On frameworks for the visualization of privacy policy implications

Rafael Accorsi and Thomas Stocker

Dept. of Telematics

University of Freiburg, Germany

{accorsi,stocker}@iig.uni-freiburg.de

Users fail to compose strong policies

- Plethora of expressive policy languages exist.
  - XACML, EPAL, OSL, ExPDT, …
- Problems on capturing users' intent.
  - Introspection and increasingly complex policies lead to "unexpected" access and usage decisions.
- Need for frameworks to help users to visualize the implications of their privacy policies.

Visualizing the policy difference

- ExPDT: Extended Privacy Definition Tools.
  - Based on OWL-DL and 3-valued logic.
  - Authorizations with provisions and obligations.
  - Policy combination and *comparison*.

- Allows the computation of policy difference.
  - P_{Sys} - P_{User} = P_{diff}.
  - Visualization using data hierarchies (trees).
  - Complexity problems w.r.t. the difference.

Policy inference in UbiComp scenarios

- What (personal) data is inferred from a policy?
  - Environment with data fusion capabilities.
  - Joint work with artificial intelligence.

- User controls the amount/quality of inference.
  - P_{User} defines a threshold for the derivation (approximation) of a data item.
  - Visualization as Bayes' belief networks (DAGs).
  - Completeness problems.

Policy implications in eCommerce

- Which data is collected and how it is used after collection?
  - Definition of business process (workflows).
  - “Simulation” of data usage on the workflows.

- User knows the traces of data usage.
  - Propagation graphs depict traces.
  - User can adjust the policy correspondingly.
  - Too strong assumption w.r.t. the workflows?

Conclusion

- Different frameworks for the visualization of privacy policy implications.

- We already have expressive policy languages.
  - Let's help users to get to precise policies.
  - Development of tools for policy management.

- Not only privacy can profit from that.
  - Compliance engineers, auditors, etc.

References

- R. Accorsi et al. On the visualization of policy inferences. Submission to WISTP 2010.
- M. Kaehmer et al. Automating Privacy Compliance with ExPDT. CEC/EEE 2008: 87-94.
- M. Kähmer and M. Gilliot: Extended Privacy Definition Tool. PRIMIUM 2008.
- S. Sackmann et al. Personalization in Privacy-Aware Highly Dynamic Systems. Comm. ACM, vol. 49(9), pp. 32-38, 2006.
- S. Trudeau et al. The Effects of Introspection on Creating Privacy Policy. WPES 2009.
- S. Höhn et al. An Approach to Usable Security for Ambient Intelligence Environments. Long-Term and Dynamical Aspects of Information Security, 2008.