TPIM: Transparent Privacy-Enhanced Identity Management of Web Services

Yong Yang[1,2*]

[1]School of Computer Science, University of Electronic Sci. & Tech. of China, China
[2]Department of Computing, Macquarie University, Australia
yongyang@ics.mq.edu.au

Abstract. The growth of web services has been accompanied by sharing more and more users' personal information with service providers, which has raised concern about possible malicious or accidental unauthorized abuse of user information. This paper focuses on how we can give the user a deep sense of safety, privacy and certainty about service invocations in the diverse and heterogeneous computing environment. We present *Transparent privacy-enhanced Identity Management of Web Services* (TPIM), a privacy-enhanced personal Identity Management architecture for web services users. TPIM is an extension of SOAP specification, which provides a sense of "circle of trust" in the identity management during the collaborations of web services. It enables that user's identity or personal data to adapt to be accessible only to whom they trust. In other words, a user can put his or her personal information on any web services and maintain privacy in different user-defined security level (including up to unconditional anonymity) as well.

1 Introduction

People are expected to remember different organization-specific user names and passwords in the online world. Identity management systems seek automated solutions for managing their identities by making them transferable across organizational boundaries. However, an increasing sharing personal information with service providers concerns the user with risks to privacy. Aside from the end-users' privacy, if the system is perceived as privacy infringing, it will endanger the reputation of involved service providers, which may lead to loss of profits in the long run.

Research has shown that how to manage the identities in web services and maintain user's privacy is really a challenge. Many efforts are made at "domain-centric" identity management, in which users have no control, and suffer from the identity theft or fraud. So scientists shift focus onto the dimensions of users control, where there is no universal agreement to date.

* This work was performed during the author's scientific visit at Department of Computing, Macquarie University, Australia.

In this paper we investigate a *transparent privacy-enhanced Identity Management* (*TPIM*), which enables the users have total control over the management of their identities. In order to enhance users' privacy, the SOAP standard is extended and a TPIM framework supporting "Single sign-on"(SSO) is proposed, which allows the user to access multiple sets of resources after being authenticated just once. It provides users with a more seamless user-experience when accessing different user accounts on the Internet.

To sum up, this paper makes the following main contributions:

- Id-based Ring signature is introduced and adapted to support unconditional anonymity. Even if ID information is leaked later on, the user can not be identified. Meanwhile the control of privacy preserving shifts from the third party to users themselves, which greatly increases users' confidence and promotes privacy.
- The SOAP architecture is extended to enhance privacy in web services. The user can manage her own profiles and have a total control on her identities. The user can set different levels of security identity. For example, a user may use a set of credentials or id name to access her blog with security level 1, a second set to discuss work with her colleagues with security level 2, a third set to purchase goods online with security level 3. Besides, a novel rule model is presented to exploit the privacy policies on both the organizational and execution levels.

2 RELATED WORK

Privacy in general has been exploited for years. However, privacy in web services is still under development. Research to date has been focused on developing privacy languages. Rezgui et al. [5] investigate the feasibility and provable reliability of privacy preserving solutions for web service infrastructures. Yee [9] and Ni et al. [3, 4] designs privacy controllers together with user privacy policies to protect privacy. Squicciiarini et al. [8] provide a set of assertions to define the privacy related properties. But none of them addresses the issue of enforcing privacy that confirms to emerging industry standards. Most commercial available systems such as Microsoft .Net Passport and Liberty Alliance can be improved on the user-friendly feature. Without consideration of unconditional anonymity, [2] presents a personal Identity Management, which can be a complement with privacy enhancement.

In cryptography, Sharmir [7] introduced the notion of identity-based (ID-based) cryptography to solve the certificate management problem, which is supposed to provide a more convenient alternative to the traditional public key infrastructure (PKI). Ring signature [6] is a type of digital signature that can be performed by any member of a group of users that each has keys. But it can not be determined which of the group members' keys was used to produce the signature. The combination of ID-based cryptography and ring signature schemes has been well-studied in the recent research. Chow et al. [1] proposed a high efficient construction of ID-based ring signature, which only needs two pairing computations for any group size.

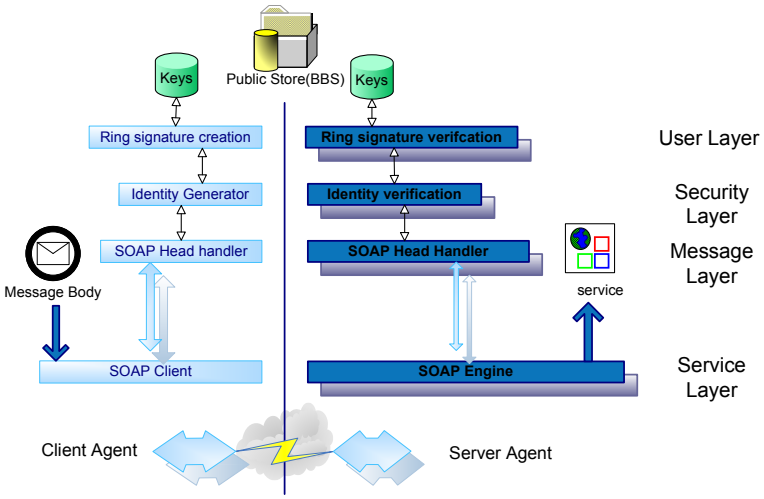

Fig. 1. Privacy-enhanced framework

3 Architecture of TPIM

3.1 Design and usage scenario

The general idea of unconditional anonymity in TPIM is to hide the user's identity in a group S during service invocations. Figure 1 illustrates the architecture for our TPIM framework. In order to be convenient for leveraging applications software, our framework does not break any existing services by acting as add-on components, which guarantees easy integration with existing web-based applications. Specifically, TPIM agents will probe in the network layer and snatch SOAP packages during the monitoring. Once identity related packages are intercepted, they are forwarded to user space to reconstitute the conversation for further judgement. After identity verification, the packages are either dropped or injected back to network layer. All the procedure are well encapsulated and executed in the background, making it completely **transparent** to the end-user.

We extend SOAP specification to support security and privacy features discussed in this paper. The <wsse:security> head blocks are designed to carry privacy related attributes:

- **ValueType**: A string identification label defines the value space and type of the encoded binary data. The value we have chosen for our anonymous group identification security token is "IdBasedRingSignature".
- **EncodingType**: It defines the encoding format of the binary data. In our protocol it is set to "wsse:Base64Binary" to denote a base64 encoding.
- **NameID**: This element describes the group S which the user choose to hide in. To promote privacy, make sure the members within their lifespan during the period of invoking. We can use colon (:) marks to concatenate all the identifiers of individuals in the group S. For instance, if such group includes three persons: Alice, Bob and Lily, the NameID should be "Alice:Bob:Lily".

– **Conditions**: Conditions must be evaluated when assessing the validity of the assertion. *NotBefore* and *NotOnOrAfter*, together with *IssueInstant* define the exact lifetime of the assertion.
– **AttributeSatement**: It asserts a multi-valued attribute associated with the authenticated principal. In the response assertion, all the group public keys information is linked by colon (:) with each other in the same order of NameID element. For instance, the attribute values for Alice, Bob and Lily may be "XD6s. . . :ZCCA. . . :ors. . . ". In addition, the correspondent life expectancy is further supplied to assure the validity of each individual.

An example of a SOAP header containing anonymous group identification is presented in Figure 2. This extension gives rise to an additional payload required for encoding anonymous identification tokens in SOAP request that is proportional to the size of the group the user belongs to.

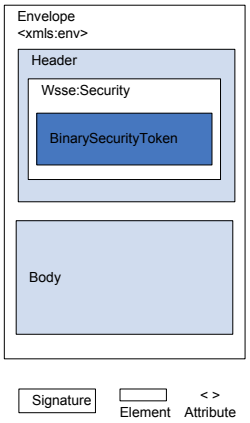

Fig. 2. SOAP extension

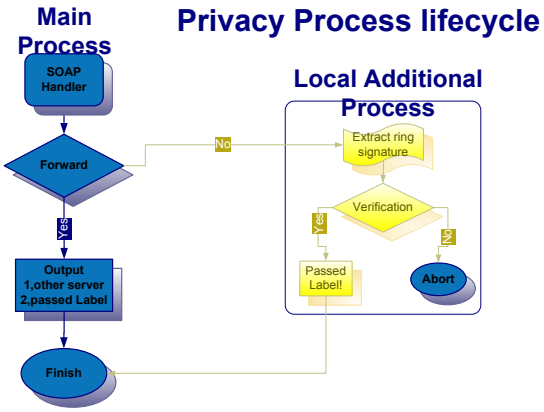

Fig. 3. Privacy enhanced structure

3.2 Privacy enhanced process

During the invocation, when the user issues a SOAP request toward Web services, the message is implicitly intercepted and processed by the client agent. This handler invokes the identity generator module and prepends the resulting identification token together with a timestamp to the SOAP header blocks of the outgoing request. The identity generator will comply with user's directive and bind the request to corresponding identity profile. For example, in the highest security user profiles, the Id-based ring signature is produced to attain unconditional anonymity.

Whenever the service provider receives a SOAP request from client agent, the server side agent is implicitly invoked to determine whether the request should be accepted or not. If the request is for an authorized Web Services and no group-relevant identification information are provided then it is rejected by raising a *SecurityTokenUnavailable* SOAP fault. In the case that the timestamp reported

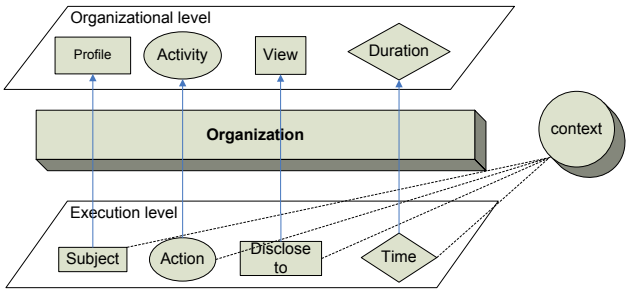

Fig. 4. rule model for TPIM

in the request is older than a fixed security time interval the request is rejected with *FailedAuthentication* SOAP fault. Otherwise, the identification request is processed by identity verification module. If the verification is successful then the service request is executed and the response is returned to the application client. Otherwise, a *FailedAuthentication* SOAP fault is sent back to the requesting client. A representation of the privacy process life-cycle is depicted in the Figure 3. In order to avoid the flow peak in SOAP header request, we forward privacy process to other available server agents for load-balancing.

3.3 A TPIM rule model

As shown in Figure 4, a rule model is designed to facilitate user's privacy policy setting under web service circumstances. Each security policy is defined for and by an organization. Thus, the specification of the security policy is completely parameterized by the organization so that it is possible to handle simultaneously several security policies associated with different organizations. The model is not restricted to identity permissions, but also includes the possibility to specify other identity related information such as priorities.

The rules are context sensitive, so the policy could be expressed dynamically at two different levels.

1. *Organizational level*: The users defines privacy rules through abstract entities (profile, activity, view, duration) without worrying about how each organization implements these entities.
2. *Execution level*: When a user login in other organization, the execution authorizations are granted (or not) to him according to the execution rules. TPIM maps from organizational level to execution level for further elaborate control.

The derivation of invocation policies can be formalized as : Rule $\Gamma = Permission \times \Upsilon \times H$ while $Permission(s, \alpha, d, t, c)$ is defined as $\forall$ subject $s \in S$, performs action $\alpha \in A$, login on to disclose-to service $d \in V$, at time $t \in D$.

- Profiles S: A set of identity profiles in different security levels.
- Activity A: A set of aims of identity requests.

– View V: a set of other services whom the identity information can be disclosed to.
– Duration D: A set of durations of validity with regard to identity information.
– Privacy level Υ: The identity information should be protected at different privacy level such as whether it allows service providers to store user's identity information.
– Handling H: Once the identity information is breached, what approaches should be issued to notify the user of the risk, such as sending an email or an alert. The event-based approach is well suited for services' distributed environments. Apart from the regular infrastructure, the design will facilitate measures to integrate accounting and notification support.

4 Conclusion

We have introduced Id-based ring signature into web services and extended the SOAP standard to achieve privacy enhancement. The user can have sufficient control on her privacy. It provides a more user-friendly and efficient ways of managing digital identities and enables people to assert their privacy rights in the online world. As future work, we will develop a tool to simulate the rule model and perform conflict detection to help the designer to refine rules.

References

1. S. S. M. Chow, S.-M. Yiu, and L. C. K. Hui. Efficient identity based ring signature. In J. Ioannidis, A. D. Keromytis, and M. Yung, editors, *ACNS*, volume 3531 of *Lecture Notes in Computer Science*, pages 499–512, 2005.
2. T. M. Eap, M. Hatala, and D. Gasevic. Enabling user control with personal identity management. *scc*, 0:60–67, 2007.
3. Q. Ni, D. Lin, E. Bertino, and J. Lobo. Conditional privacy-aware role based access control. In *ESORICS '07: Proceedings of the 12th European Symposium On Research In Computer Security*, pages 72–89. Springer, 2007.
4. Q. Ni, A. Trombetta, E. Bertino, and J. Lobo. Privacy-aware role based access control. In *SACMAT '07: Proceedings of the 12th ACM symposium on Access control models and technologies*, pages 41–50, New York, NY, USA, 2007. ACM Press.
5. A. Rezgui, M. Ouzzani, A. Bouguettaya, and B. Medjahed. Preserving privacy in web services. In *WIDM '02: Proceedings of the 4th international workshop on Web information and data management*, pages 56–62, New York, NY, USA, 2002. ACM.
6. R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In C. Boyd, editor, *ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, 2001.
7. A. Shamir. Identity-based cryptosystems and signature schemes. *Proceedings of CRYPTO*, 84, 1984.
8. A. C. Squicciarini, A. A. Hintoglu, E. Bertino, and Y. Saygin. A privacy preserving assertion based policy language for federation systems. In *SACMAT '07: Proceedings of the 12th ACM symposium on Access control models and technologies*, pages 51–60, New York, NY, USA, 2007. ACM.
9. G. O. M. Yee. A privacy controller approach for privacy protection in web services. In *SWS '07: Proceedings of the 2007 ACM workshop on Secure web services*, pages 44–51, New York, NY, USA, 2007. ACM.