Privacy Data Envelops for Moving Privacy-sensitive Data

Armen Aghasaryan, Marie-Pascale Dupont, Stéphane Betgé-Brezetz, and Guy-Bertrand Kamga

Alcatel-Lucent Bell Labs
Centre de Villarceaux, Route de Villejust, 91620 Nozay, France
{armen.aghasaryan, marie-pascale.dupont, stephane.betge-brezetz, guy-bertrand.kamga}@alcatel-lucent.com

Position Paper

Privacy is one of the most important issues in our evolving information age where technological developments lead to intensive processing and storage of personal information. In addition to the individual user privacy, we are particularly interested in user group privacy protection which is becoming critical with the recent development of virtual communities both in the domain of private life, e.g., group of friends or members of a family, as well as in the professional area, e.g., members of a project or colleagues of a company [1]. A key characteristic of these environments is given by the fact that large quantities of privacy sensitive data are not just stored at central servers or at end-devices, but these data continuously travel across networks of interconnected applications (via various social networks and communication tools) or move within cloud computing service infrastructures.

To deal with the privacy control of moving data a family of approaches based on sticky policies has been introduced. The basic idea consists in accompanying the moving data with privacy protection policies which should apply all along the movement path of these data [1][3][4]. In this position paper, we advocate an approach within the family of sticky policies that allows dealing with hierarchical data structures as well as covering group privacy protection scenarios. In our approach, named Privacy Data Envelops (PDE), each piece of information identified as privacy-sensitive is embodied (or "enveloped") into a data structure that in addition to the initial raw data carries privacy-related properties and policies. The PDE structure contains three fields, see also Figure 1:

- *Properties or metadata*: specify some semantics on the respective data entities, e.g. the data type and category, owner, issue date.
- *Privacy-sensitive entities* (or sensitive entities): define the parts of raw data that are different from the point of view of privacy; these parts are characterized by their individual properties. Note that in case of a flat PDE structure there is only one sensitive entity which represents the entire set of raw data contained by the PDE (Figure 1, left side). On the other hand, the nested PDE structure (Figure 1, right side) is needed to specify different expected behaviours with regard to different parts of the initial data. For example, under some circumstances certain parts of a given document can be required to be masked (i.e. anonymized); personal identifiers like names or phone numbers need to be removed when diffusing a document to a larger audience.
- *Privacy policies*: indicate which actions are authorized when the PDE travels across the network, (e.g., access control, time-to-live, data handling and disclosure

policies) and which obligations must be fulfilled (e.g., data deletion after a certain time period, notification or consent request to owners). These policies are enforced on each recipient of the PDE.

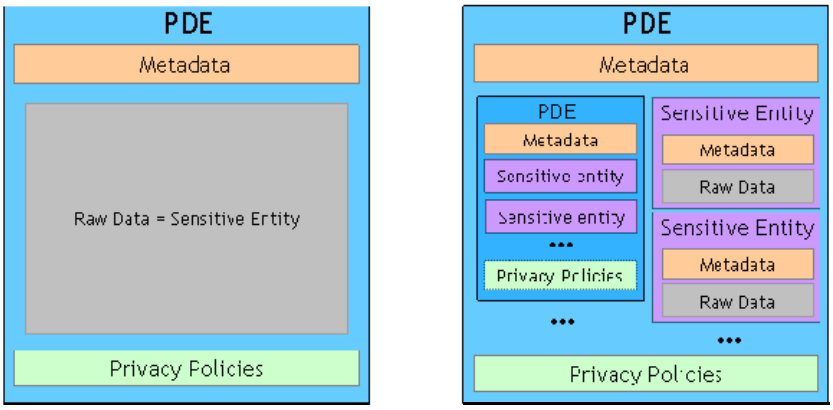

Figure 1: Flat (left) versus nested (right) structures of Privacy Data Envelops.

As examples of group privacy-related data traveling across an infrastructure one can consider the messages exchanged within a group, the documents produced within a group or the list of group members. The problem here is to control the way these data are propagated and used outside of the group. This can be done by policies like "all members must agree before disclosure" (unanimity policy), "the majority of members must agree" (majority policy), or "a particular member must agree" (mouthpiece policy). Of course, these rules would depend on the type of data (e.g., photos, enterprise documents) and their usage context corresponding to the actions intended to be executed (e.g., accessing to data for copying, sending email, publishing photos). A typical scenario in a corporate environment is the exchange of a document within different departments of the same enterprise (considered as user groups) or with other enterprises. The PDE-aware communications tools will then enforce the group policies extracted from the corresponding envelop and prevent inappropriate forwards of the document or other non-authorized actions from being executed.

To conclude, the outlined research study brings answers to recent developments in virtual communities that lead to continuous generation and propagation of privacy-sensitive group data. Furthermore, the massive penetration of cloud computing intensifies the traveling of such sensitive data over the network as well as their dynamic exploitation by various services.

So far we have proposed a cooperative model where different application instances collaborate for enforcement of the specified privacy policies. For that purpose, the existing communication tools can be extended with software components (plugins) allowing to handle the PDE messages and enforce the policies. New applications can support this feature natively by integrating the notion of privacy-sensitive data units at the early stages of their conception.

While allowing to guide the behavior of regular applications with respect to the privacy-sensitive data, the PDE does not yet provide a security mechanism to protect against malicious applications. To achieve it, the presented approach must be combined with DRM encryption or other similar techniques. Finally, last but not least, a wide adoption of such PDE-based technologies and their extension to an open environment requires standardization efforts that would ensure the continuity of user and group privacy control.

References

[1] N. Surendra and A.G. Peace, *A conceptual analysis of group privacy in the virtual environment*, Internation Journal of Networking and Virtual Organisations, Vol.6, n.6, pp. 543-557, 2009.

[2] M. Casassa Mont, S. Pearson and P. Bramhall, *Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services*, Technical Report HPL-2003-49, HP Laboratories, March 2003.

[3] D.W. Chadwick and S.F. Lievens, *Enforcing "Sticky" Security Policies throughout a Distributed Application*, ACM Workshop (MidSec 2008), Leuven, Belgium, December 1-5, 2008.

[4] P. Kodeswaran and E. Viegas, *A Policy Based Infrastructure for Social Data Access with Privacy Guarantees*, In Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks, July 21, 2010.