2012 IEEE 4th International Conference on Cloud Computing Technology and Science

A Survey on Security Issues of Federated Identity in the Cloud Computing

Eghbal Ghazizadeh
Advanced Informatics School
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
gzeghbal2@live.utm.my

Jamalul-lail Ab Manan
Strategic Advanced Research Cluster, MIMOS Berhad,
Technology Park Malaysia,
57000, Kuala Lumpur, Malaysia
Jamalul.lail@mimos.my

Mazdak Zamani
Advanced Informatics School
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
mazdak@utm.my

Abolghasem Pashang
Advanced Informatics School
Universiti Teknologi Malaysia
54100 Kuala Lumpur, Malaysia
pabolghasem2@live.utm.my

***Abstract*— Cloud computing is a new generation of the technology that has been designed to cater for commercial necessities and to run suitable applications or solve IT management issues. While cost and ease of use are two top benefits of cloud, trust and security are the two top concerns of cloud computing users. Federated identity as a useful feature for user management and Single Sign-on (SSO) has also become an important part of federated identity environment. Misuse of the identity, identity theft, and platform trustworthiness are some of the problems in the federated identity environment. OAuth, OpenID, SAML are three main concept in cloud authentication and federated environment. This paper overviews the security issues of federated identity in the cloud authentication and highlights the proposed models to solve identity theft in the federated environment.**

Keywords-Cloud computing; SSO; OpenID; Federated Identity; Identity Theft; Trusted computing

I. INTRODUCTION

The definition of cloud computing has been defined by Amazon's EC2 in 2006 in territory of information technology. Cloud computing has been designed and constructed because of commercial necessities and it has turned into a large scale future application. According to NIST definition in [1], "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources." Resource pooling, on-demand self-service, rapid elasticity, measured service and broad network access are the five vital features of cloud computing. Other definitions of cloud that has been used by the community are: Executing, Supplying Material, Organizing, and Infrastructure that they should be rapidly provisioned and unrestricted, automatically accessed or service provider (SP) interaction [1].

While cost and ease of use are two top benefits of cloud, trust and security are the two main concerns of cloud computing users. Cloud computing has claimed insurance for sensitive data such as those from accounting, government, and healthcare and bring opportunities for end users. However, new technologies emerged, such as Virtualization, multi tenancy, elasticity, and data owner, which traditional security techniques cannot solve in cloud computing.

We believe that Trusted Computing (TC) can be used to strengthen existing security solutions by creating the right trust relationship amongst participating federated entities, components of the Infrastructure and systems within the cloud. Today's internet user has about thirteen accounts that require user names and passwords and enters about eight passwords per day. It has become a big hassle for internet users, and they face the issue of managing huge number of accounts and passwords, which leads to users using password management strategies that reduce security of their private information. Besides, site centric web has difficulties in managing online user account and personal content sharing [2-4].

SSO today has a critical role in cloud security and it becomes essential to determine how secure the deployed SSO mechanisms truly are. The integration of Web SSO and Cloud Security may be a new challenge since no previous work has especially been done on commercially-deployed systems, and this becomes a key to understanding to what extent these real systems are subject to security breaches [5]. In addition, Wang et al showed potential weaknesses that do not show on the protocol level, that could be brought in by what the system essentially agree each SSO party can do [6].

Federated environment applications system can achieve many advantages from Trusted Computing Group (TCG) technologies. The core objective is to generate mutual trust relationships between server, networking, client, and communications platforms. In summary, we intend to show how trusted computing technologies can essentially reduce phishing attack on user assets within the cloud.

The rest of the paper is organized as follows. In Section II related work which is divided to SSO, OpenID, OAuth, and federated identity and trust is defined. Section III tries to state the problems. Finally in the section IV reviews the content of this paper and presents the conclusions.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

II. RELATED WORK

Nowadays, federated identity security has become an interesting research area and it has attracted huge investment in industries such as Tivoli in IBM. Huang and Wang have addressed security concern in federated environment proposed an identity federation broker that introduced a trust third party between SP and the IDP [7]. In addition, Roddriguez described a proposed FIA solution and analysed the main characteristics, remaining issues and challenges [8]. Furthermore, Cloud Security Alliance discussed and addressed a wide area of security via Security Guidance for critical areas of focus in cloud computing [9].

A. SSO

Somorovsky et al investigated fourteen models of SAML standard and they founded many security problems that related to Extensible Mark-up Language (XML) signature wrapping. WS-Security and REST based SSO use SAML assertion for making security statement between subjects. Therefore, they developed an automated penetration testing tool for XML signature wrapping. Also, for analyse and test attack on relying party, they proposed the RST framework which is based on information relying party's components [10].

Wang et al reported their extensive security study on commercial web SSO systems. Their study showed that there are some critical logic flaws in SSO system, which can be discovered from browser relayed messages, and can potentially be exploited even without access to the source code or other insider knowledge of these systems. They studied and analysed practical steps that attackers might take on commercial systems and how they are able to detect them.

Vulnerabilities in detection flaw can be exploited by the attacker to sign in as the victim. Furthermore, they exposed new failures in web SSO systems and highlighted the dire need to enhance the security of SSO community [6].

Wang performed security analysis of three commonly available SSO, which include Microsoft Passport, OpenID 2.0 and SAML 2.0. He highlighted some vulnerabilities and security issues for each system with their applications. He further analysed Privacy Aware Identity Management and Authentication for the Web (SAW) as two alternative solutions for SSOs [11]. Rodriguez et al argued in their study that there are some difficulties in digital identity. They focused on Federated Identity Architecture (FIA) and analysed some of the problem related to it. In addition, they explored industrial FIA solutions and investigated security and privacy issues and others challenges [8]. Besides, Yan et al proposed a cryptography based federated identity with some desirable features, to adapt with cloud computing. They harmonized hierarchical identity-based cryptography with federated identity management in the cloud environment [12].

B. OpenID

You and Jun proposed Internet Personal Identification Number or I-PIN technique to strengthen user authentication with the cloud OpenID environment to curb phishing. They evaluated and compared their method with the existing OpenID method, and recommended some ways to secure OpenID environment [13].

Figure 1 illustrates their proposed model in which a user has to choose only 1 company out of 3 companies, which delivers OpenID in order to obtain OpenID service. A user receives I-PIN information from main Confirmation Authority via OpenID Provider. In addition, based on Figure 2, they evaluated and compared their proposed solution with an existing OpenID, and confirmed that authentication was secure and safe against attack and private information exposition and hence against phishing attacks.

C. OAuth

Sun claimed that by using formal methods to examine security and privacy of OAuth protocol, he did not find any new threat. He investigated possible security threats by examining executions of OAuth 2.0 SSO systems used by three main IDPs such as Facebook, Microsoft, and Google, to appreciate its implementation in real-world settings. He found numerous methodical weaknesses that permit an attacker to have unauthorized access to user's profile, which opens up possibility of impersonating the victim on the

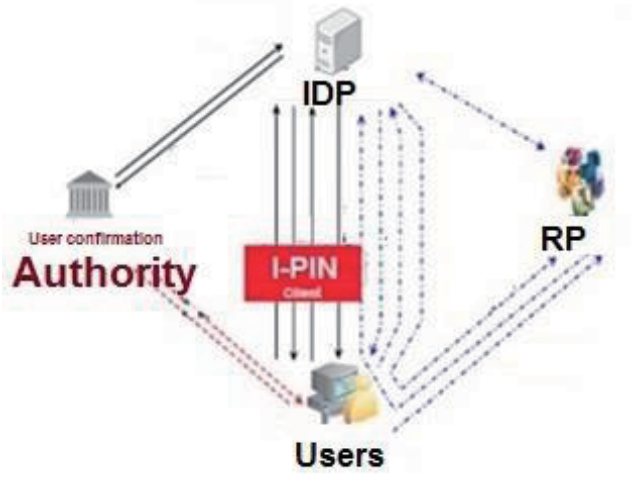

Figure 1: You and Jun proposed model [13]

	OpenID	I-pin adopting OpenID
membership registration Information	ID, Password, E-mail	OpenID Information and I-PIN Information
Name and Authentication	impossibility	possibility
Limitless ID Creation Protection	impossibility	possibility
Resident number expose	absence	absence
Trust	Low	High

Figure 2: You and Jun comparison table [13]

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

supporting website. He recommended useful countermeasures to mitigate the discovered threats including his proposal for SSO environment identity provider (IDP or IP) to increase security for relying party, and to strengthen the security of each authorization process. He proposed a method for relying parties to use server-flow every time possible, and protect the authenticity and confidentiality of SSO credentials. Furthermore, vital part of the security of OAuth SSO systems is in JavaScript SDKs [14].

Kim illustrated the step by step OAuth authentication as shown in Figure 3. He proposed the use of card space (which is a self-issued card) for user to log in to IDP. Since self-issued cards are used in place of username and password, it will prevent identity theft. The system employs public key cryptography and generates dissimilar keys for each site the user visits. For example, even if an Evil Scooper is used, it will not expose anything at all. This solution is better and a lot stronger than traditional solutions [15].

D. Federated Identity and Trust

Madsen et al investigated password attack, phishing, and farming in federated identity and argued that this risk of identity theft increases through federated identity. Furthermore, they proposed an identity management at critical place in the federated model [16].

Leandro et al proposed a model based on Shibboleth for cloud-based environments with multi-tenancy authorization system. It is essential to deliver access control based on concerns about the privacy of data. They provided identity management with authorization and authentication mechanisms for access control in cloud computing to emphasize on self-governing and control of trusted third-parties, according to the digital identity federation. They believe that user's privacy policies should be used to authenticate and access cloud services [17].

Khattak et al studied SSO authentication and exposed some of its current weaknesses. They found that misuse of user identity information could happen via SSO services in IDP and SP, which could lead to identity theft, i.e. the main concern in FIM systems. Besides, they explored trusted computing technology, which covers TPM security such as Integrity Measurement and Key certification. In addition, they demonstrated a theoretical threat model for inter-domain web SSO in FIM system. Lastly, they elaborated how trusted computing technology helps to effectively resolve identity theft, misused of identity information, and trust relationship concerns in FIM system [18].

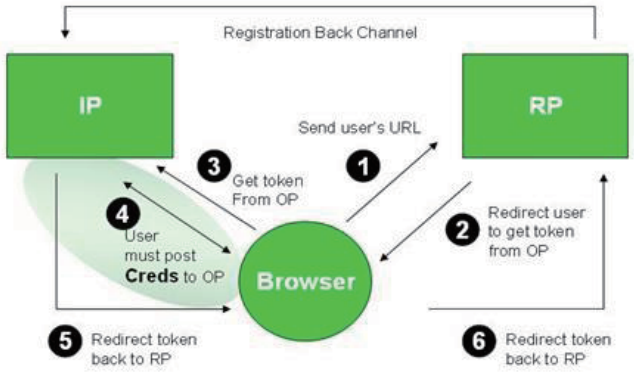

Figure 3: Step by step OAuth message exchange [15]

Ahmad et al determined that there are some types of attack in FIM such as Man in the Middle (MITM) in open network, which is basically theft on ID to access confidential information, and misuse of the IDP and SP with user identity information causing the risk of IDP becoming malicious and risking the use of user identity information in SPs to share it with other SPs or third parties in FIM. They discovered that there is no platform trust between the communicating platforms. Lastly, they proposed a user requirement model based on trusted hardware functionalities. Also they presented scenarios related to identity theft, illegal information tracking and gathering [19].

III. PROBLEM STATEMENT

Madsen et al defined some problems of federated identity and illustrated that Federated Identity Management (FIM) which is established on standards permits and simplifies the processes used by federated organizations in term of sharing user identity attributes, simplifying authentication and accessing permission using service access requirements. SSO is defined as "using its facility, user authenticates only once to home IDP and log-in to access successive services provided by SPs within the federation". There are some active problems and concerns in a federated identity environment such as misuse of user identity information through SSO capability in SPs and IDPs, user's identity theft, and trustworthiness of the user. These security problems should be taken into account in the real implementation [16].

Issues of identity management involve many dimensions; among others they include users having to share their identities with numerous service providers, leading to personal information of the user being compromised during implementing a federated identity. Rodriguez et al presented Federated Identity Architecture (FIA) as a way for solving vulnerabilities. There are three architectures for implementing security issue in FIA including Liberty Alliance, Shibboleth, and WS- Federation [8].

Archer et al argued that one of the most common attacks is identity theft mainly because it is very difficult to identify until the harm is done. They believed that the identity attack mainly occurred in the insecure channel. Besides identity attack, legal compliance and privacy guaranty are other security problems in federated identity. The current FIA does not have a good way protect user's information. Platform for Privacy Performances Project or P3P (which was established by W3C) has been released as a standard and a project for improving FIA, by integrating P3P into the FIA [9].

There are five security issues related to federated identity and identity attributes concerning relationships between users and vendors.

- Connection to Human Resources (HR) is difficult because HR is the only master source for staff identities.
- No authoritative information sources to know identities in partner organizations.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE

- Capability to manage federated identities does not exist in most organizations.
- Self-asserted identity for public has been provided by identity service and it does not cover other entity types.
- Most organizations do not have the ability to communicate directly with identities in another organization.

These issues and the lack of provisioning standards emphasize the need for good planning and a comprehensive approach to handle how identity attributes, accounts, and lifecycle management of all entity-types will operate in the cloud eco-system [9].

Suriadi et al identified that one of the main problems with the model is user privacy in an SSO environment, relying parties (RP) or service providers (SP). It can also be gathering information about a user of the information they get from the IDPs. They also analysed sharing of user's information by malicious IDPs and SPs which can disclose a complete user's identity and activities[20]. In addition, Zarandioon et al shows that this issue has caused web users to be cautious of SSO implementations and is one of the main causes for the lack of widespread adoption [21].

Wang discovered another problem of federated identity that is switching authentication mechanisms to an SSO solution. It means further education of the users is required and possible loss of the user base if the transition is not smoothly executed. Also worsening the situation is the lack of demand from users for a Web SSO solution. Studies have shown users are already satisfied by their own password managers [11].

IV. CONCLUTIONS

We have presented the concept of using trusted computing, federated identity management and OpenID Web SSO to solve identity theft in the cloud. We presented an overview of federated identity management system, cloud computing, single sign on, as well as SSO protocol such as OpenID and OAuth. Furthermore, we have tried to state the SSO security problems. While this paper presented a number of attacks against cloud authentication but the main aim is to highlight the identity theft concern because some of the issues are partially solved but identity theft requires further thought.

REFERENCES

[1] L. Badger, T. Grance, R. Patt-Corner, and J. Voas, "Draft cloud computing synopsis and recommendations," *NIST Special Publication,* vol. 800, p. 146, 2011.

[2] S. T. Sun, E. Pospisil, I. Muslukhov, N. Dindar, K. Hawkey, and K. Beznosov, "What makes users refuse web single sign-on?: an empirical investigation of OpenID," 2011, p. 4.

[3] M. Gharooni, M. Zamani, M. Mansourizadeh, and S. Abdullah, "A confidential RFID model to prevent unauthorized access," 2011, pp. 1-5.

[4] M. ALIZADEH, M. SALLEH, M. ZAMANI, J. SHAYAN, and S. KARAMIZADEH, "Security and Performance Evaluation of Lightweight Cryptographic Algorithms in RFID."

[5] A. C. Armando, R. Compagna, L. Cuellar, J. Tobarra, L., "Formal analysis of SAML 2.0 web browser single sign-on: breaking the SAML-based single sign-on for google apps," 2008, pp. 1-10.

[6] R. Wang, S. Chen, and X. F. Wang, "Signing Me onto Your Accounts through Facebook and Google: a Traffic-Guided Security Study of Commercially Deployed Single-Sign-On Web Services," 2012.

[7] H. Y. Huang, B. Wang, X. X. Liu, and J. M. Xu, "Identity federation broker for service cloud," in *2010 International Conference on Service Sciences, ICSS 2010, May 12, 2010 - May 14, 2010*, Hangzhou, China, 2010, pp. 115-120.

[8] U. F. Rodriguez, M. Laurent-Maknavicius, and J. Incera-Dieguez, "Federated identity architectures," 2006.

[9] D. C. J. Archer, Nils Puhlmann, Alan Boehme, Paul Kurtz, and J. Reavis, "Security guidance for critical areas of focus in cloud computing v3.0," *Cloud Security Alliance,* 2011.

[10] J. Somorovsky, A. Mayer, J. Schwenk, M. Kampmann, and M. Jensen, "On breaking saml: Be whoever you want to be," 2012.

[11] Wang, "An Analysis of Web Single Sign-On," 2011.

[12] L. Yan, C. Rong, and G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," in *1st International Conference on Cloud Computing, CloudCom 2009, December 1, 2009 - December 4, 2009*, Beijing, China, 2009, pp. 167-177.

[13] J. H. You and M. S. Jun, "A Mechanism to Prevent RP Phishing in OpenID System," 2010, pp. 876-880.

[14] S. T. Sun, "Simple But Not Secure: An Empirical Security Analysis of OAuth 2.0-Based Single Sign-On Systems," 2012.

[15] C. Kim. (2007). *Integrating OpenID and Infocard* Available: http://www.identityblog.com/?p=659

[16] P. Madsen, Y. Koga, and K. Takahashi, "Federated identity management for protecting users from ID theft," 2005, pp. 77-83.

[17] M. A. P. Leandro, T. J. Nascimento, D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "Multi-Tenancy Authorization System with Federated Identity for Cloud-Based Environments Using Shibboleth," 2012, pp. 88-93.

[18] Z. Khattak, S. Sulaiman, and J. Manan, "A study on threat model for federated identities in federated identity management system," 2010, pp. 618-623.

[19] Z. Ahmad, J. L. Ab Manan, and S. Sulaiman, "User Requirement Model for Federated Identities Threats," 2010.

[20] S. Suriadi, E. Foo, and A. Jøsang, "A user-centric federated single sign-on system," *Journal of Network and Computer Applications,* vol. 32, pp. 388-401, 2009.

[21] S. Zarandioon, D. Yao, and V. Ganapathy, "Privacy-aware identity management for client-side mashup applications," 2009, pp. 21-30.

978-1-4673-4510-1/12/$31.00 ©2012 IEEE