An Analysis of Seven Concepts and Design Flaws in Identity Management Systems

João José Calixto
Cesar.edu
CESAR – Center for Advanced Studies and Systems
Recife, Brazil
e-mail:calixtounicap@gmail.com

Felipe Silva Ferraz
Informatics Center
Federal University of Pernambuco
Recife, Brazil
e-mail:fsf3@cin.ufpe.br

***Abstract* –Identity management uses models to accredit, manage and use digital identities. These models connect isolated islands of authentication and authorization systems in a federated system. However flaws in the design and concept of these models, such as identity theft and even users' lack of confidence in truly using these models, can lead systems that use its benefits to being non-successful on the market. This article presents an analysis of seven design and concept flaws of the identity management model of the main tools on the market, including Security Assertion Markup Language (SAML), OpenID, Microsoft CardSpace and an academic framework called Inter-Cloud Identity Management (ICEMAN).**

Keywords-Identity Management; flaws; Identity; design; Security.

I. INTRODUCTION

The huge transformation that cloud computing prompted within the IT industry made software development as a service more attractive [1]. This large-scale paradigm cut out the need for large investments [2]. The transparency of the services provided by the cloud is a key point of this supply-side paradigm [3].

Cloud computing combines virtualization and service-oriented architecture (SOA) in order to provide shared services with regard to computing, data storage, software, applications or for a business [4][5]. However, the resource capacity of a single cloud is finite, so cloud computing has been migrating to a perspective of InterClouds, namely an environment in which several clouds can be configured that can communicate with each other and share data and services.

There are identification mechanisms for each service hosted in cloud computing environments and these make use of solutions for user authentication. However, this approach leads to user fatigue as users must memorize logins and passwords [6]. A study in 2007 on password habits showed that typical web users have on average 27 accounts that require a password, and they type eight passwords per day [7]. Therefore this results in users registering similar or even identical logins and passwords for different types of services [7]–[9]. Another problem associated with user authentication and identification is the disclosure of users' personal information after they are successfully identified in a service.

In this scenario, the identity management (IdM) is needed to mitigate and resolve some of these issues. IdM is a set of technologies and processes that enable computer systems to distribute identity information and delegate tasks by using one or more domains with more security [4][10]. Identity management in cloud computing environments is primarily responsible for authenticating users and supporting access based on his/her attributes. IdM for InterClouds can be represented by a single authentication system can be deployed in heterogeneous clouds [11].

Identity management systems are complex and offer all parties involved, powerful features so as to facilitate the mechanism for identities, credentials, personal information, and to present such information to third parties. These systems can bring about potential failures [12].

This article studies major flaws in the concept, usability and design of the most popularly successful identity management systems on the market, namely OpenID [13], Security Assertion Markup Language (SAML) [14], Microsoft CardSpace InfoCards [15] and an academic framework called Inter-Cloud Identity Management (ICEMAN) [16].

The paper is organized as follows. Section 2 gives a short overview of identity management. Section 3 describes the seven flaws of design in identity management systems, while Section 4 discusses the identity models themselves and their flaws are the topic of Section 5. Finally, in Section 6, conclusions are drawn and recommendations outlined.

II. IDENTITY MANAGEMENT

An identity is defined by an entity or group of entities (a person, computer, organization, etc.) represented solely within a specific scope. Yet much can be derived from the definition. Which are entities and how each identity be uniquely identified? Entities may be objects, or, as in most cases a personal identity.

In each context we have different attributes that make up the identity of how we ourselves are identified. What identifies us are the attributes we possess. Different attributes of identity lead to different entities being identified. In such contexts, we can assume an identity, such as a driver's license number coupled with an the 2-letter code of a Brazilian state. Another simple example is our national, Brazilian ID, which has a numeric record and a fingerprint. All these identities cited are merely a set of attributes that if not inserted in a context and certified lose their objective, which is assertively to identify the user who gives such information is who that user purports to be. In this scenario, we can perform an analogy with our digital identities, which consist of identifying attributes such as login and password, which, if not inserted in the correct context, are not valid.

Identity management, or IdM, consists of the process and all technologies associated with this to accredit, manage, and use digital identities [17]. In the most common models for an identity management, three parties are highlighted: users, identity providers (IdP) and relying Parties (RP) [4][18].

There are centralized identity models, ie where there is only one authority as IdP that performs authentication and authorization actions and there are also decentralized models, which have more than one IdP [19]. Some examples of decentralized identity management systems are the OpenID, SAML and Microsoft CardSpace. In this article, we will focus on non-centralized identity management systems because they do not require a previous relationship between RP and IdP.

III. SEVEN FLAWS OF CONCEPT AND DESIGN

To be successful in the market, identity management systems must win the trust of users and RPs. For this to occur, the systems must improve security, simplify the control of the flow of personal information, and most important of all, simplify process for authenticating, identifying and checking credentials. The seven failures presented below are topics that should be addressed so that the public absorbs the use of identity management systems to a greater extent [12].

A. Identity management is not the main goal

A user simply wants to utilize the functionality of his/her website. Identity management systems should aim to facilitate those tasks by including features such as security and privacy, but these features that are aggregated with an IdP are considered secondary. Usually functions that offer long-term gain are less valued [20]. Some identity management systems offer time saving features, such as automated form-filling, simplification such as single sign-on, or high-value reputation, all of which can be leveraged across many sites. However, these benefits are often perceived as “secondary” [20].

B. Users follow the path of least resistance

The key to maximizing the direct cost is to construct systems that are easily adopted. This includes processes of authentication and interface with the password, which should become easier compared to current standards. When the technology interferes with desired activities, users tend to create shortcuts to circumvent the security embedded in the process [21][22]. For the success of identity management systems to be successful, users should find them easy, accurate and safe to use them and configure them.

C. Cognitive Scalability is as equally important as technical scalability

Today users undergo so-called password fatigue. They have approximately 25 accounts and they can type 8 passwords a day [7]. To avoid burdening their memory in this way, users generally choose the same logins and similar passwords for various accounts they use [23]. Focusing on cognitive scalability is one of the keys to success. Designing the application only by thinking of one IdP should be avoided. Instead, the designer should analyze the system as a whole.

D. The user's consent may lead to maximum disclosure of information

Many identity management schemes describe themselves user-centric, whereby users or customers have to give their consent so that certain transactions may occur [24]. However, surveys show that when warning messages are displayed consecutively to users, they only read them only superficially and move quickly on so as to achieve their goals, thus jeopardizing their privacy and possibly disclosing unnecessary information to third parties [25]–[27].

An identity management system should provide the uses with more control of the data that they are disclosing, without overloading them and even less without doing so in an uncontrolled way.

E. There is a need for mutual authentication (not just user authentication)

Many identity management models focus mainly on authenticating the user [12]. These types of models can be susceptible to phishing attacks [22]. With software support, attackers can easily simulate the interface of a web site, put in sections that require authentication and steal the user’s credentials [28].

In this scenario, what is needed is to authenticate both the RP and the IdP, thereby performing a mutual authentication. This indicates that possibly the conduct of spoofing and phishing attacks can be hampered.

F. RPs want to control the user’s experience

In general, for the purposes of monitoring or tracking of users’ activities RPs tend to want to control the actions that users perform. However, when an identity management system is used, these steps can be lost and there can be a marked difference between the RP layout and that of the IdP.

To make this transition smooth, it is possible to use the IdP before entering the RP layout, thus hiding that there is communication between the RP and the Idp. The Verisign's OpenID Seatbelt use this strategy.

G. *Trust must be earned*

The decision on to whom users may entrust sensitive data is an extremely difficult one. Various models lead to different authentication requirements and assignments of responsibility. Even the IdP of large corporations may contain vulnerabilities or may be poorly implemented. There are differing privacy policies and business models. No organization can guarantee a completely secure system. Systems designers should have their applications evaluated by specialized security companies before launching systems on the market.

IV. IDENTITY MANAGEMENT SYSTEMS

This section gives a general description of the main flow of authenticating the identity management systems examined in the article.

A. *SAML*

SAML is an XML-based framework for representing and exchanging of security information [29]. The use of SAML for an identity management system follows a flow that differs from the current identification process based on login and password. An RP that groups several services wants the user of each service offered to be identified and authorized. Therefore, the RP must have an IdP and from that moment on, all users must register and identify themselves to that IdP.

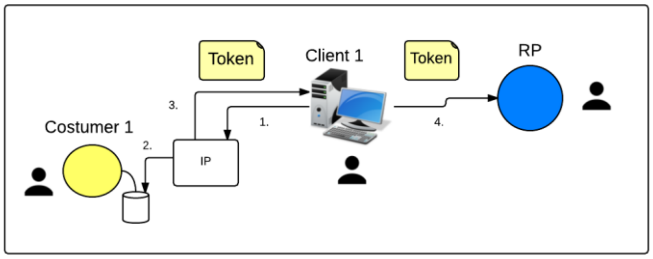

Figure 1. Authentication-flow with SAML.

The IdP will consult a database containing information about the user and will return a SAML token that represents the user identified. This token have the user’s attributes such as his/her age, gender and name [30]. Figure 1 illustrates the authentication flow with SAML.

B. *OpenId*

Also based on the Single Sign On (SSO) is the OpenId identity management model [31]. In this model the RP must rely on information from the OpenId provider (OP), the IdPs of the OpenId. Each identifier is represented by a URL, which is unique to each OP so as to reduce collisions between identical URLs [32]. The base authentication flow in the OpenId has the following steps:

1. The user wants to login with RP and inserts his/her OpenID identifier.
2. Using information contained in the handle the RP discovers the OP of the Original.
3. RP connects to the OP using a secret shared between the two parties.
4. RP redirects the user to the OP, which checks its information and redirects to the RP.
5. The user cross-checks information shared with the OP in step 3 with data that the user obtains after step 4.

Figure 2 illustrates the base authentication flow of OpenID.

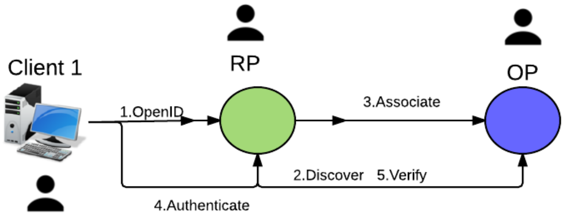

Figure 2. Base authentication flow of OpenId.

C. *Microsoft Card Space*

Microsoft CardSpace (formerly known as InfoCard) was built to give users a conscious digital identity [33]. Since CardSpace is an XML-based framework, CardSpace plug-ins for browsers other than Microsoft Internet Explorer can also be developed, such as the Firefox Plug-in [34]. The framework is based on the identification process users experience in the real world when using physical identification cards CardSpace uses collections of cards, presented in software, which has a similar design to that of a portfolio called identity selector [5]. Each card represents an identity. When an SP searches for an identity the user chooses which card he/she will use from the identity selector [35]. When the SP requires an attribute of the identity, a set of data corresponding to the user's choice is sent to the SP [33].

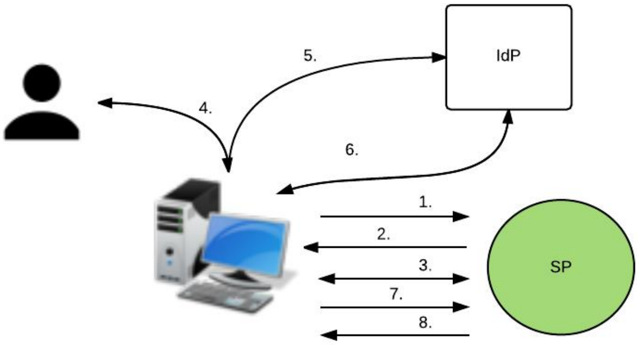

Figure 3. CardSpace Flow.

Figure 3 provides a simplified sketch of the CardSpace framework. In step 1, de the CardSpace enables the user agent or the Service Requestor. In step 2, using a public key the RP identifies itself. After recognizing that the RP is CardSpace- enabled, the CardSpace Enable User Agent (CEUA) retrieves the RP security policy in step 3. In step 4, the CEUA matches the RP’s security policy with the InfoCards that the user has. The user performs an authentication process with the IdP in step 5. If the authentication process succeeds, step 6 takes place, in which the CEUA asks the IdP to provide a security token that holds an assertion of the truth of the claims listed within the selected InfoCard. Finally, the CEUA forwards the security token to the RP in step 7, and, if the RP verifies it successfully, the service will be granted in step 8 [34].

D. ICEMAN

ICEMAN differs from the traditional approach, which has only one IdP for an SP or RP, which is an unreal environment in interclouds. This academic framework proposes a more suitable scheme for interclouds. ICEMAN provides a high interoperability mechanism between any pattern of identity thus facilitating the management of the life flow of the authentication [12]. However, this architecture is still being developed, thus preventing further analysis of the seven failures. Nevertheless, the ICEMAN model for identity management was included in the article as it has a mechanism that can come to add more than one identification and authorization model. Such an approach may ultimately unite existing models, which may be able to mitigate weaknesses and strengthen strong points [16].

V. IDENTIFYING FAULTS IN IDENTITY MANAGEMENT MODELS

We have chosen four Identity Management Systems for our analysis and seven de design flaws which either have dominant positions in Identity Management scenarios or introduced a novel concept which is worth exploring.

1. **Identity management is not the main goal:**

The MS CardSpace model was considered to have the first flaw since it adds a new software to the user's standard way to access information and services. Microsoft has discontinued their CardSpace project. However, we have opted to include it into our analysis because of its fundamentally novel concept of how Identity is presented.

2. **Users follow the path of least resistance:**

It was considered that all models display some difficulty when it comes to installing and configuring them for use. The very concept of the SAMU follows an alternative flow that does not allow the user to follow the path of least resistance.

3. **Cognitive Scalability is as equally important as technical scalability:**

Cognitive scalability in all but the ICEMAN is adequate. The ICEMAN is a framework for better integration of identity management in InterClouds. The scalability of technical cognition scalability does not follow the average of the other models presented.

4. **The user's consent may lead to maximum disclosure of information:**

On the consent of the information to be passed to the user MS CardSpace user is well ahead. However, it is important to emphasize that the type of approach to maintain management of cards can be stressful for users and can generate a new kind of dissatisfaction with the tool. In the case of SAML, in the basic flow of authentication there is nowhere that will say what information can be accessed by the service.

5. **There is a need for mutual authentication (not just user authentication):**

There is the possibility of phishing and spoofing in the identity models. Therefore, it was considered that all configuration management models contain such flaws, which leads the parties involved to add other security mechanisms to mitigate these vulnerabilities [35].

6. **RPs want to control the user’s experience:**

No model analyzed initially presents monitoring of the user’s actions on the site and the transition between the layout of authentication between IdP and the Client is not specified in any model. Thus, it was assumed that all flows present this flaw.

7. **Trust must be earned:**

On models with greater maturity and interaction with the market, it has been identified that users place greater trust in these. It was considered that the ICEMAN has such a flaw. However, according to research carried out on regular Internet users, it was shown that there is still no confidence in service providers that use MS CardSpace [34].

Table 1 illustrates the results of a comparison between flaws and models.

TABLE I. RESULTS OF A COMPARISON BETWEEN MODELS AND FLAWS.

Flaw	MS Card	OpenId	SAML	ICEMAN
1	✓	X	X	partial
2	partial	✓	✓	✓
3	X	X	X	✓
4	partial	✓	✓	✓
5	✓	✓	✓	✓
6	✓	✓	✓	✓
7	✓	X	X	✓

VI. CONCLUSION

Identity management systems are not just systems for authenticating and authorizing identities but are also a set of methods and procedures that can contribute to greater user immersion within a system which uses, for example, the single sign on. However, some identity management systems failed at least partly because they ignored the topics discussed in this paper.

An overview was given of the most popular identity management systems in the market, namely: OpenId, MS CardSpace, SAML and an academic framework called ICEMAN. Seven flaws in the concept and design of identity management in these systems were analyzed. The flaws found in the models were compared in a critical analysis of the study of their concept study and how the user can achieve greater reliance on the technology, and the identity management process.

In this article, problems to do with the lack of control in the process of identifying and authorizing users were listed, in addition to flaws in the concept of identity management systems. The study found that the lack of commitment to dealing with the flaws can result in large projects being poorly received by the current market. Strategies to mitigate and solve the problems discussed in the article were also discussed.

Finally, we intend to examine flaws in identity management in greater depth in future studies, which will focus on aspects of privacy, availability and integrity. We would also like to add new systems to the market and to put forward new academic frameworks.

REFERENCES

[1] A. Acquisti and J. Grossklags, “Privacy and rationality in individual decision making,” IEEE Secur. Priv. Mag., vol. 3, no. 1, pp. 26–33, Jan. 2005.

[2] G. Pallis, “Cloud computing: The new frontier of internet computing,” IEEE Internet Computing, vol. 14, no. 5. pp. 70–73, 2010.

[3] A. Gopalakrishnan, “Cloud Computing Identity Management Online security concerns are on the rise and what cloud needs now,” vol. 7, no. 7, pp. 45–55, 2009.

[4] D. Núñez, I. Agudo, P. Drogkaris, and S. Gritzalis, “Identity Management Challenges for Intercloud,” pp. 198–204.

[5] E. Maler and D. Reed, “The venn of identity: Options and issues in federated identity management,” IEEE Secur. Priv., vol. 6, no. 2, pp. 16–23, 2008.

[6] “Password fatigue - Wikipedia, the free encyclopedia.” [Online]. Available: http://en.wikipedia.org/wiki/Password_fatigue. [Accessed: 12-Oct-2015].

[7] F. , N. , and H. Shannon. "Technology Corner: Brute Force Password Generation--Basic Iterative and Recursive Algorithms." Journal of Digital Forensics, Security and Law 6.3 (2011): 79-86.

[8] S. Gaw and E. W. Felten, “Password management strategies for online accounts,” in Proceedings of the second symposium on Usable privacy and security - SOUPS ’06, 2006, p. 44.

[9] R. Chow, Ori Eisen, et al. "The future of authentication." IEEE Security & Privacy 1 (2012): 22-27.

[10] E. Maler and D. Reed. "The venn of identity: Options and issues in federated identity management." IEEE Security & Privacy 2 (2008): 16-23.

[11] A. Celesti, F. Tusa, M. Villari, and A. Puliafito, “Security and Cloud Computing: InterCloud Identity Management Infrastructure,” 2010 19th IEEE Int. Work. Enabling Technol. Infrastructures Collab. Enterp., pp. 263–265, 2010.

[12] R. Dhamija and L. Dusseault, “The seven flaws of identity management: Usability and security challenges,” IEEE Secur. Priv., vol. 6, no. 2, pp. 24–29, 2008.

[13] “Final: OpenID Authentication 2.0 - Final.” [Online]. Available: http://openid.net/specs/openid-authentication-2_0.html. [Accessed: 12-Oct-2015].

[14] “XACML SAML Profile Version 2.0.” [Online]. Available: http://docs.oasis-open.org/xacml/xacml-saml-profile/v2.0/xacml-saml-profile-v2.0.html. [Accessed: 06-Nov-2015].

[15] K. Cameron and J. Michael. "Design rationale behind the identity metasystem architecture." ISSE/SECURE 2007 Securing Electronic Business Processes. Vieweg, 2007. 117-129.

[16] G Dreo, M Golling, et al. "ICEMAN: An architecture for secure federated inter-cloud identity management." Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on. IEEE, 2013.

[17] G. Alpár and J. H. Johanneke, “The Identity Crisis Security , Privacy and Usability Issues in Identity Management,” pp. 1–15, 2011.

[18] D. W. Chadwick, “Federated Identity Management,” vol. 5705, pp. 96–120, 2009.

[19] S. Dongwan , A. Gail-Joon and S. Prasad, “Ensuring information assurance in federated identity management,” in IEEE International Conference on Performance, Computing, and Communications, 2004, 2004, pp. 821–826.

[20] A. Acquisti and J. Grossklags, “Privacy and rationality in individual decision making,” IEEE

Secur. Priv. Mag., vol. 3, no. 1, pp. 26–33, Jan. 2005.

[21] A. Adams and M. A. Sasse, “Users are not the enemy,” Commun. ACM, vol. 42, no. 12, pp. 40–46, Dec. 1999.

[22] U. C. Berkeley, “Why Phishing Works,” 2006.

[23] B. M. Gross and E. F. Churchill, “Addressing Constraints: Multiple Usernames, Task Spillage and Notions of Identity,” in CHI ’07 extended abstracts on Human factors in computing systems, 2007, pp. 2393–2398.

[24] A. Cavoukian, “7 Laws of Identity - The Case for Privacy-Embedded Laws of Identity in the Digital Age,” Technology, no. 30 January 2008, p. 24, 2006.

[25] N. Good, R. Dhamija, J. Grossklags, D. Thaw, S. Aronowitz, D. Mulligan, J. Konstan, and S. Hall, “Stopping Spyware at the Gate : A User Study of Privacy , Notice and Spyware Definition of Spyware,” pp. 1–10.

[26] J. Grossklags and N. S. Good, “Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers,” in Financial Cryptography and Data Security, 2008, pp. 341–355.

[27] D. A. Norman, “Design rules based on analyses of human error,” Commun. ACM, vol. 26, no. 4, pp. 254–258, Apr. 1983.

[28] S. E. Schechter, R. Dhamija, A. Ozment, and I. Fischer, “The Emperor’s New Security Indicators,” 2007 IEEE Symp. Secur. Priv. (SP ’07), 2007.

[29] A. Armando, R. Carbone, L. Compagna, J. Cuellar, and L. Tobarra, “Formal Analysis of SAML 2.0 Web Browser Single Sign-on: Breaking the SAML-based Single Sign-on for Google Apps,” Proc. 6th ACM Work. Form. Methods Secur. Eng., pp. 1–10, 2008.

[30] P. Arias Cabarcos, F. Almenarez Mendoza, A. Marin-Lopez, and D. Diaz-Sanchez, “Enabling SAML for Dynamic Identity Federation Management,” Wirel. Mob. Networking, Proc., vol. 308, pp. 173–184, 2009.

[31] “Pros and Cons of OpenID - O’Reilly Radar.” [Online]. Available: http://radar.oreilly.com/2007/02/pros-and-cons-of-openid.html. [Accessed: 08-Nov-2014].

[32] “What is OpenID?.” [Online]. Availablehttps://openid.net/get-an-openid/what-is-openid. [Accessed: 05-Nov-2015].

[33] S. Gajek, J. Schwenk, M. Steiner, and C. Xuan, “Risks of the cardspace protocol,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 2009, vol. 5735 LNCS, pp. 278–293.

[34] W. A. Alrodhan and C. J. Mitchell, “Addressing privacy issues in CardSpace,” in Third International Symposium on Information Assurance and Security, 2007, pp. 285–291.

[35] V. Bertocci et al.,Understanding Windows CardSpace An Introduction to the Concepts and Challenges of Digital Identities Technical Reviewers.