An Autonomous Social Web Privacy Infrastructure with Context-Aware Access Control

Michael Netter, Sabri Hassan, and Günther Pernul

Department of Information Systems
University of Regensburg
Regensburg, Germany
{michael.netter,sabri.hassan,guenther.pernul}@wiwi.uni-regensburg.de

Abstract. The rise of online social networks (OSNs) has traditionally been accompanied by privacy concerns. These typically stem from facts: First, OSN service providers' access to large databases with millions of user profiles and their exploitation. Second, the user's inability to create and manage different identity facets and enforce access to the self as in the real world. In this paper, we argue in favor of a new paradigm, decoupling the management of social identities in OSNs from other social network services and providing access controls that take social contexts into consideration. For this purpose, we first propose Priamos, an architecture for privacy-preserving autonomous management of social identities and subsequently present one of its core components to realize context-aware access control. We have implemented a prototype to evaluate the feasibility of the proposed approach.

Keywords: Privacy, Online Social Networks, Context-Aware Access Control, Privacy-Preserving Social Identity Management

1 Introduction

Over the last decade, the evolution of the WWW led to a significant growth of Online Social Networks (OSN). While Social Networks have always been an important part of daily life, the advent of Web 2.0 and its easy-to-use services increasingly shift social life to their online counterparts. OSNs provide an infrastructure for communication, information and self-expression as well as for building and maintaining relationships with other users.

However, the rise of OSN services has been accompanied by privacy concerns. Typically, two sources of privacy threats can be distinguished [21]: On the one hand, privacy threats stem from OSN service providers. Currently, the oligopolistic social web landscape leads to few OSN service providers possessing large databases with millions of user profiles. On the other hand, privacy concerns target the challenges of presenting different identity facets of the self in different social contexts and to keep those views consistent. While this bears

resemblance to managing different appearances of the self in the real world, the inherent properties of mediated OSN communication (e.g. permanency and searchability of personal information) put privacy at risk. Although privacy controls are in place to restrict access to personal data today, users seem to be shortsighted concerning future issues of current behavior [20] [10].

To address the aforementioned privacy issues, different research areas evolved. One direction of research are decentralized OSNs that employ user-centric management of digital identities and create a provider-independent social network. While being a promising approach to enhance privacy and data ownership, current implementations such as Diasproa[1] lack user adoption due to high transaction costs of replicating existing identities [10] and strong lock-in effects of established centralized OSNs [5]. Another area of research aims at enhancing privacy within centralized OSNs, e.g. by proposing more fine-grained access controls to enable selective sharing of personal data. Ultimately however, their enforcement depends on the OSN service provider's willingness to adopt these approaches.

To overcome the aforementioned drawbacks, we present a new paradigm of managing social identities in an autonomous, provider-independent manner to enhance users' privacy. We envision identities being decoupled from other OSN services and managed in a user-controlled environment yet integrated into the existing social web landscape. To realize this vision, this paper introduces **Priamos**, an architecture for **Pri**vacy-preserving **a**utonomous **m**anagement **o**f **s**ocial identities and its components. One of the components, a context-aware access control component that facilitates selective sharing of personal information by considering contextual information, is presented in detail. Finally, we present a prototypical implementation of our solution.

This paper contributes to OSN privacy by (1) proposing an architecture for autonomous and privacy-preserving social identity management (PPSIdM), (2) enabling context-aware access control to imitate real world sharing of personal information, and (3) enforcing these access control decisions.

The remainder of this paper is structured as follows. After describing related work in Section 2, we present our autonomous social identity management architecture and its components in Section 3. In Section 4, we focus on one component and introduce a context-aware access control model. Section 5 shows the implementation of the proposed architecture. We conclude the paper in Section 6 with an outlook on future work.

2 Related Work

As shown in Section 1, two major research directions have evolved to face privacy challenges of centralized OSNs, namely decentralization and selective sharing of personal information.

Decentralization and cross-OSNs management of identities has been studied by various research groups [4], [15], [19]. Bortoli et al. [4] propose a web-based

[1] http://www.diasporaproject.org/

application for automatic social network integration, based on globally unique identifiers and semantic web technologies. The authors focus on the decentralized and boundary-crossing management of OSN identities. Similarly, the OpenPlatform proposed by Mostarda et al. [15] aims at improving OSN interoperability. The approach is based on OpenID[2] and uses connectors and converters to access the user's social graphs in different OSNs. The InterDataNet project [19] proposes a distributed data integration approach to support the management of digital profiles. The authors employ an overlay network to uniformly manage personal data in a trustworthy manner. Managing social identities in our autonomous architecture differs from the above systems in the following ways: First, we protect the user's privacy by preventing OSN service providers from getting access to personal data. Second, our architecture enables contextual sharing of personal information and enforcement of access control policies. Third, our approach is OSN agnostic and does not rely on connectors to integrate different OSNs.

Additionally, research [14] shows that selective and context-sensitive sharing of personal information is a key element to enhancing privacy in OSNs. Regarding this, the PrimeLife project [6] has developed two prototypes called Clique and Scramble!. Clique [3] is a prototypical OSN that implements the concept of audience segregation to facilitate the definition of fine-grained access control policies. The Firefox plugin Scramble! [2] is a cryptographic approach to define and enforce access control policies for personal data in OSNs. In contrast to the first prototype, we aim at enhancing privacy within the existing centralized OSN landscape while the second prototype differs from our approach as we aim at managing identities and access to personal information beyond OSN boundaries. To additionally improve selective sharing, OSN-specific access control models have been proposed [13], [7], [8], [1]. The D-FOAF architecture proposed in [13] relies on semantic web technologies and utilizes existing OSNs to define access rights based on the relationship between users, which are described by trust level and path length between requester and resource owner. Similar, the works by Carminati et al. [7], [8] employ semantic web technologies to create a Social Network Knowledge Base (SNKB) that contains OSN related information. Based thereupon, the authors propose a rule-based access control model that takes type, depth and trust level of a relationship into consideration. In [1], Ali et al. propose a social access control model in which objects and subjects are annotated with trust levels and authentication and access to objects is controlled by a trusted third party. Our context-aware access control mechanism differs from the aforementioned approaches in the following two ways: First, for defining contextual access constraints we only regard contextual information provided by the user (e.g. the trust he puts in a contact) to prevent spoofing. Second, unlike the aforementioned approaches that rely on OSN service providers to adapt their models and enforce access control policies, the user-controlled environment of Priamos ensures enforcement.

[2] http://www.openid.net/

3 Priamos architecture

Based on the shortcomings of existing approaches, this section introduces Priamos, an architecture for privacy-preserving, autonomous social identity management. We first present the design characteristics that constitute the foundation of Priamos followed by an in-depth presentation of its components.

3.1 Design characteristics

As aforementioned, neither solely decentralized OSNs (e.g. Diaspora) nor isolated extensions to centralized OSNs (e.g. fine-grained access control models) are sufficient for enhancing OSN privacy. Our analysis underlines these findings stating that a user-centric and user-controlled environment is essential to enforce the user's privacy preferences while integration into today's centralized OSN landscape is mandatory for user adoption, resulting in the following design characteristics. Firstly, **user-centric management of identities** is required to effectively model and enforce the user's sharing and privacy preferences. Currently, most OSN service providers only allow for creating a single identity profile, a paradigm that counters Nissenbaum's concept of acting in different social contexts using different identities [17]. Enabling the user to create multiple (potentially contradicting) identities and allowing for multiple attribute representation (attribute types can have multiple values) enables the user to map his real-world identities to the social web. Additionally, autonomous social identity management fosters identity portability and prevents OSN service providers from profiling [21]. Secondly, **fine-grained access controls** need to be capable of modeling the user's information sharing behavior of the real-world. Controlling access to a user's social identity requires to additionally take contextual properties such as tie strength and temporal restrictions of personal information into consideration. On the contrary, relationships in existing OSNs are initially flat and personal information is persistently stored [18].

Besides those two core characteristics, additional components of Priamos facilitate user awareness and decision making. As research [20] has shown that people are shortsighted about future conflicts of current disclosure of personal information, **logging and awareness** are key requirements of social identity management enabling the user to track previous information disclosure and facilitating the construction of non-conflicting identities. In addition, privacy-invading characteristics of OSN service provider mediated communication, such as persistence and searchability demand **user assistance** to support users in deciding which personal information to share with whom [18].

3.2 Priamos Components and Functionality

Based on the previous design characteristics, this section outlines our proposed autonomous social IdM architecture. Figure 1 provides a high level overview

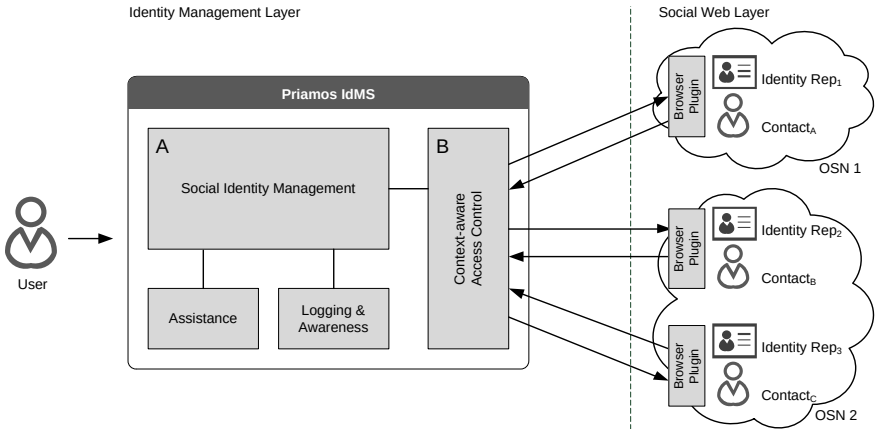


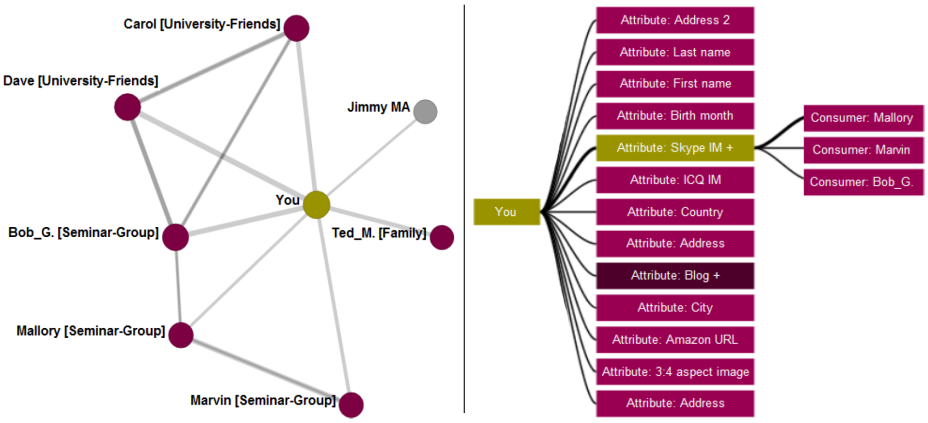
Fig. 1. Priamos architecture and components

which can be divided into two major components: The Priamos Identity Management System (IdMS) and a local browser plugin on the contact's side. Together, both components realize the concept of managing identities in a provider-independent manner while being integrated into the existing OSN landscape.

Priamos IdMS. The Priamos IdMS represents the central element of our architecture and aims at managing the user's social identities in a user-centric and provider-independent manner. It is designed to be either self-hosted or hosted by a trusted third party. Priamos consists of four components to address the design characteristics as presented in Section 3.1. Each of the components is discussed below.

Social Identity Management component The Social Identity Management component (component A in Figure 1) allows for creating personal attributes, which can be bundled to different identity facets. Each attribute value as well as each identity facet is accessible via a unique URL, realizing the concept of URL-based identities. Note that the proposed concept of privacy-preserving, user-centric social identity management and URL-based identities can easily be extended to other, non-OSN services that require access to the user's personal attributes (similar to OpenID, see Section 5 for implementation).

Context-aware Access Control component Additionally, for each attribute fine-grained access control policies can be defined and enforced using the Context-aware Access Control component (component B in Figure 1), which is described in detail in Section 4. The combination of URL-based identities and context-based access control allows for an OSN-agnostic distribution of identities, as the identity representation solely depends on the requester's access rights.



(a) Network View (You, Priamos contacts, OSN contacts) (b) Attribute View

Fig. 2. Visualization of personal data propagation

Logging & Awareness component Building upon defined access policies as well as previous access requests of the user's contacts, the Logging & Awareness component aims at increasing the user's awareness and understanding of flow and distribution of personal information using visualization techniques. Thereby, it enables the user to construct future identities that do not confer with existing identities and keep a consistent self-image [12]. In Figure 2, the two main visualization techniques of Priamos are depicted. Figure 2(a) depicts a graph-based view on the user's network, showing Priamos contacts as well as contacts from existing OSN that have been imported. The network view enables the user to capture the relations between his contacts and thereby understand potential flows of shared personal information. Besides, in Figure 2(b), a tree-like attribute view is offered. Using this visualization, the contact's having access to the user's personal information can be visualized on a per-attribute basis. This enables the user to easily track which contacts have access to which attributes and thereby facilitates transparency.

Assistance component Additionally, the Assistance component supports the user in constructing and maintaining different social identities. This comprises means to automatically propose groups of semantically similar contacts and thereby facilitate audience segregation and targeted sharing of personal information, which we have presented in [16].

Browser Plugin. In order to realize the concept of URL-based identities, the browser plugin is an auxiliary tool that is preconfigured and provided by the Priamos user and installed at his contacts side. While a contact is surfing the web, its goal is to detect identity URLs, to resolve their value and embed it

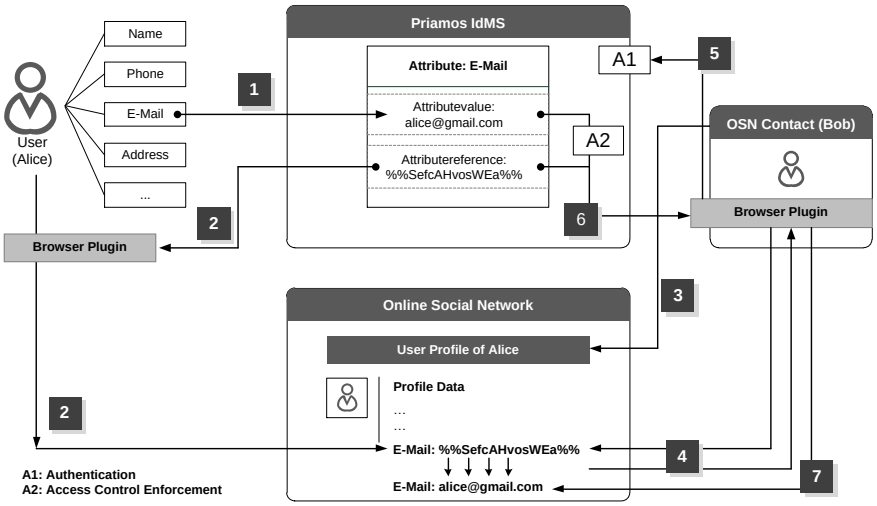


Fig. 3. Attribute definition and access workflow

on the fly into the current website. It is designed to work completely in the background with no user interaction required. Its design as a browser plugin makes this component completely agnostic in terms of the visited website.

3.3 Personal attribute definition and access workflow

This section outlines the workflow of defining and accessing personal information using the Priamos architecture. Prior to this, the user is able to import contacts from existing OSNs using a built-in connector. Subsequently, each of the user's contacts is provided with a preconfigured browser plugin, containing the required access tokens (see Section 5 for details). Thus, the initial distribution of access tokens is not within the scope of this work, but can easily managed by other communication channels such as E-Mail. Figure 3 depicts the workflow for a single personal attribute that is subsequently described. First, the user logs in his Priamos instance account to create a new attribute type (e.g. E-Mail), enters the corresponding value and assigns access rights for this attribute (1). Internally, a Base64-encoded URL, referencing the attribute value, is created. Next, the user employs a browser-based wizard that is included in the browser plugin to seamlessly add the attribute to his social network profile (e.g. on Facebook) which completes the user-related tasks (2). Eventually, one of the user's OSN contacts visits his social network profile (3). In the background, the browser plugin detects the encoded URL in the DOM[3] tree (4) and initiates an OAuth-based[4] authentication process with the user's Priamos instance (5). If successful, predefined access control policies for the request are evaluated and enforced (A2

[3] http://www.w3.org/DOM/
[4] http://oauth.net/

in Figure 3). If access is granted, the attribute value is returned (6) and the BASE64-encoded URL in the DOM tree is replaced by the corresponding value (7). It is notable that Steps 4-7 require no interaction an thus are completely transparent to the contact.

4 Context-aware Access Control Component

As shown in Section 1, sharing personal information is highly contextual, i.e. depending on different factors such attending people and the user's goals. However, existing OSNs support contextualization only to a limited extent. To overcome these limitations, in this section we built upon the previously introduced autonomous and user-controlled architecture for social IdM and outline our *Context-aware Access Control component* (Component B in Figure 1). We first introduce a conceptualization of context for OSNs and subsequently describe the characteristics of the component. Therein, rather than aiming at a formal definition, we focus on the in-depth presentation of defining and applying contextual constraints with the ultimate goal to imitate the situation-dependent sharing of personal information of the real world.

4.1 Conceptualization of context in OSNs

Defining context in OSNs is a prerequisite for a context-aware access control model, however to the best of our knowledge, no conceptualization of context for sharing personal information in OSNs exists. To define context in OSNs, we built upon the generic definition of Zimmermann et al. [22], introducing the contextual dimensions *Individuality*, *Activity*, *Location*, *Time*, and *Relations*.

In OSNs, we define *Individuality* to comprise information on the user's attributes, such as profile data, that create a desired identity facet. The *Activity* dimension comprises information on the user's goals. In OSNs common goals are, for instance, maintaining relationships and impression management. Both aforementioned contextual dimensions are covered by our user-centric social IdM component (see component A in Figure 1) by supporting users in shaping their online identities according to personal preferences (for instance by allowing for multiple attribute representation).

The three dimensions *Location*, *Time* and *Relations* contain contextual information helping a user to adapt the amount and type of personal information to be shared in a specific situation and thus are important sources for our context-aware access control component. The *Location* dimension describes the digital equivalent of a physical space in the real world, which is created by grouping people, a feature which is already available in many OSNs and therefore not described more detailed in the remainder. Besides, sharing personal information is often temporally bound to the situation a user is currently in. Thus, the *Time* dimension captures lifetime and temporal restrictions of information sharing. Finally, the *Relations* dimension describes users connections to other OSN users within a context. A relation can be characterized in terms of level of trust, describing the tie strength between the user and a contact.

4.2 Applying contextual constraints in Priamos

Based on *Time* and *Relations*, we introduce three types of contextual constraints for our access control component, whereas additional constraints can easily be added. Note that (as in the real world) people can store or simply remember personal information while available. Thus these constraints do not aim at preventing a contact from accessing and copying personal information while available but rather at increasing the transaction costs to do so.

Temporal constraints (Time). In the real world, a situation exists only at a specific point in time and personal information shared in this situation is usually ephemeral [18]. In order to transfer this real world concept to OSNs, we introduce two types of temporal constraints: Expiry date and time period. While the former sets a specific date until which a personal attribute is accessible, the latter specifies a timeframe for granting access.

Quantitative constraints (Relations). A common motivation for joining OSNs is to build new relationships but at the same time, users are afraid of stalking and cyberbulling [9]. To resolve this paradox, we propose to quantitatively constrain access to personal attributes by allowing the user to set the number of granted access requests per contact and per attribute before access is denied.

Social constraints (Relations). In addition, the binary conception of friendship of most OSNs does not reflect the different tie strengths of relationships in the real world [18]. To overcome this shortcoming of flat relationships, we propose to assign a trust value (specified by the user and representing the tie strength) to each contact and constrain access to personal attributes based on this trust value.

4.3 Context-aware access control in Priamos

To implement the previously defined contextual constraints, we adapt the Core RBAC standard [11] in Figure 4 using the notation of OSNs (e.g. contacts and personal attributes). For the sake of simplicity, we do not consider sessions and read access is the only operation available. A major difference to the Core RBAC model lies in the role-permissions assignment relationship. In the Core RBAC model, permissions are statically assigned to a role, i.e. each role member has the same permissions. Likewise, in our model each contact that is member of a role (corresponds to groups in OSNs) is assigned a set of permissions. However this set of permissions is additionally constrained by contextual parameters at runtime, arriving at a constrained permission set.

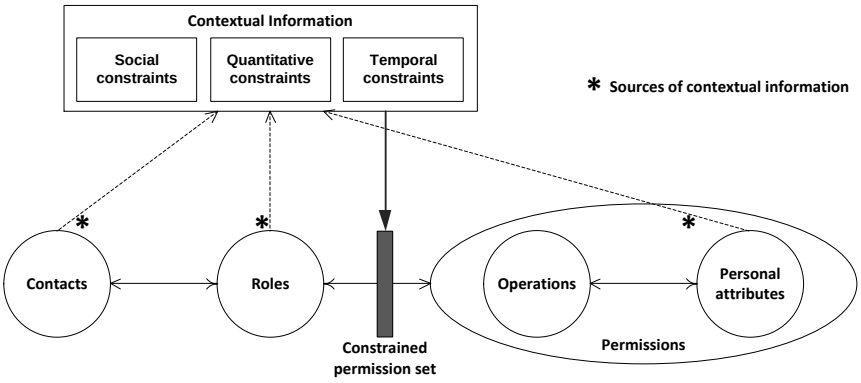


Fig. 4. Context-aware access control model, based on the Core RBAC model [11]

Contextual constraint specification. Contextual constraints are specified while defining access rights for personal attributes (Step 1 in Section 3.3 and implementation in Figure 5). We define three different sources of contextual information, whereupon access permissions can be further restricted, namely *Contacts*, *Roles*, and *Personal Attributes* (Figure 4). For each *Contact*, the user specifies a trust value (ranging from 0.0 - 1.0) that represents the tie strength of this relationship. Additionally, the minimum required trust value to access a single *Personal Attribute* (or a set of attributes representing an identity facet) can be assigned **(social constraints)**. To improve usability, a default trust value can be assigned to a *Role* that is inherited by each role member if no separate trust value has been assigned. Besides, Priamos allows for specifying the maximum number of permitted access requests for each *Contact* and *Personal Attributes*, i.e. the visibility of an identity facet can be limited in terms of pageviews, e.g. to prevent stalking **(quantitative constraints)**. Finally, **temporal constraints** can be specified for a single *Personal Attribute* or a whole identity facet. The user can set an availability period for personal attributes and specify an expiration date, after which access is denied.

Contextual constraint enforcement. To effectively enforce access control policies and contextual constraints, each contact must authenticate with the user's Priamos instance (A1 in Figure 3). We employ an OAuth-based authentication for our implementation (see Section 5) which is completely handled in the background by the browser plugin. After authentication, the contact's role is selected and the set of permissions is determined. Role assignment is a prerequisite for access, i.e. each contact must be member of a role to access personal attributes. For each of a contact's requests for personal attributes, contextual parameters are determined at request time (such as the contact's trust level and the attribute's minimum required trust level). Based thereupon, the set of permissions is additionally constrained if one or more requirements are not met.

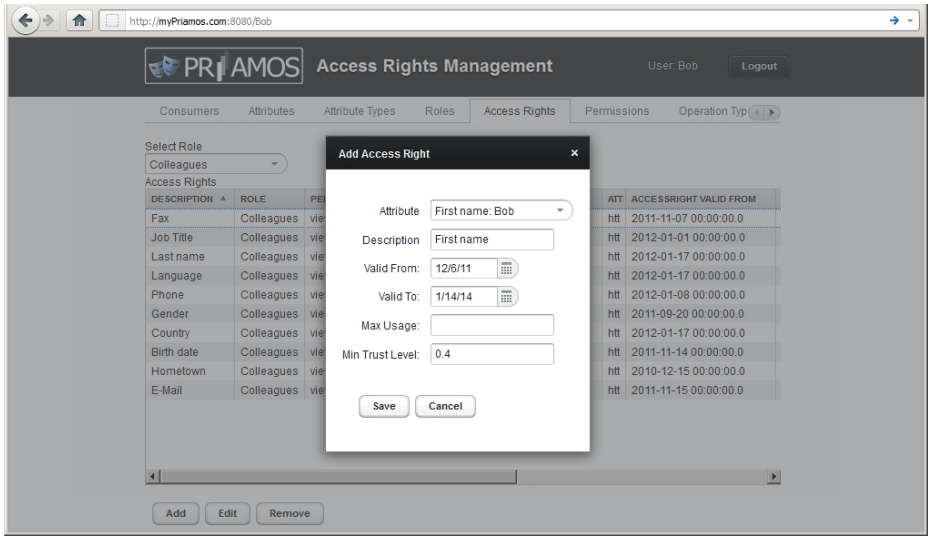


Fig. 5. Priamos IdMS implementation

Access is granted if the constrained set of permissions is sufficient for accessing the requested attributes, otherwise access is denied.

5 Implementation

We have implemented the proposed Social IdMS with context-aware access control to evaluate the feasibility of our approach. As we envision our IdMS to be either self-hosted or by a trusted third party, it is designed as a Web Application Archive (WAR) File that can easily be deployed at any provider. Our implementation is based on Java EE 6. For the backend we have implemented RESTful webservices with OAuth authentication to access personal information. The client-side browser plugin is implemented for Firefox and integrates a Javascript-based OAuth client to communicate with the Priamos IdMS.

To demonstrate the functionality of our approach, consider a simplified scenario in which Bob employs his Priamos IdMS instance to create various identity facets for different user audiences. One of those audiences are Bob's four work colleagues (Alice, Carol, Dave and Ted) with whom he wants to share only parts of his personal information. Out of all his personal attributes Bob thus selects his *first name*, *last name* and *relationship status* as being visible for the role *work colleagues*. However, Bob additionally restricts access to his relationship status on the basis of a trust value using the Priamos context-aware access control component. Only colleagues with a minimum trust value of 0.8 shall be allowed to access his relationship status. Carol, Dave and Ted are Bob's trusted long-term work colleagues (trust value=1.0). Alice, however, only recently joined Bob's team and thus Bob assigns a lower trust value of 0.5 to her. After defining

those constraints, a Base64-encoded URL value is added to Bob's Social Network Profile (e.g. his Facebook profile) using Priamos IdMS. Alice has installed the Priamos Browser-Plugin provided by Bob that contains the required OAuth tokens. Eventually, Alice visits Bob's social network profile. In the background, the Browser-Plugin detects the Base64-encoded Identity URLs and sends an OAuth request to Bob's Priamos instance (Request in Listing 1.1). Priamos employs the OAuth consumer key and secret to authenticate Alice and to activate the *work colleague* role. Subsequently, the contextual constraints are evaluated and access to Bob's relationship status is denied as Alice's trust level is below the required minimum trust level of 0.8. Priamos' response (Response in Listing 1.1) thus contains only the remaining two attributes (Bobs' first and last name).

Identity request (OAuth)

```
GET /resources/Bob/attributes HTTP/1.1
Host: myPriamos.com:8080
Authorization: OAuth realm="http://myPriamos.com:8080/resources/Bob/attributes/",
    oauth_consumer_key="e856c3ec6c32b6b603c87c4286160657",
    oauth_token="4f9377815b41b34e7704038cc823d20e",
    oauth_nonce="9BiRV7",
    oauth_timestamp="1325521195",
    oauth_signature_method="HMAC-SHA1",
    oauth_version="1.0",
    oauth_signature="g0qaRUpJUaAHjvQCqkc0sLqFK9w"
```

Identity response (JSON format)

```
{ "oauth_consumer_key":"e856c3ec6c32b6b603c87c4286160657",
  "AttributeSet":[
  { "axSchemaURI":"http://axschema.org/namePerson/first",
    "value":"Bob",
    "label":"First name"
  },
  { "axSchemaURI":"http://axschema.org/namePerson/last",
    "value":"Dylan",
    "label":"Last name"}
  ]}
```

Listing 1.1. OAuth-based identity request and response

6 Conclusions

Currently, OSNs users are confronted with the dilemma that fully exploiting the benefits of OSNs requires to increasingly provide personal data to commercially-driven service providers and rely on their insufficient tools to manage identities consistently. To improve privacy, in this paper we argued for a paradigm shift where identity information is decoupled from other OSN services and managed in a user-controlled environment. Therefore, we introduced Priamos, an architecture for autonomous management of social identities, that (1) prevents centralized OSN providers from accessing personal information, (2) allows for more accurate sharing of personal information by considering context information and (3) enforcing these decisions. For the future, we envision OSN service providers to focus on value-added services to attract users and provide interfaces to seamlessly integrate their users' social identity management systems to access infrastructural services, such as for the purpose of user discovery. Moreover the use of such external social identity management systems allows individuals to

use their personal data for multiple purposes and application domains beyond OSNs like expert search systems and collaboration platforms. With users being faced to deal with identity management tasks it seems that user privacy does not come without expenses. At least the effort users bring up on managing their identity is well spent considering that they remain in control of their data and that they are even able to use it for multiple purposes. With regard to the effort users have to spent usability aspects shift into focus. Ideally users should be given a hand to manage their identity in an intuitive and less time consuming manner whilst supporting them in access control decisions by the provision of tools that assist the user (e.g. by offering recommendations) and that have been crafted with usability aspects in mind. From a technical point, future work will focus on automatically adjusting the contacts' trust values over time and to support the user in defining an online situation by suggesting proper contacts and an appropriate identity facet addressing the need for usabillity enhancements.

Acknowledgments

The research leading to these results is partly funded by the European Union within the PADGETS project under grant agreement no. 248920. Any opinion, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the European Union.

References

1. Ali, B., Villegas, W., Maheswaran, M.: A trust based approach for protecting user data in social networks. In: Proceedings of the 2007 conference of the center for advanced studies on Collaborative research. pp. 288–293. ACM (2007)
2. Beato, F., Kohlweiss, M., Wouters, K.: Scramble! your social network data. In: Fischer-Hübner, S., Hopper, N. (eds.) Proceedings of the 11th international conference on Privacy enhancing technologies. pp. 211–225. PETS'11, Springer (2011)
3. van den Berg, B., Leenes, R.: Audience Segregation in Social Network Sites. In: Proceedings of the 2010 IEEE Second International Conference on Social Computing. pp. 1111–1116. SOCIALCOM '10, IEEE Computer Society (2010)
4. Bortoli, S., Palpanas, T., Bouquet, P.: Decentralised social network management. International Journal of Web Based Communities 7(3), 276–297 (2011)
5. Boyd, D.: Taken Out of Context: American Teen Sociality in Networked Publics. Ph.D. thesis, University of California, Berkeley (2008)
6. Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.): Privacy and Identity Management for Life. Springer (2011)
7. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: A semantic web based framework for social network access control. In: Proceedings of the 14th ACM symposium on Access control models and technologies. p. 177. ACM, New York (Jun 2009)
8. Carminati, B., Ferrari, E., Heatherly, R., Kantarcioglu, M., Thuraisingham, B.: Semantic web-based social network access control. Computers & Security 30(2-3), 108–115 (2011)

9. Doruer, N., Menevi, I., Eyyam, R.: What is the motivation for using Facebook? Procedia - Social and Behavioral Sciences 15, 2642–2646 (Jan 2011)
10. Edwards, L., Brown, I.: Data Control and Social Networking: Irreconcilable Ideas? Harboring Data: Information Security, Law, and the Corporation pp. 202 – 228 (2009)
11. Ferraiolo, D.F., Sandhu, R., Gavrila, S., Kuhn, D.R., Chandramouli, R.: Proposed NIST standard for role-based access control. ACM Transactions on Information and System Security 4(3), 224–274 (2001)
12. Goffman, E.: The Presentation of Self in Everyday Life. Anchor (1959)
13. Kruk, S., Grzonkowski, S., Gzella, A., Woroniecki, T., Choi, H.C.: D-FOAF: Distributed Identity Management with Access Rights Delegation. In: Proceedings of the Asian Semantic Web Conference, pp. 140–154. Springer (2006)
14. Leenes, R.: Context is Everything - Sociality and Privacy in Online Social Network Sites. In: Bezzi, M., Duquenoy, P., Fischer-Hübner, S., Hansen, M., Zhang, G. (eds.) Privacy and Identity, IFIP AICT 320. pp. 48 – 65. Springer (2010)
15. Mostarda, M., Zani, F., Palmisano, D., Tripodi, S.: Towards an OpenID-based solution to the Social Network Interoperability problem. In: W3C Workshop on the Future of Social Networking (2009)
16. Netter, M., Riesner, M., Pernul, G.: Assisted Social Identity Management - Enhancing Privacy in the Social Web. In: Proceedings of the 10th International Conference on Wirtschaftsinformatik (2011)
17. Nissenbaum, H.: Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford Law Books (2010)
18. Peterson, C.: Losing Face: An Environmental Analysis of Privacy on Facebook. SSRN eLibrary (2010)
19. Pettenati, M.C., Ciofi, L., Parlanti, D., Pirri, F., Giuli, D.: An Overlay Infrastructural Approach for a Web-Wide Trustworthy Identity and Profile Management. In: Salgarelli, L., Bianchi, G., Blefari-Melazzi, N. (eds.) Trustworthy Internet, pp. 43–58. Springer (2011)
20. Tufekci, Z.: Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites. Bulletin of Science, Technology & Society 28(1), 20–36 (2008)
21. Ziegele, M., Quiring, O.: Privacy in Social Network Sites. In: Trepte, S., Reinecke, L. (eds.) Privacy Online. Perspectives on Privacy and Self-Disclosure in the Social Web, pp. 175–189. Springer (2011)
22. Zimmermann, A., Lorenz, A., Oppermann, R.: An operational definition of context. In: Proceedings of the 6th international and interdisciplinary conference on Modeling and using context. pp. 558—-571. Springer (2007)