Privacy and Health Care

Doctor

Electronic Health Record

Patient Portal

Specialist

HIPAA Compliance

Patient

Surrogate
Legislative Privacy Requirements

- **Gramm-Leach-Bliley Act (GLBA)**
  - 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.

- **HIPAA Privacy Rule**
  - Patients can access their protected health information held by covered entities, except for their psychotherapy notes (which can be accessed after a psychiatrist approves).
Enterprise Privacy Requirements

• E*TRADE
  – We may also disclose information that we collect from you such as your name, contact information, and customer relationships with us to nonaffiliated third parties that perform services, such as marketing or market research, on our behalf.

  – We require that all entities with which we share your nonpublic personal information, including companies that process or service transactions for us, agree to keep your information confidential.
Contextual Integrity

- Philosophical account of privacy
  - Transfer of personal information
  - Describes what people care about

- Flow governed by norms
  - Agents act in roles in social contexts
  - Rejects public/private dichotomy

- Principles of transmission
  - Confidentiality, reciprocity, dessert, etc
Model: Communicating Agents

- Agents can send each other messages
  - Messages carry information about subjects
  - Agents learn information in messages they receive
- Policies judge traces of agent communication
  - Past and future important to privacy judgments

Charlie’s SSN is 078-05-1120
CI: A Logic for Privacy Policies

- Formalizes part of Contextual Integrity
- Syntax

\[ \varphi ::= \text{send}(p_1, p_2, m) \quad \text{\(p_1\) sends \(p_2\) message \(m\)} \]

\[ | \text{contains}(m, q, t) \quad \text{\(m\) contains attribute \(t\) about \(q\)} \]

\[ | \text{inrole}(p, r) \quad \text{\(p\) is active in role \(r\)} \]

\[ | t_1 \leq t_2 \quad \text{Attribute \(t_1\) is part of attribute \(t_2\)} \]

\[ | \varphi \land \varphi | \neg \varphi | \exists x. \varphi \quad \text{Classical operators} \]

\[ | \varphi U \varphi | \varphi S \varphi | O \varphi \quad \text{Temporal operators} \]

- Policies use a restricted class of formulas
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.

If send($p_1$, $p_2$, $m$) and inrole($p_1$, institution) and inrole($p_2$, non-affiliated) and contains($m$, $q$, npi) and inrole($q$, consumer), then eventually send($p_1$, $q$, notification) or previously send($p_1$, $q$, notification).
HIPAA Example

• **English policy**
  - Patients can access their protected health information held by covered entities, except for their psychotherapy notes (which can be accessed after a psychiatrist approves).

• **Formal policy**
  + $send(p, q, m)$ and inrole($p$, covered-entity) and inrole($q$, patient) and contains($m$, $q$, protected-health-information)
  
  - If $send(p, q, m)$ and inrole($p$, covered-entity) and inrole($q$, patient) and contains($m$, $q$, psychotherapy-notes), then previously send($p'$, $p$, $m'$) and inrole($p'$, psychiatrist) and contains($m'$, $q$, approve-disclosure-of-psychotherapy-notes)
E*TRADE Example

• English policy
  – We may disclose your nonpublic personal information (NPI) to third parties that perform services on our behalf.
  – Entities with which we share your NPI agree to keep your information confidential.

• Formal policy
  + send($p_1$, $p_2$, $m$) and inrole($p$, etrade) and inrole($p_2$, serviceprovider) and contains($m$, $q$, npi) and inrole($q$, customer)

  – If send($p_1$, $p_2$, $m$) and inrole($p$, etrade) and contains($m$, $q$, npi) and inrole($q$, customer), then henceforth not send($p_2$, $p_3$, $m'$) and contains($m'$, $q$, npi)
Policy Algorithms

• Policy refinement in PSPACE
  – Given legislative requirements and enterprise policy
  – Does policy enforce all legislative requirements?

• Weak compliance in polynomial time
  – Given a policy and a communication history
  – Does contemplated action meet present requirements?

• Strong compliance in PSPACE
  – Given a policy, a history, and a weakly-compliant action
  – Can future obligations be met without violating policy?
## 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>0</td>
<td>×</td>
<td>0</td>
<td>•</td>
</tr>
<tr>
<td>EPAL</td>
<td>Fixed</td>
<td>Role</td>
<td>Fixed</td>
<td>•</td>
<td>×</td>
<td>0</td>
<td>×</td>
</tr>
<tr>
<td>P3P</td>
<td>Fixed</td>
<td>Role</td>
<td>Fixed</td>
<td>•</td>
<td>0</td>
<td>×</td>
<td>0</td>
</tr>
<tr>
<td>CI</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
  - • full supported
- CI fully supports attributes and combination
Policy Enforcement Paradigms

- Reference Monitor
- Run-time Monitor
- Audit Logs

- Business Process Execution
  - Audit for policy violations
  - Find accountable agents

Agents

DB
Role-based Responsibilities

- Workflow engine enforces partial policy
  - Agents learn sensitive information
  - Cannot enforce entire policy

- Responsibilities for agents in each role
  - Business process rules

- Agents responsible $\rightarrow$ policy fulfilled
  - Check at design time (in PSPACE)
  - Audit at run time to find irresponsible agents
Business Process Design

Contextual Integrity

Purpose

Norms

Business Objectives

Privacy Policy

Utility Checker (ATL*)

Privacy Checker (LTL)

Utility Evaluation

Privacy Evaluation

Business Process Design

Purpose

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

Yes! except broccoli
Auditing Algorithms

• Accountable agent
  – Acted irresponsibly
  – Caused policy violation

• Finding accountable agents
  – Search audit log using Lamport causality structure
  – Minimize work of human auditor

• Finding irresponsible actions
  – Suspicious actions: do not appear possible from tags
  – Mistagged message must be “nearby”
Conclusions

• Precise language for privacy policies
  – Expresses most privacy laws
  – Past and future important
  – Policy operations tractable

• Enforcement in business processes
  – Partial mechanical enforcement
  – Individual responsibilities
  – Audit to find agents accountable for policy violations
Questions?