Extending Policy Negotiation in User-Controlled Identity Management by Privacy & Security Information Services

– Position Paper Submission to the W3C Workshop on Languages
for Privacy Policy Negotiation and Semantics-Driven Enforcement –

Marit Hansen, Jan Schallaböck
Independent Centre for Privacy Protection Schleswig-Holstein
Holstenstr. 98, 24103 Kiel, Germany

Motivation

For user-controlled identity management privacy policies of services, the user's preferences and a – possibly simple – negotiation process between policies and preferences are important. In advanced concepts for user-controlled identity management systems (IMS) this should be implemented in a machine-readable format (e.g., P3P-based) as far as possible which requires standardization in this field. This clearly will be in the focus of the W3C Workshop on Languages for Privacy Policy Negotiation and Semantics-Driven Enforcement. However, this position paper concentrates on a different issue: Besides the two-party policy-preferences communication which involves the user and the data processing authority, additional information may be relevant for the user to deliberately decide on which personal data to release to whom.

Privacy & Security Information Service

To support the user in managing his/her identities, in particular information on privacy and security risks or incidents may highly be of interest, e.g., concerning protocols, applications, cryptographic algorithms, communication partners, or the IMS software itself. Specific privacy & security information service providers may offer such information, but also the communication partners themselves. In several countries at least in the case of security breaches they are legally required to inform persons concerned.[1]

We propose to realize such information services apart from machine-readable privacy policies because of their different character: While privacy policies usually could be seen as longer-lasting contracts, the additional privacy & security information rather belongs to news items or emergency warnings. The information service could be implemented as RSS feed to be regularly polled by the user's system [2]. Information from the feeds which is relevant for the user could be stored at the user's side and displayed

- when the user is going to disclose data,
- in a transaction log ("Data Track") to understand potential risks related to former transactions,
- immediately when the identity management software being used is vulnerable itself.

[1] As regulated in Security Breach Notification Acts which exist in several US States and are under discussion in the European Commission.

Need for Standardization

Clearly the format of news items and the way for interpretation by the user's system should be standardized. Existing formats, e.g., from the area of security information offered by Computer Emergency Response Teams (CERTs) or other organizations, could be extended to enable machine interpretation for the purpose of identity management support. In a diploma thesis [1] a format for security information feeds has been proposed which among others contains:

- Product concerned (incl. version) and its issuer;
- Description of the vulnerability (incl. priority) and the date of its detection[2];
- Recommendation for action (e.g., countermeasures or specific checks) with information on the effectiveness of the proposed solution;
- Digital signature for authenticity check.

For convenience reasons related warnings should be grouped, and priorities assigned to the feed items could be evaluated together with the user's estimation of reliability of the respective feed provider (i.e. a "trust level" "low", "medium" or "high").

The draft in [1] should be carefully discussed and then further elaborated so that also specific privacy-related information could be addressed appropriately.

Ontologies could help to identity products or components concerned, e.g., if a crypto algorithm (or its implementation) shows weaknesses, it would be good to find out which application software relies on this specific algorithm (or its implementation).

Conclusion

We believe that the work and standardization in the field of privacy & security information services will be increasingly necessary for users to get support in a more and more complex world. As the provided privacy & security information could influence the negotiation process of policies and preferences, this should be taken into account when discussing standardization of policies and negotiation of user-controlled identity management.

References

[1] Antje Nageler: Integration von sicherheitsrelevanten Informationen in ein Identitätsmanagementsystem, Diploma Thesis, Kiel University, May 2006

[2] Ronald Leenes, Simone Fischer-Hübner (Eds.): PRIME Framework Version 2, 27 July, 2006, https://www.prime-project.eu/prime_products/reports/fmwk/pub_del_D14.1.b_ec_wp14.1_V1_final.pdf

[2] Which might be considerably earlier than the publication of the news item.