# Process Modeling as a Basis for Auditing Information Privacy

Ralph Herkenhöner, Hermann de Meer
Faculty of Informatics and Mathematics
University of Passau, Germany
{rhk|hdm}@fim.uni-passau.de

**Abstract:** Information privacy has become an important task for every data processing organization. To meet its demands, organizations apply privacy-enhancing technologies and identity management to their business processes. But the increasing number of privacy breaches shows that this task is complex and not well understood.

In this position paper, a formal method for modeling an proving information privacy within a process model is envisioned. Such a model would allow an integration at process design, increase the understanding and effectiveness of the privacy protection mechanisms, and enable compliance checks and data protection auditing.

**Acknowledgment:** This research work was funded by the Federal Ministry of Education and Research of the Federal Republic of Germany (Funding-Id: 01|S08016B).

## 1 Information Privacy in Business Processes

With the shift from a paper-based to a digital information society, collection and processing of data have become much easier and very fast. Without the proper carefulness, information easily can be used for purposes they are neither intended for nor permitted to. This problem is documented by the increasing number of incidents regarding data leakages, missuses of personal data and even identity thefts. Like in the latest incident, where a secret file of the US-Army was found by a civilian on an second-hand mp3-player[1], often the reason is the missing awareness in using non-confidential communication channels. This results in loss of control on information flow and enables data misuse and theft. A predictable and comprehensible information flow could avoid such incidents or even aids investigation. We call this information privacy.

Reasonable information privacy requires at least reconcilement of privacy and accountability of a data subject's electronic interaction (empowering the data subject in its self-determination) [CSS+05] and a privacy-aware identity and information lifecycle management within the data processing organizations (including compliance, data protection, and access control) [MB07]. Both depend on the underlying business processes and the involved information privacy techniques.

[1] In January 2009, the New Zealand news channel One News gets possession of a 60 page long file containing name and contact information of US-Soldiers, details on equipment, and other secret information. The file was stored on an mp3-player bought at a second-hand shop by a civilian.

## 2 Privacy-Aware Process Modeling

As presented in a case study on biobanks [Her08], modeling business processes can help to gain a better understanding on information privacy within the data processing organization using the UML extension UMLsec.

The idea is to integrate security characteristics within the process model granting information privacy . Such an integration enables the additional benefit that the interaction of control flow, information flow, and information privacy is visible within a single model. With proper levels of abstraction—avoiding an information overload during examination—such a model increases the understanding of the privacy mechanisms and, for example, allows data protection auditing [Aud01].

For that purpose, the modeled security characteristics must cover the major security target *confidentiality*, including the *non-propagation* of protected information and the non-observability of the processes by a non-authorized third. To assure the processing of correct data subjects' information and to avoid incorrect alterations, *integrity* and *authenticity* must be taken into account. Nevertheless, as the protection of the data subjects' privacy is the main target, anonymization mechanisms have to be clearly specified within the model. This also includes the pseudonym management in a case of pseudonymization. Last but not least, there must be an *accountability* and *non-repudiation* for every access on and processing of the protected data. Therefore, access and processing have to be able to be audited.

## 3 Proving Information Privacy

The goal of data protection auditing is to comprehensibly prove information privacy. Therefore, it is helpful to have a formal argumentation to prove correctness and effectiveness for a given privacy protection concept. For this purpose, using UMLsec for process modeling, has an additional benefit. As shown by Jürjens [Jür03], UMLsec provides a formal basis to prove the fulfillment of security targets within the process model . For utilization of these methods to prove information privacy, it is necessary to refine information privacy from provable security characteristics. This goal is located within the research field of the authors.

## References


[Aud01] Data Protection - Complete Audit Guide. Technical report, The Information Commissioner's Office, UK, 2001.

[CSS+05] J. Camenisch, A. Shelat, D. Sommer, S. Fischer-Hübner, M. Hansen, H. Krasemann, G. Lacoste, R. Leenes, and J. Tseng. Privacy and Identity Management for Everyone. In *DIM '05: Proceedings of the 2005 Workshop on Digital Identity Management*, pages 20–27, New York, NY, USA, 2005. ACM.

[Her08] Ralph Herkenhöner. Process Modeling for Privacy-conformant Biobanking: Case Studies on Modeling in UMLsec. In *Proceedings of the 6th International Workshop on Security Information Systems*, pages 3–12, Portugal, 2008. INSTICC Press.

[Jür03] Jan Jürjens. *Secure Systems Development with UML.* SpringerVerlag, 2003.

[MB07] Marco Casassa Mont and Filipe Beato. On Parametric Obligation Policies: Enabling Privacy-Aware Information Lifecycle Management in Enterprises. In *POLICY*, pages 51–55. IEEE Computer Society, 2007.