Enhancing Privacy on Identity Providers

Rafael Weingärtner Carla Merkle Westphall

Department of Informatics and Statistics
Networks and Management Laboratory
Federal University of Santa Catarina
Florianópolis, Brazil
Email: {weingartner, carla}@lrg.ufsc.br

***Abstract*—Cloud computing is widely used to provide on demand services as a consequence of its benefits such as reduced costs, structure flexibility and agility on resource provisioning. However, there are still people that are not comfortable with the idea of sending their sensitive data to the cloud such as the personally identifiable information (PII) that could be used to identify someone in the real world. Moreover, there have been cases of data leaks, which resulted in huge losses both for companies and its clients. Therefore, this article addresses the security and privacy aspects of identity management. We present a model that tackles privacy issues within the PII that is stored on identity providers (IdPs). Thus, our proposal supports users and improves theirs awareness when disseminating PIIs.**

Keywords–Cloud Computing; Security; Privacy; Federation; Identity providers;

I. Introduction

Cloud computing is been largely adopted to provide services to industry. As presented in [1] and [2], the reduced costs, flexibility and agility are the main characteristics for the widespread successful of cloud computing. However, there are people that are not comfortable to send their sensitive data to the cloud [3]. Moreover, it is pointed out by the Cloud Industry Forum in [2] that when the cloud is in discussion there are huge debates not about the technology aspect per se, but rather about the commercial and governance issues that relate to data security and privacy.

Users have the right to be skeptic about the privacy and security aspects of that model. Hence, there have been recent cases of data breaches and leaks as noticed in [4] [5] [6], which resulted in identity data leaks. Therefore, as pointed by Betgé-Brezetz, Kamga, Dupont and Guesmi in [7] cloud service providers should focus on protecting sensitive data than on tight security perimeters, hence, the biggest threat may be internal.

Sánchez, Almenares, Arias, Díaz-Sánchez and Marín in [8] and De Capitani di Vimercati, Foresti and Samarati in [9] discussed that as soon as users' data is on identity providers (IdP) the control on how that data is disclosed, stored and used is lost. Moreover, data stored in the cloud may be sensitive and if linked with its owner identity may violate his/her privacy.

This paper addresses some security and privacy aspects of identity providers. In one side, we tackle the lack of control that users have over their identification data (PII) that is stored on identity providers. On the other side, it is proposed an enhancement in the dissemination process to support users with their PII data disclosure, in a way that it is lowered the risks of unaware/unintentional data dissemination.

The rest of this paper is structured as follows. Section II gives a brief overview of the concepts that are going to be used throughout this paper. Section III presents and discusses related works. Section IV describes the issue that is going to be addressed and presents our proposals. Section V closes the paper with the conclusions and future works.

II. Background

In order to provide a better understanding of the issue that is being addressed and the proposed model, this section presents a brief overview on each concept that will be used throughout the rest of this paper.

A. Privacy

Landwehr and et al. in [10] defines privacy as the control of release of personal data that users have. Furthermore, privacy is a fundamental human right as pointed out by United Nations (UN) in its universal declaration of humans rights [11]. In addition, the Human Rights Council reinforced that the same right that people have off-line must also be protected on-line [12].

Therefore, privacy is a vital characteristic that has to be considered into every system. Identity provider systems should not be an exception and have privacy added into its design.

In addition, Diaz and Gürses presented in [13] three different paradigms of privacy:

- Privacy as a control – privacy violations are often associated with disclosure of data to third parties. In this context, privacy technologies provide individuals with means to control the disclosure of their information and organizations with means to define and enforce data security policies to prevent abuse of personal information for unauthorized purposes. Thus, the main goal of this paradigm is to provide users with control and oversight over collection, processing and use of their data;
- Privacy as confidentiality – the previous paradigm relies on the assumption that organizations that collect and process users' data are completely honest. However, once data is under the control of an organization, it is hard for individuals to verify how their data is being used. This paradigm aims to prevent information disclosure, focusing on minimizing the information

disclosed in a way that cannot be linked to users identity;

- Privacy as practice – this paradigm views privacy in a social dimension, as users make privacy decisions often based on how their social groups make those decisions. In this context, technologies strive to make information flow more transparent through feedback and awareness, enabling a better individual and collective understanding on how information is collected, analyzed and used.

Moreover, there are plenty of legislations that aim to protect users' privacy in the Internet and communication systems. In Europe, there is the Data Protection Directive [14], in USA, we have the Health Insurance Portability and Accountability Act (HIPAA) [15], the Gramm-Leach-Bliley Act [16], the Children's Online Privacy Protection Rule [17] and in Brazil, it was recently approved the Internet Bill of Rights[18]. All of those aforementioned acts aim to protected users against unwilling data disclosure and processing.

B. *Identity management*

Identity management can be defined as the process of managing users' identity attributes [19]. Moreover, Hansen, Schwartz and Cooper in [20] stated that identity management systems are programs or frameworks that administer the collection, authentication, and use of identity and information linked to identity. Thus, it provides means to create, manage and use identities' attributes.

Bertino and Takahashi in [21] presented the roles that exist in an identity management system:

- Users – entities that want to access some kind of service or resource;
- Identity – set of attributes that can be used to represent a user, it is also called personally identifiable information (PII);
- Identity provider (IdP) – provide means to manage users' attributes. It delivers users' PIIs to service providers;
- Service provider (SP) – delivers the resource/service desired by a user. It delegates the process of authentication to IdPs and usually is responsible for the authorization process.

Therefore, identity management systems are the frameworks, which enable users to properly manage their PIIs. Thus, they enable users to access resources and services using identification data that is stored in identity providers, from which a subset of the identification attributes may be disclosed to service providers.

In this context we also have the concept of federation, which is define by Chadwick in [19] as an association of service providers and identity providers. Furthermore, Orawiwattanakul, Yamaji, Nakamura, Kataoka and Sonehara in [22] said that a federation allows users to access resources in multiple administrative domains (ADs) by initially authenticating with their home AD instead of authenticating with the accessed one.

Therefore, identity federation is a set of standards and technologies that enable the exchange of identities in a secure way between different administrative domains.

Shibboleth [23] is one of the tools that can be used to create a federation; it uses Security Assertion Markup Language (SAML) to exchange data between IdPs and SPs. In one hand, it has an IdP module that is developed in Java and can cope with distinct data repositories, such as databases, Lightweight Directory Access Protocol (LDAP) and Central Authentication Service (CAS). On the other hand, its SP module is developed in *C* as a module for the Apache Web Server and it is used to manage the access control of a protected resource.

Shibboleth [23] has a plug-in called uApprove.jp, which is presented in [22] that provides users with some means to manage PII disclosure and some feedback about the reasons of the data collection. Figure 1 presents the Shibboleth's with its plug-in uApprove.jp work flow. Each step is described as follows:

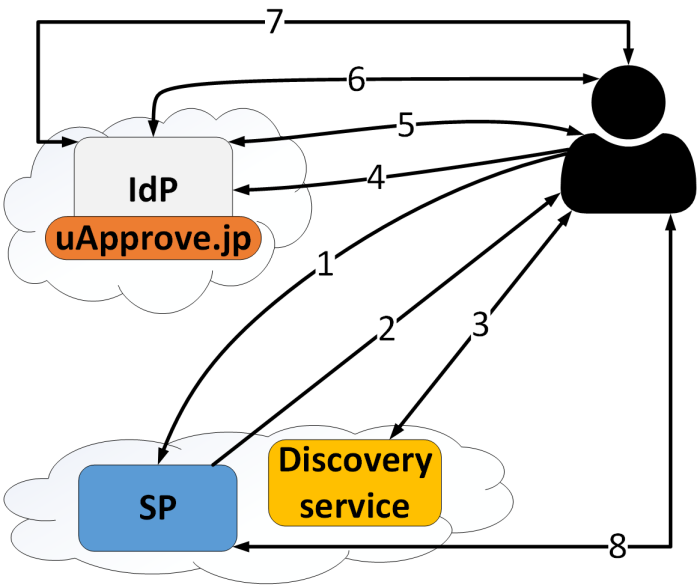


Figure 1. Shibboleth + uApprove.jp workflow

1) Unauthenticated users by means of a browser access a protected resource;
2) The service provider sends users to the discovery service (DS) in which they have to choose an IdP that has their attributes;
3) Users submit to DS the IdP they are enrolled. The DS starts the session initiators at the protected resource and sends users to the selected IdP;
4) IdP answers the request and presents users with a login page in which they have to enter their credentials;
5) Users present their credentials that are checked upon the IdP database. If the authentication process ends with success, the IdP presents users with SP's terms of usage (ToU), which users should read and accept;
6) After the ToU acceptance, users are presented with an attribute release page of uApprove.jp, which will display user's attributes from which the user can select/unselect the optional ones, accordingly to she/he will.
7) The IdP creates an assertion with the result of the authentication and user's attributes that were chosen

by the user to be disclosed, which is sent to the SP through the users' browser;

8) With the authentication confirmation and some PII data the SP can deliberate about the resource delivery.

There are other tools that can be used to create federations such as OpenAM and OpenId Connect. This paper uses Shibboleth for its widespread adoption in the academia and because it is developed and maintained by the Internet 2 foundation as a free open source framework to build federations.

III. Related work

Switch in [24] developed a plugin to Shibboleth IdPs that provides awareness of data disclosure when accessing some resource/service. However, users cannot select which data is going to be disclosed, the user has either to agree or disagree with the PII dissemination.

Orawiwattanakul, Yamaji, Nakamura, Kataoka and Sonehara in [22] tackled the lack of control on PII disclosure in cloud federations. It proposed an extension of [24] that would enable users to select among all non-mandatory attributes which ones they wish to disclose to the SP that is being accessed. This way, it guarantees that data disclosure is happening with user consent.

In a different approach to deal with privacy in cloud, Sánchez, Almenares, Arias, Díaz-Sánchez and Marín in [8] proposed a reputation protocol that weights the reputation of entities in a federation in order to support data disclosure. This way, users can check SPs reputations among the federation before they send any data to it. It is also provided a way in which users would have the ability to check what is being done with their data, and based on that they could lower or increase the provider reputation.

Betgé-Brezetz, Kamga, Guy-Bertrand, Mahmoud and Dupont in [25] addressed the cloud privacy and security issues in which users send data to cloud providers without any guarantee that it is going to be secured in a proper way. As Sánchez, Almenares, Arias, Díaz-Sánchez and Marín did in [8], it was proposed a o define if a user trusts or not a cloud provider and the level of trust. Based on how much the user trusts the cloud provider, he/she could send data in plain text, partially encrypted (encrypted with some metadata in plain text) or fully encrypted to the cloud. It was also proposed a package called PDE (Privacy Data Envelope) to carry users' data to the cloud. That package could hold the data (encrypted or not) with some policies that state how, where, by whom and when that data can be used.

Works [8] and [25] suffer from the same problem, a SP with a good reputation does not mean that it is not vulnerable to attacks, and that it is taking all the required measures to guarantee users privacy.

As an alternative to previous presented works, Chadwick and Fatema in [26] addressed the lack of means to create access policies for data stored in the cloud and the absence of standards to apply such policies defined not just by users, but also, by countries where data is stored. It was proposed a series of web services that would analyze policies that are uploaded within the data before any action is executed. Therefore, once an application receives a request to process some data, it should consult the proposed web services if it can proceed with the requested action.

TABLE I. PROPERTIES OF WORKS

Publications		Characteristics				
Reference	Year	Use of cryptography	Based on reputation	Use of Policies	Awareness of data disclosure	Disclosure support
[24]	–				X	
[22]	2010			X	X	
[8]	2012		X			
[25]	2012	X	X			
[26]	2012			X		
[7]	2013	X	X	X		
Our proposal	2014	X		X	X	X

Betgé-Brezetz, Kamga, Dupont and Guesmi in [7] combined the approached of reputation presented in [25] with policies presented in [26]. Its proposal addresses privacy issues of cloud computing in an end-to-end fashion way. It used stick policies with the PDE proposed in [25] to carry all together policies and data to the cloud. The proposal consists in adding on cloud service providers points that evaluate those policies before using the data, these points are called data protection module (DPM), which would guarantee the evaluation of defined policies before any process is made with the data. It is also defined that the PDE containing the policies and data would just be sent (processed, copied and stored) into cloud nodes that have the DPMs modules deployed.

Works [7] and [26] experience the same problem, that is the lack of guarantee that a provider is truly obeying the proposed models. Users do not have means to check if the protection modules were developed, deployed and are working properly.

Having presented the related works, we can categorize the papers that were presented into the following properties:

- Use of cryptography – use of cryptography to store data at a provider;
- Based on reputation – use of reputation to back up users' decision of which data and how it is sent to SPs;
- Use of Policies – policies that regulate how data is used/disclosed at a provider;
- Awareness of data disclosure – provide feedback to make users aware of data dissemination;
- Disclosure support – provide means to support users when they are disseminating data from an IdP to a SP.

Table I matches the properties shown above with the ones found in presented related works. Therefore, it can be noticed that our proposal combines the properties found in related works, striving to enhance the support and privacy in identity providers.

IV. Enhancing privacy on identity providers

This section discusses and presents the issues that are being addressed. Thus, it introduces our proposals to tackle those problems.

A. Privacy issues

There are legislations [14] [15] [16] [17] [18] and guidelines create by Jansen and et al. [27] and Security Alliance in [28] to address privacy issues that arise in information systems. Those laws and standards aim to guarantee users rights over their data. Furthermore, works [7] [8] [22] [24] [25] [26] tried

to address some of the issues that exist when data is stored out of users boundaries. However, there are still a lack of models and mechanisms:

- Lack of control over user's PII – users do not have effective means to manage their data that is stored in identity providers;
- Disclosure support – as presented in a research by Zhang and et al. in [29] people could not successfully define their personal information disclosure policies. Therefore, there should be created a way to support users when they are disseminating PII information.

The lack of control that users have over their sensitive data gets worse once they migrate to cloud services. As presented by Mather, Kumaraswamy and Latif in [30], once organizations have migrated to the cloud they lose control over their structure used to host services. Moreover, Zhang and et al. discussed in [31] that loss of control can lead to data leaks as a consequence of curious/malicious system administrators of the underlying structures.

B. *Working with privacy in identity providers*

Our proposal uses the concepts of privacy described by Diaz and Gürses [13], striving to minimize data disclosure and provide means for users to effectively control personal data disclosure. Thus, it makes the flow of data more transparent providing users awareness of data dissemination.

In addition, users are responsible for data entered into IdPs, which is then used to access some service provided by an SP. Thus, users should have means to proper control data disclosure, and that process must be improved to be more transparent for its users.

Therefore, we extended the federation framework presented earlier. In one hand, we added templates for data dissemination to support users with the PII disclosure. On the other hand, we used the cryptography approach to store PII data encrypted in IdPs.

Our model is presented in Figure 2, users would enter their PII data into IdP providers encrypted with some key, therefore, the disclosure process had to be extended to allow users to open the data they wish to disseminate. We propose that layer of protection over the PII data, in order to make it harder to access and disseminate that data without users' awareness and consent.

We also created a way in which users can send their preferences for data dissemination to IdPs in order to ease and secure the disclosure process. As pictured in Figure 2, those preferences would be created as policies written in XML, they would be drawn by entities such as security labs, privacy commissioners and security experts of the area who hold the knowledge of which data can cause more or less harm to users' privacy if disclosed.

The process of data dissemination from IdPs to SPs was extended to cope with our proposal of templates for data dissemination. The dissemination process has to use the proposed templates to support users with data disclosure.

Therefore, our proposal adds new objects into the model of identity management of the Shibboleth framework. Each object and its role is described as follows:

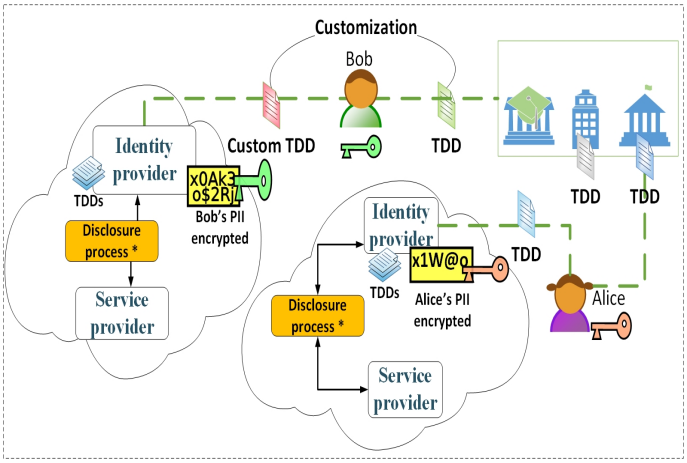


Figure 2. Enhancing privacy on identity providers.

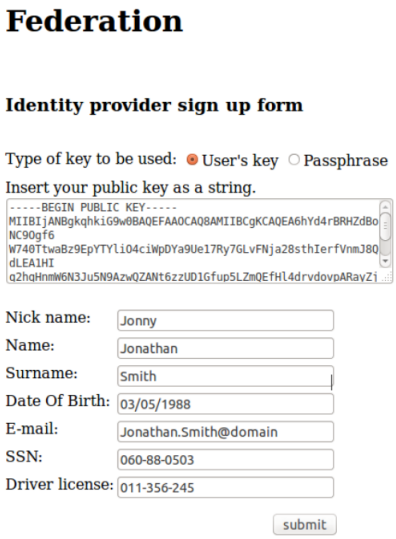
- Template data dissemination (TDD) – it is the template which users can get from entities that the user trust, customize if needed (as Bob does in Figure 2) and enter it into IdPs to help them manage their PIIs release. It guides users throughout the disclosure process with different granular configuration to different SPs;
- Cryptography Keys – are the keys used to encrypt and decrypt users PII that is store in the IdP. Users would encrypt their PIIs before sending them to IdPs with Key I, and during a transaction when some PII data is needed users would be asked to open that data with key II in order to disseminate it to a SP.

The following subsections present the extensions that we developed in order to make Shibboleth IdP and its uApprove.jp plugin cope with our proposals. We divided the work into addressing the loss of control on users PIIs and adding support to users at the disclosure process.

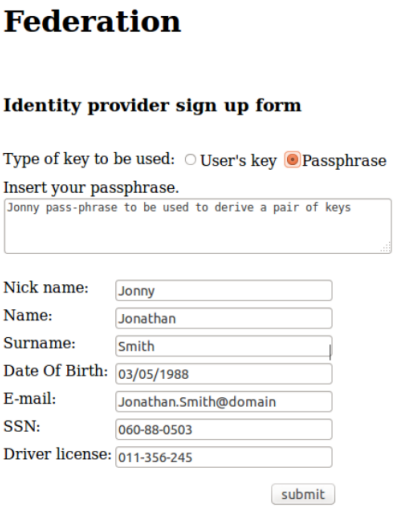
1) Addressing the loss of control on users PIIs: Papers [7] [31] [26] suggested that there could be curious/malicious internal entities into providers (SP and IdP) with privileges and technical means to harm users privacy. Therefore, we propose to store users' PIIs into IdPs encrypted in a way that just the user can decrypt the data and use it.

We did not propose any way to deal with this situation at the SP side at this moment. In one hand, because as argued by Chadwick in [19] if the fair principles of data collection and minimization are followed the SP will just receive a pseudonym and some data that by themselves do not give any hint about the user's identity. On the other hand, because the IdP concentrate all the sensitive information needed to link a system user to a person. Furthermore, as presented by De Capitani di Vimercati, Foresti and Samarati in [9], data per se is not sensitive, what is sensitive is its association with an identity.

We developed a tag library using Java Web technologies to be used as a basic framework to create forms in which users would enter their PII data as they usually do when creating an account in some IdP system as shown in Figure 3. However, the data that is sent to the IdP will be encrypted with some key, just the password and the login would not be encrypted, as they are needed to execute the authentication process.

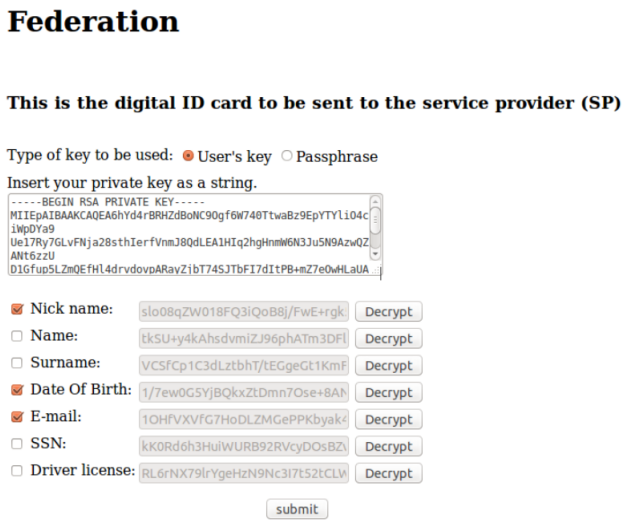


(a) User's public key.

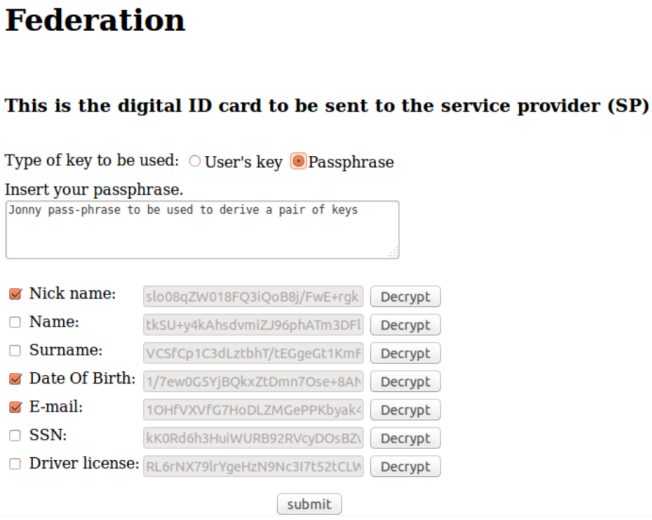


(b) Key derivation from passphrase.

Figure 3. Privacy enhanced sign up forms for IdP.



(a) User's private key.



(b) Key derivation from passphrase.

Figure 4. User decrypting data to send to SP.

The framework we developed gives the following options to users when asking for a key:

- Use a public key – the user can choose to enter a public key that she/he already has as the key to encrypt the PII data, as shown in Figure 3(a);
- Use a pass-phrase – users can enter a pass-phrase that is used to derive a pair of keys from which we take the first one and encrypted their data before sending them to the IdP, as depicted in Figure 3(b).

Both of the aforementioned approaches are performed at the client side, the user's keys are never sent to the IdP server. Thus, to encrypt the data at the client site we used the web programming language Javascript with libraries Cryptico [32] and pidCrypt [33] respectively when users desire to use a passphrase or a public key to encrypt her/his data. Thus, both libraries are based on the Javascript cryptography library developed by Wu [34].

Our proposal inserts data into the IdP encrypted. Thereby, we had to change the flow of message presented in Figure 1, hence the IdP would not have users' PII in clear text anymore. It was needed an extension to enable users to decrypt the data that is going to be sent to SPs as pictured in Figure 4.

If the user selected to send data encrypted with a pass-phrase or a public key, there will be some difference when we decrypt the PII needed to send to the SP.

In one side, if users selected to encrypt data with a public key, when the decryption is required we ask them for a private key as depicted in Figure 4(a). On the other side, if they chose to encrypt data with a key derived from a pass-phrase, we then ask for the pass-phrase to derive the keys, from which we use the second key generated to decrypt the data as pictured in Figure 4(b).

2) Adding support to users at the disclosure process: Birrell and Schneider discussed in [35] that the control of PII dissemination can be inconvenient forcing users to decide which data can be sent to which SP every time they access a new service. Furthermore, Zhang and et al. in [29]

demonstrated that users usually fail to successfully define their data disclosure policies. Thus, Hansen, Schwartz and Cooper in [20] argued that one single default setting would not suit properly every user needs. Therefore, we proposed the use of TDDs based on different user types, this way, we could have different TDDs, enabling users to customize data disclosure in a granular way. The TDDs developed in XML look like the document presented in Figure 5.

```
<?xmlversion="1.0"encoding="UTF?8"?>
<templateDataDissemination
xmlns="http://privacy.lrg.ufsc.br/tdd"
xmlns:xsi=
"http://www.w3.org/2001/XMLSchema?instance" xsi:schemaLocation="
http://privacy.lrg.ufsc.br/tdd
http://privacy.lrg.ufsc.br/tdd-1.0.xsd">
<spDomain>sp.domain.com</spDomain>
<spAttributesBehaviours>
       <attributeBehaviour>
              <attributeName>name</attributeName>
              <selectedByDefault>true</selectedByDefault>
       </attributeBehaviour>
       <attributeBehaviour>
              <attributeName>lastName</attributeName>
              <selectedByDefault>true</selectedByDefault>
       </attributeBehaviour>
       <attributeBehaviour>
              <attributeName>email</attributeName>
              <selectedByDefault>false</selectedByDefault>
       </attributeBehaviour>
       <attributeBehaviour>
              <attributeName>SSN</attributeName>
              <selectedByDefault>false</selectedByDefault>
       </attributeBehaviour>
       <attributeBehaviour>
       <!-- Any other we use false -->
              <attributeName>*</attributeName>
              <selectedByDefault>false</selectedByDefault>
       </attributeBehaviour>
</spAttributesBehaviours>
</templateDataDissemination>
```

Figure 5. Example of TDD

Thereby, we extended the Shibboleth IdP to use the TDDs shown above. This way, when users reach the process of PII disclosure, they will be presented with a page in which the attributes to be disclosed will already be selected/deselected.

V. Conclusion

While papers [8] [25] and [7] [26] tried to manage privacy in the cloud respectively by assessing cloud service providers reputation and creating sticky policies within data, our proposal tackles the lack of control of users' PIIs into IdPs and the lack of support when disclosing PIIs to SPs, respectively by encrypting PIIs into IdPs and using templates for data dissemination to support users when disclosing data.

Our proposal avoids curious and malicious system administrators to gather users' PII data without permission in IdPs. If an administrator accesses the data repository she/he will not be able to retrieve any relevant data about a user identity, hence, that sensitive information will be encrypted.

Furthermore, our proposal is a lightweight extension on top of Shibboleth identity provider and its uApprove.jp plugin, which works transparently to SPs, thence, all of the extensions were developed at the IdP. Moreover, once the proposal is deployed it can prevent PII data leaks that cause identity theft and the correlation of big data processing with a specific user's identity without her/his consent.

In addition, this paper focused on tackling some privacy issues in identity providers, there are still issues to be dealt with at the service provider side, such as means to control attributes that were released from an IdP to a SP. Our proposal of personas to manage the granular release of users PIIs has the goal to lower the risks that arise with the dissemination of certain combination of attributes. It does not protect privacy by itself; users are still vulnerable to malicious SPs that may collude to profile a user identity in a federated environment. Therefore, as a future works we intend to investigate means to enforce users privacy in service providers.

As a next step to be taken in our research we will extend the OpenId Connect federation protocol, in order to add our proposals. The OpenId Connect protocol uses JSON instead of SAML (XML), which makes it easier to use in mobile environments in which XML processing can become a problem. We also intend to investigate the possibility to use web semantic into our proposals, to ease the adaptation of systems already developed and to decouple identity management models and protocols from the technology aspect.

Acknowledgment

The research is funded by the Brazilian Funding Authority for Studies and Projects (FINEP) under the Brazilian National Research Network in Security and Cryptography project (RENASIC) and conducted at the virtual laboratory of secure implementations (LATIM) at the Federal University of Santa Catarina (UFSC) in the Networks and Management laboratory (LRG).

References

[1] P. Hall, "Opportunities for csps in enterprise-grade public cloud computing," OVUM, May, 2012.

[2] C. I. Forum, "Uk cloud adoption and trends for 2013," Tech. Rep., 2013. [Online]. Available: http://cloudindustryforum.org/downloads/whitepapers/cif-white-paper-8-2012-uk-cloud-adoption-and-2013-trends.pdf

[3] S. Srinivasamurthy and D. Liu, "Survey on cloud computing security," in Proc. Conf. on Cloud Computing, CloudCom, vol. 10, 2010.

[4] M. Helft, "After breach, companies warn of e-mail fraud," The New York Times, Abril 2011, retrieved: February, 2014. [Online]. Available: http://www.nytimes.com/2011/04/05/business/05hack.html

[5] D. Kocieniewski, "Adobe announces security breach," The New York Times, Outubro 2013, retrieved: February, 2014. [Online]. Available: http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html

[6] C. Sang-Hun, "Theft of data fuels worries in south korea," The New York Times, Janeiro 2014, retrieved: February, 2014. [Online]. Available: http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html

[7] S. Betgé-Brezetz, G.-B. Kamga, M.-P. Dupont, and A. Guesmi, "End-to-end privacy policy enforcement in cloud infrastructure," in Cloud Networking (CloudNet), 2013 IEEE 2nd International Conference on. IEEE, 2013, pp. 25–32.

[8] R. Sánchez, F. Almenares, P. Arias, D. Díaz-Sánchez, and A. Marín, "Enhancing privacy and dynamic federation in idm for consumer cloud computing," Consumer Electronics, IEEE Transactions on, vol. 58, no. 1, 2012, pp. 95–103.

[9] S. De Capitani di Vimercati, S. Foresti, and P. Samarati, "Managing and accessing data in the cloud: Privacy risks and approaches," in Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on. IEEE, 2012, pp. 1–9.

[10] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau, and M. E. Lesk, "Privacy and cybersecurity: The next 100 years," Proceedings of the IEEE, vol. 100, no. Special Centennial Issue, 2012, pp. 1659–1673.

[11] H. Lauterpacht, "Universal declaration of human rights, the," Brit. YB Int'l L., vol. 25, 1948, p. 354.

[12] H. R. Council, "The promotion, protection and enjoyment of human rights on the internet (a/hrc/20/l.13)," 2012, retrieved: February, 2014. [Online]. Available: http://ap.ohchr.org/documents/alldocs.aspx?doc_id=20280

[13] C. Diaz and S. Gürses, "Understanding the landscape of privacy technologies," Extended abstract of invited talk in proceedings of the Information Security Summit, 2012, pp. 58–63.

[14] E. Directive, "95/46/ec of the european parliament and of the council of 24 october 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data," Official Journal of the EC, vol. 23, no. 6, 1995, retrieved: February, 2014. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[15] U. S. Congress, "Health insurance portability and accountability act of 1996," 1996, retrieved: February, 2014. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW-104publ191/html/PLAW-104publ191.htm

[16] U. Congress, "Gramm-leach-bliley act," 1999, retrieved: February, 2014. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

[17] U. S. F. T. Commission, "Children's online privacy protection rule," 2013, retrieved: February, 2014. [Online]. Available: http://www.gpo.gov/fdsys/pkg/FR-2013-12-20/html/2013-30293.htm

[18] C. Civil, "Lei nº12.965, de 23 abril de 2014," 2014, retrieved: July, 2014. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

[19] D. W. Chadwick, "Federated identity management," in Foundations of Security Analysis and Design V. Springer, 2009, pp. 96–120.

[20] M. Hansen, A. Schwartz, and A. Cooper, "Privacy and identity management," Security & Privacy, IEEE, vol. 6, no. 2, 2008, pp. 38–45.

[21] E. Bertino and K. Takahashi, Identity Management: Concepts, Technologies, and Systems. Artech House, 2011.

[22] T. Orawiwattanakul, K. Yamaji, M. Nakamura, T. Kataoka, and N. Sonehara, "User-controlled privacy protection with attribute-filter mechanism for a federated sso environment using shibboleth," in P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2010 International Conference on. IEEE, 2010, pp. 243–249.

[23] Shibboleth, "What's shibboleth?" retrieved: July, 2014. [Online]. Available: https://shibboleth.net/about/

[24] SWITCH, "uapprove - user consent module for shibboleth identity providers," retrieved: June, 2014. [Online]. Available: https://www.switch.ch/aai/support/tools/uApprove.html

[25] S. Betgé-Brezetz, G.-B. Kamga, M. Ghorbel, and M.-P. Dupont, "Privacy control in the cloud based on multilevel policy enforcement," in Cloud Networking (CLOUDNET), 2012 IEEE 1st International Conference on. IEEE, 2012, pp. 167–169.

[26] D. W. Chadwick and K. Fatema, "A privacy preserving authorisation system for the cloud," Journal of Computer and System Sciences, vol. 78, no. 5, 2012, pp. 1359–1373.

[27] W. Jansen, T. Grance et al., "Guidelines on security and privacy in public cloud computing," NIST special publication, vol. 800, 2011, p. 144.

[28] C. Alliance, "Security guidance for critical areas of focus in cloud computing v3. 0," Cloud Security Alliance, 2011.

[29] Q. Zhang, Y. Qi, J. Zhao, D. Hou, T. Zhao, and L. Liu, "A study on context-aware privacy protection for personal information," in Computer Communications and Networks, 2007. ICCCN 2007. Proceedings of 16th International Conference on. IEEE, 2007, pp. 1351–1358.

[30] T. Mather, S. Kumaraswamy, and S. Latif, Cloud security and privacy: an enterprise perspective on risks and compliance. " O'Reilly Media, Inc.", 2009.

[31] W. Han-zhang and H. Liu-sheng, "An improved trusted cloud computing platform model based on daa and privacy ca scheme," in Computer Application and System Modeling (ICCASM), 2010 International Conference on, vol. 13, Oct 2010, pp. V13–33–V13–39.

[32] R. Terrell, "An easy-to-use encryption system utilizing rsa and aes for javascript." 2012, retrieved: May, 2014. [Online]. Available: https://github.com/wwwtyro/cryptico

[33] Pidder, "pidcrypt – a javascript crypto library." retrieved: May, 2014. [Online]. Available: https://www.pidder.de/pidcrypt/

[34] T. Wu, "Rsa and ecc in javascript." 2009, retrieved: May, 2014. [Online]. Available: http://www-cs-students.stanford.edu/~tjw/jsbn/

[35] E. Birrell and F. B. Schneider, "Federated identity management systems: A privacy-based characterization," IEEE security & privacy, vol. 11, no. 5, 2013, pp. 36–48.