) \land \text{inrole}(p_2, \text{non-affiliate}) \land \text{inrole}(q, \text{consumer}) \land (t \in \text{npi}) \rightarrow \\
\diamond \text{send}(p_1, q, \text{privacy-notice}) \lor \diamond \text{send}(p_1, q, \text{privacy-notice})
\]
Outline

1. Motivating Example
2. Framework
   - Model
   - Logic of Privacy and Utility
3. Workflows and Responsibility
4. Algorithmic Results
   - Workflow Design assuming agents responsible
   - Auditing logs when agents irresponsible
5. Conclusions
MyHealth@Vanderbilt Improved

Doctor should answer health questions

Assign responsibilities to roles & workflow engine

Now that I have cancer, Should I eat more vegetables?

Yes! except broccoli
Graph-based Workflow

- **Graph**
  
  \((R, R \times R)\), where \(R\) is the set of roles

- **Edge-labeling function**
  
  \(\text{permit}: R \times R \rightarrow 2^T\), where \(T\) is the set of attributes

- **Responsibility of workflow engine**
  
  Allow msg from role \(r_1\) to role \(r_2\) iff \(\text{tags}(msg) \subseteq \text{permit}(r_1, r_2)\)

- **Responsibility of human agents in roles**
  
  Tagging responsibilities
  - ensure messages are correctly tagged
  Progress responsibilities
  - ensure messages proceed through workflow
MyHealth Responsibilities

◆ Tagging
Nurses should tag health questions
\[ G \ \forall p, q, s, m. \text{inrole}(p, \text{nurse}) \land \text{send}(p, q, m) \land \text{contains}(m, s, \text{health-question}) \Rightarrow \text{tagged}(m, s, \text{health-question}) \]

◆ Progress
• Doctors should answer health questions
\[ G \ \forall p, q, s, m. \text{inrole}(p, \text{doctor}) \land \text{send}(q, p, m) \land \text{contains}(m, s, \text{health-question}) \Rightarrow \neg \exists m'. \text{send}(p, s, m') \land \text{contains}(m', s, \text{health-answer}) \]
Abstract Workflow

◆ Responsibility of workflow engine
  • LTL formula $\varphi$
  • Feasible (enforceable) if $\varphi$ is a safety formula without the contains() predicate

◆ Responsibility of each role $r$
  • LTL formula $\varphi_r$
  • Feasible if agents have a strategy to discharge their responsibilities
    \[ \forall p. \varphi \land \text{inrole}(p, r) \Rightarrow \ll p \gg \varphi_r \]

Graph-based workflows are a special case
Outline

1. Motivating Example
2. Framework
   - Model
   - Logic of Privacy and Utility
3. Workflows and Responsibility
4. Algorithmic Results
   - Workflow Design assuming agents responsible
     - Abstract workflows
   - Auditing logs when agents irresponsible
     - Only graph-based workflows
5. Conclusions
Now that I have cancer, should I eat more vegetables?

Yes! Except broccoli.

• Minimal disclosure
• Privacy: HIPAA compliance+
• Utility: Schedule appointments, obtain health answers

• Responsibility: Doctor should answer health questions
Workflow Design Results

- **Theorems:**
  - Assuming all agents act responsibly, checking whether workflow achieves
    - Privacy is in PSPACE (in the size of the formula describing the workflow)
    - Utility is decidable

- **Definition and construction of minimal disclosure workflow**

Algorithms implemented in model-checkers, e.g. SPIN, MOCHA
Deciding Privacy

◆ PLTL model-checking problem is PSPACE decidable

\[ G \models \text{tags-correct} \cup \text{agents-responsible} \Rightarrow \text{privacy-policy} \]

\( G \): concurrent game structure

Result applies to finite models (\#agents, msgs,...)
MyHealth Privacy

- MyHealth@Vanderbilt workflow satisfies this privacy condition

In all states, only nurses and doctors receive health questions

\[ G \forall p_1, p_2, q, m \]
\[ \text{send}(p_1, p_2, m) \land \text{contains}(m, q, \text{health-question}) \Rightarrow \text{inrole}(p_2, \text{nurse}) \lor \text{inrole}(p_2, \text{doctor}) \]

- Run LTL model-checker, e.g. SPIN
Deciding Utility

◆ ATL* model-checking of concurrent game structures is
  • Decidable with perfect information
  • Undecidable with imperfect information

◆ Theorem:
  There is a sound decision procedure for deciding whether workflow achieves utility

◆ Intuition:
  • Translate imperfect information into perfect information by considering possible actions from one player’s point of view
MyHealth Utility

MyHealth@Vanderbilt workflow satisfies this utility condition

Patients have a strategy to get their health questions answered

\[ \forall p \text{ inrole}(p, \text{patient}) \Rightarrow \exists q, m. \text{send}(q, p, m) \land \text{contains}(m, p, \text{health-answer}) \]

Run ATL* model-checker, e.g. MOCHA
Minimal Disclosure Workflow

◆ Abstract workflows:
  \[ W_1(\varphi_1, \varphi_R) \leq W_2(\varphi_2, \varphi_R) \text{ if } G \text{ satisfies } \varphi_1 \Rightarrow \varphi_2 \]

◆ Graph-based workflows:
  \[ W_1(R, \text{permit}_1) \leq W_2(R, \text{permit}_2) \text{ if } \forall r_1, r_2 \in R. \text{permit}_1(r_1, r_2) \subseteq \text{permit}_2(r_1, r_2) \]

◆ Lemma:
  If \( W_1 \leq W_2 \) and \( W_2 \) achieves a privacy goal, then so does \( W_1 \)

◆ Minimal Disclosure Workflow:
  \( W \) is minimal wrt to a utility goal if \( W \) achieves the goal and all feasible \( W' < W \) fails to achieve the goal
Now that I have cancer, Should I eat more vegetables?

Yes! except broccoli
Now that I have cancer, should I eat more vegetables?

Yes! except broccoli.
Outline

1. Motivating Example
2. Framework
   ◆ Model
   ◆ Logic of Privacy and Utility
3. Workflows and Responsibility
4. Algorithmic Results
   ◆ Workflow Design assuming agents responsible
     ◆ Abstract workflows
   ◆ Auditing logs when agents irresponsible
     ◆ Only graph-based workflows
5. Conclusions
Auditing Results

 Definitions
  - Policy compliance, locally compliant
  - Causality, accountability

 Design of audit log

 Algorithms
  - Finding agents accountable for locally-compliant policy violation in graph-based workflows using audit log
  - Finding agents who act irresponsibly using audit log

 Algorithms use oracle:
  - $O(\text{msg}) = \text{contents}(\text{msg})$
  - Minimize number of oracle calls
Policy compliance/violation

- **Strong compliance**
  - Action does not violate current policy requirements
  - Future policy requirements after action can be met

- **Locally compliant policy**
  - Agents can determine strong compliance based on their local view of history
Definition. The relation “⇒” on the set of events of a system is the smallest relation satisfying the following three conditions: (1) If $a$ and $b$ are events in the same process, and $a$ comes before $b$, then $a \Rightarrow b$. (2) If $a$ is the sending of a message by one process and $b$ is the receipt of the same message by another process, then $a \Rightarrow b$. (3) If $a \Rightarrow b$ and $b \Rightarrow c$ then $a \Rightarrow c$. Two distinct events $a$ and $b$ are said to be concurrent if $a \leftrightarrow b$ and $b \leftrightarrow a$. 

Causality

Lamport Causality [1978]
Accountability & Audit Log

◆ Accountability
  • Causality + Irresponsibility

◆ Audit log design
  • Records all Send(p,q,m) and Receive(p,q,m) events executed
  • Maintains causality structure
    - $O(1)$ operation per event logged
Auditing Algorithm

◆ **Goal**
Find agents accountable for a policy violation

◆ **Algorithm**(Audit log $A$, Violation $v$)
1. Construct $G$, the causality graph for $v$ in $A$
2. Run BFS on $G$.
   At each Send($p$, $q$, $m$) node, check if tags($m$) = $O(m)$. If not, and $p$ missed a tag, output $p$ as accountable

◆ **Theorem:**
- The algorithm outputs at least one accountable agent for every violation
  - of a locally compliant policy in an audit log
  - of a graph-based workflow that achieves the policy in the responsible model
Proof Idea

- **Causality graph $G$ includes all accountable agents**
  - Accountability = Causality + Irresponsibility

- **There is at least one irresponsible agent in $G$**
  - Policy is satisfied if all agents responsible
  - Policy is locally compliant

- **In graph-based workflows, safety responsibilities violated only by mistagging**
  - $O(\text{msg}) = \text{tags}(\text{msg})$ check identifies all irresponsible actions
1. Policy violation:
   Secretary Candy receives health-question mistagged as appointment-request

2. Construct causality graph $G$ and search backwards using BFS
   Candy received message $m$ from Patient Jorge.
   - $O(m) = \text{health-question}$, but $\text{tags}(m) = \text{appointment-request}$.
   - Patient responsible for health-question tag.
   - Jorge identified as accountable
Conclusions

1. Framework
   - Concurrent game model
   - Logic of Privacy and Utility
     - Temporal logic (LTL, ATL*)

2. Business Process as Workflow
   - Role-based responsibility for human and mechanical agents

3. Algorithmic Results
   - Workflow design assuming agents responsible
     - Privacy, utility decidable (model-checking)
     - Minimal disclosure workflow constructible
   - Auditing logs when agents irresponsible
     - From policy violation to accountable agents
     - Finding irresponsible agents

   Using oracle
   Automated
Thanks

Questions?
Local communication game

◆ Quotient structure under invisible actions, $G_p$
  
  • States: Smallest equivalence relation
    
    $K_1 \sim_p K_2$ if $K_1 \xrightarrow{a} K_2$ and $a$ is invisible to $p$
  
  • Actions: $[K] \xrightarrow{a} [K']$ if there exists $K_1$ in $[K]$ and $K_2$ in $[K']$
    
    s.t. $K_1 \xrightarrow{a} K_2$
  
◆ Lemma: For all LTL formulas $\varphi$ visible to $p$, $G_p \models \langle\langle p\rangle\rangle \varphi$ implies $G \models \langle\langle p\rangle\rangle \varphi$
Refinement and Combination

◆ Policy refinement
  • Basic policy relation
  • Does hospital policy enforce HIPAA?

◆ $P_1$ refines $P_2$ if $P_1 \rightarrow P_2$
  • Requires careful handling of attribute inheritance
  • PSPACE decidable

◆ Combination becomes logical conjunction
  • Defined in terms of refinement
## Related Languages

<table>
<thead>
<tr>
<th>Model</th>
<th>Sender</th>
<th>Recipient</th>
<th>Subject</th>
<th>Attributes</th>
<th>Past</th>
<th>Future</th>
<th>Combination</th>
</tr>
</thead>
<tbody>
<tr>
<td>RBAC</td>
<td>Role</td>
<td>Identity</td>
<td></td>
<td></td>
<td>×</td>
<td>×</td>
<td>•</td>
</tr>
<tr>
<td>XACML</td>
<td>Flexible</td>
<td>Flexible</td>
<td>Flexible</td>
<td></td>
<td>0</td>
<td>×</td>
<td>0</td>
</tr>
<tr>
<td>EPAL</td>
<td>Fixed</td>
<td>Role</td>
<td>Fixed</td>
<td></td>
<td>•</td>
<td>×</td>
<td>0</td>
</tr>
<tr>
<td>P3P</td>
<td>Fixed</td>
<td>Role</td>
<td>Fixed</td>
<td></td>
<td>•</td>
<td>0</td>
<td>×</td>
</tr>
<tr>
<td>LPU</td>
<td>Role</td>
<td>Role</td>
<td>Role</td>
<td></td>
<td></td>
<td></td>
<td>•</td>
</tr>
</tbody>
</table>

◆ Legend:
- × unsupported
- o partially supported
- • fully supported

◆ LPU fully supports attributes, combination, temporal conditions
Why Not Use P3P?

Different application
- P3P understood by web browsers
- LPU intended for internal policy enforcement

Not expressive enough
- P3P cannot express HIPAA, GLBA, COPPA
- Each policy only has one sender and one subject
- Missing temporal conditions; only has simple opt-in / opt-out
Heath care providers can tell patients their health information

Sender role  Recipient role  Subject role  Attribute

Heath care providers can tell patients their psychotherapy notes *only if a psychiatrist has approved*