Towards Integrated Policy Management for Privacy

Dr Nick Papanikolaou
e-Security Group
International Digital Laboratory
WMG, University of Warwick
http://go.warwick.ac.uk/nikos
Context

- Joint work with Marco Casassa Mont & Siani Pearson [HP Labs], Sadie Creese & Michael Goldsmith [Warwick IDL]
- EnCoRe project
  - [http://www.ensemble-project.info](http://www.ensemble-project.info)
  - “Ensuring Consent and Revocation”
  - Goal is to manage and enforce users’ privacy (consent and revocation) preferences in enterprise information systems
Privacy Policies

• Cannot underestimate importance of adequate information handling practices in enterprises to ensure
  – Continued ability to collect information
  – Privacy of individuals

• Legal requirements (National, EU), Codes of Practice, Corporate privacy policies
Enforcing Privacy Policies

- There are many different levels of requirements and no common representation or consistent means of enforcement across an enterprise.

- Automated enforcement is simple for lowest levels of policy only (e.g. Access control policies).
  - Automated enforcement of privacy policies not very successful (cf. P3P).
Policy management levels

• In an enterprise, privacy requirements will be typically handled at different levels by different experts
  – Legal requirements – legal team
  – Data access requirements – IT team

• Hierarchy of policies (privacy requirements)

• There may be overlaps and conflicts between requirements at different levels
Policy management approaches

- In our view, taking an approach to dealing with privacy requirements that is too low level (e.g. focusing only on XACML representation of access control restrictions) misses important legal aspects and outcomes of risk assessment
Policy management approaches

- **Pragmatic approaches**
  - Risk assessment (standard business practice)
  - Typically results in non-reusable solutions

- **Technical approaches**
  - Focus on designing languages and software tools for policies of a particular kind [*only*]
Policy Levels vs. Approaches

- Technical Policies, Policy languages eg. XACML, P3P, EPAL, P-RBAC
- Legal & Regulatory Policies, risk assessment
- ?
- ?
Reconciling policy requirements

- Low-level approaches have the advantage of **automation**
- High-level approaches account for overall security concerns, the law, and the business processes in an enterprise
- Can we obtain the benefits of both by building a **conceptual model**?
Conceptual Model for Policies

High-level policies
- European Privacy Directive
- Data Protection Act
- Codes of Practice
- Corporate Policies, ...

Conceptual Model
- Templates for different policy requirements

Low-level policies
- Implementable policies
- XACML code for access control
- P3P and APPEL, ...
- Machine-checkable (verifiable)
More about conceptual model

- Conceptual model may take different forms
  - Varying levels of formality can be useful
  - Just identifying typical clause structures of legal texts can provide clarity
  - More formal models can enable automatic checking that
    - A lower-level policy satisfies the requirements of a higher-level one (policy refinement)
    - Policy statements do not conflict with one another
Examples

• In the paper we have considered examples of policy statements e.g. for transborder data flow, ...

• Privacy-aware access control e.g.

IF (Data Requestor wants to access personal data D for Purpose P)
AND (data subject has given consent for this data)
THEN Allow Access
ELSE Deny Access
Privacy-aware access control

Database tables with PII data and customers’ consents

<table>
<thead>
<tr>
<th>uid</th>
<th>Name</th>
<th>Condition</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Alice</td>
<td>Alcoholic</td>
<td>Cirrhosis</td>
</tr>
<tr>
<td>2</td>
<td>Rob</td>
<td>Drug-addicted</td>
<td>HIV</td>
</tr>
<tr>
<td>3</td>
<td>Julie</td>
<td>Contagious Illness</td>
<td>Hepatitis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Consent</th>
<th>Marketing</th>
<th>Research</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Encoded access-control policy

If role == “Statistician” & intent == “Marketing”
Then
 Allow Access (T1.Condition, T1.Diagnosis) & Enforce (Consent)

Else If role == “Scientist” & intent == “Research”
Then
 Allow Access (T1.Diagnosis) & Enforce (Consent)

Else Deny Access

Privacy Policy Enforcement

Access Table T1 (Select ALL from T1)
Intent = “Marketing”

Enforcement: Filter data

SELECT "-", Condition, Diagnosis FROM T1, T2
WHERE T1.uid=T2.Consent AND T2.Marketing="YES"

Filtered-out data

<table>
<thead>
<tr>
<th>uid</th>
<th>Name</th>
<th>Condition</th>
<th>Diagnosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>- Alcoholism</td>
<td>Cirrhosis</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>3</td>
<td>- Contagious Illness</td>
<td>Hepatitis</td>
<td></td>
</tr>
</tbody>
</table>
Summary of position

- Current approaches to policy specification and enforcement are either too high-level or too low-level.
- The EnCoRe project is developing an approach that balances risk assessment and high-level requirements with low-level considerations, esp. what is implementable using current policy languages and tools.
Related and Future Work

- We have already considered how privacy policies in P3P may be translated to a form suitable for automated verification
  - See [http://go.warwick.ac.uk/nikos/publications](http://go.warwick.ac.uk/nikos/publications)
- We hope to develop a formal access control model that is designed to express privacy policies at all the levels that they arise