EVALUATING SINGLE SIGN ON SECURITY FAILURE IN CLOUD SERVICES

Brian Cusack; Eghbal Ghazizadeh
Auckland University of Technology
{brian.cusack; eghbal.zadeh} aut.ac.nz

ABSTRACT

The business use of cloud computing services is motivated by the ease of use and the potential financial cost reductions. Service failure may occur when the service provider does not protect information or when the use of the services becomes overly complex and difficult. The benefits also bring optimisation challenges for the information owners who must assess the service security risk and the degree to which new human behaviours are required. In this research we look at the risk of identity theft when ease of service access is provided through a Single Sign On (SSO) authorisation and ask: What are the optimal behavioural expectations for a Cloud service information owner? Federated identity management is a well-developed design literature for solutions to optimising human behaviours in relation to the new technologies. We briefly review the literature and then propose a working solution that optimises the trade-off between disclosure risk, human user risk and service security. Both breech and non-use of a system are failures.

KEYWORDS

Cloud, Security, Behaviour, SSO, Failure

INTRODUCTION

The problem of authentication of users in the cloud environment has arisen as a usability issue where users object to repeating the logon behaviour multiple times to multiple identities for many different services and service providers (Shackel, 1990; Wang and Shao, 2011). Similarly users may be using multiple devices to access services simultaneously and independently. The problem is accentuated in the Cloud when the layers of complexity are reduced and the risk of unauthorised access to services increased. One of the broad research areas providing solutions to the problem has been that of federated identity management. These solutions include SSO, OpenID, One Time Passwords (OTP) and other innovative designs that facilitate the ease of human behaviour while hardening the technology protection (Gupta and Zhdanov, 2012; Hocking, et al., 2011). Each solution has usability strengths and weaknesses but also security risk and effectiveness trade-offs. In this paper our interest is in the management of risk around an identity. A suitable acceptance by all parties is required that sufficient precautions are taken to prevent theft by an unauthorised party while allowing a seamless user experience for legitimate beneficial parties (Hess, et al.,2014).

Federated authentication in the cloud environment relies on the advancement and development of authentication mechanisms that can securely and effectively distribute the identity information across platforms and devices (Yan, et al, 2009). The challenges to be overcome relate to the proprietary nature of many services and the lack of general standardisation for interoperability (Leandro, et al., 2012). To some extent the problem is addressed in independent authorisation agencies to whom each service provider referrers to authenticate users. The scope of authorisation may be further controlled by the use of strong and weak determinations. For example if three forms of identity including a biometric are provided then a strong assurance can be issued whereas if a singular password or PIN is provided then a weak assurance is issued (Madsen, et al., 2005). It is up to the authentication service user to determine the use of the authorisation for matters of access control and so on. In a cloud environment one point of entry authentication is desirable by the user but the chance of breach from a single set of credentials is higher than many (assuming differentiation). The problem is accentuated if a user identity is compromised or if a service is left open for long periods of time (Huang, et al., 2011). In both instances the user expectation presents technical and design challenges for information security. If the risk management requires a user to provide identification every 2-3 minutes to keep the service active; or if for each service or device activated, a fresh authentication of identification is required, then the user must adopt new behaviours. The user may resist the new behaviours and forgo the service (Rivard and Lapointe, 2012). Both breach and non-use of a system are failures. Hence the optimisation of human behaviour against a robust security design requires innovation and scoping for cloud environments (Sun, et al., 2011).

This paper is structured to introduce the problem area and then to elaborate potential solutions. The following section briefly introduces federation theory and the SSO opportunity. The issues of risk and behavioural

modification are discussed in terms of potential system failure. It is assumed humans prefer SSO as a behavioural solution but the challenge is to match this behaviour with a secure architecture. The literature analysis shows that there is no model which can provide system integrity verification in the cloud SSO framework. We propose a mutual attestation framework based on a trusted platform model (TPM) that provides a platform verification check within the SSO protocol in order to implement trustworthiness among the cloud authentication workflow. The proposed model guarantees a secure mutual attestation with encrypted messages, by using TPM keys. A solution is proposed and then tested theoretically (from the literature) for attack resistance. The paper concludes with a discussion of trust as a utility facilitator in socio-technical security systems.

SINGLE SIGN ON RISKS

Federated authorisation relies on the existence of mechanisms beyond an organisation or domain to co-operate for the authentication of users (Yan, et al., 2009). In cloud environments the ideal is to have transparent and global mechanisms that permit general authorisation regardless of service, device or location. The current challenge is the level of co-operation that may be gained for mechanisms to communicate with different systems and yet to retain the integrity of the authorisation process (Leandro, et al., 2012). A general solution is to take the responsibility for authentication from any system and to refer it to an external authority. Such an architecture introduces the concept of "trust" and a "trusted" third party (Abbadi and Martin, 2011; Thibeau and Drummond, 2009). The independence of the third party permits one enrolment and removes duplication. A user may then have a single profile within the Managed Authentication Service Provider (MASP) where they are able to manage and monitor their profile. Any MASP enabled device or service can then send one request and gain the current confidence level for the user. The MASP too can gain information on the user from other MASPs and both public and private information sources. In this manner authentication can be provided for multiple services, devices and information requirements for the user without duplicated costs for messaging, data processing, and data storage. These benefits are passed to the user by way of minimal behavioural modifications for Cloud services (Faulkner and Runde, 2013).The ideal behaviour for a user is to perform a single sign on (SSO) for all services.

SSO opportunity has implications for system architecture and the management of risk levels associated with system failure. Failure concerns utility level and disclosure performance. If the system falls below a perceived utility level because of delivery or complexity then the user reacts negatively. Similarly if the information is disclosed or damaged beyond a control level then negative consequences occur. The level of risk in these instances impacts the objectives of the system and requires mitigation (Rivard and Lapointe, 2012; Sun, 2012). A SSO opens the system to a number of attacks (see Figure 3 for some) that may eventuate in the user identification being compromised. Identity theft is described as being "exploitation of another user's individual information to perform fraud" (Madsen, et al., 2005). Federated Identity Management (FIM) simplifies authorisation by removing repetition and layers of complexity that would usually be barriers to an adversary attack and hence a secure system requires barriers to be put back in, but barriers that do not detract from the user experience and expectation (Sloan, 2009). An attacker who cracks a SSO enabled service is likely to gain authorisation to much more than in a domain and device specific authorisation (Sun, et al., 2010).

The SSO FIM requirements also open the user identity to intentional and unintentional misuse. In the first instance the federated arrangements in a cloud environment pass the user identity and information to various parties that are often out of the user control and knowledge. The information exposure can include cross-jurisdictional matters, misaligned SLA arrangements, and different information security standards (Yan, 2009). For example, carefully embedded identification marking and cryptographic measures may not pass from the user to each service supplier without spoliation. Also different service suppliers may have different standards for the reuse of identification information, the supply of service and privacy rules. The result can be the user may receive unsolicited advertising, representation in unexpected forums and exposure to unintended information sharing between different FIS and MASPs. Each risk has to be weighed against the expectation for benefit and what a user is prepared to agree is a reasonable cost for the experience (Hess, et al., 2014; Sun, 2012). The five properties for useability of a system frame a user expectation for experience (ease of learning, efficiency, ease of recollection, error recovery, and user satisfaction). The degree to which a SSO failure impacts on the user experience may be observed in behavioural changes. Unfortunately the misuse of an Identity is usually only detected after the security breech and in association with an unplanned event which may be frightening, threatening and financially costly. Effective error recovery for example may regain a user trust in a Cloud service and the emotional and financial frights be put in perspective. However, successive negative feedback across the five usability properties leads to risk aversion and user resistance to the Cloud services (Faulkner and Runde, 2013; Rivard and Lapointe, 2012; Shackel, 1990).

A PROPOSED SOLUTION

The review of current literature suggests that the positioning of an external authorisation authority is the best solution for federation architecture issues. The exteriority creates an independent entity that is global to user

devices and systems but not necessarily unique in existence. The literature also suggests that OpenID currently has the greatest uptake by Cloud service providers and hence has a protocol that satisfies more of the current users' requirements than other competitors. Our proposal is to take the best of this learning on systems architecture and FIS protocols and to add layers of complexity that replace those removed by SSO adoption. The new layers are to assure user experience and to strengthen the risk treatment for identity theft. Principally the adoption of Trusted Computing concepts and system in the form of trusted platform models (TPM) strengthens the lower layers out of sight of a user. The proposal is presented as a conceptual relationship model (Figure 1) for ideal relationships. A work flow model (Figure 2) that itemises the steps in a SSO process, and an architectural model that captures the relationships and information flows. Finally the proposed solution is subjected to eleven theoretical attacks identified from the literature and assessed against the other alternative SSO opportunities (Table 1).

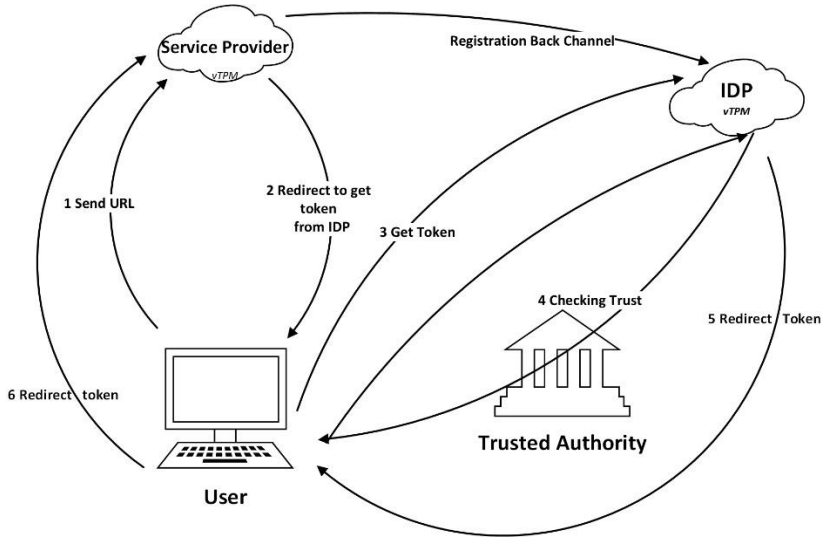

Figure 1: The Conceptual Relationship Model

Figure 1 process steps are summarised as follows:
Step1: OpenID allows us to sign in to web sites using a single identifier in the form of a URL.
Step2: the SP locates the User's location and creates an authentication token. SP asks the user to prove that he/she is who he/she is.
Step3: the browser proceeds with token exchange based on SAML protocol.
Step4: Step 4 is the most critical part of our proposed OpenID trust-based Federated Identity Architecture. Using Trusted Authority (TA) as the core, user's browser, Relying Party (RP) or Service Provider (SP), and IDP must prove their identity based on mutual attestation process using their TPM-enabled platforms and verified by the TA.
Step5: If and only if the mutual attestation process has been successful, i.e. the user and IDP have confidence each other, then the IDP will deliver SAML token to the user's browser.
Step6: IDP sends a encrypt token by the user's public key that shows IDP is legitimated and verified by a trusted authority.

The conceptual relationship model captures the relationships described in the literature reviewed and some assumptions are made. For simplicity the three entities of interest are the user, the service provider (SP) and the OpenID provider (IDP). In addition and external trusted party is required for security maintenance of all transactions. The system is built on trusted platform modules (TPM) and virtual trusted platform models (VTPM) that assure secure communications. These requirements are prerequisites for registration with OpenID services. We assume the communications are taking place in a public cloud but the same scenario can be played in a private cloud by the user obtaining a new OpenID registration. Trusted communication between two cloud entities can be established through attestation. Attestation is a process in which a platform that requires to be verified (attester) will have to provide an integrity report to the remote verifier. The Integrity report inside the attester platform can be created by using a trusted boot process. The trusted boot in a TPM-based platform operates like a chain whereby a first component needs to measure the second component and the trusted second component then needs to measure the third component and then step by step through until the last component. This process is called chain of trust for measurement and its goal is to gain trust from the first entity until the last entity. The integrity measurement value inside a TPM in the cloud service provider is the integrity report to prove it is trustable to the Trust Authority (verifier).

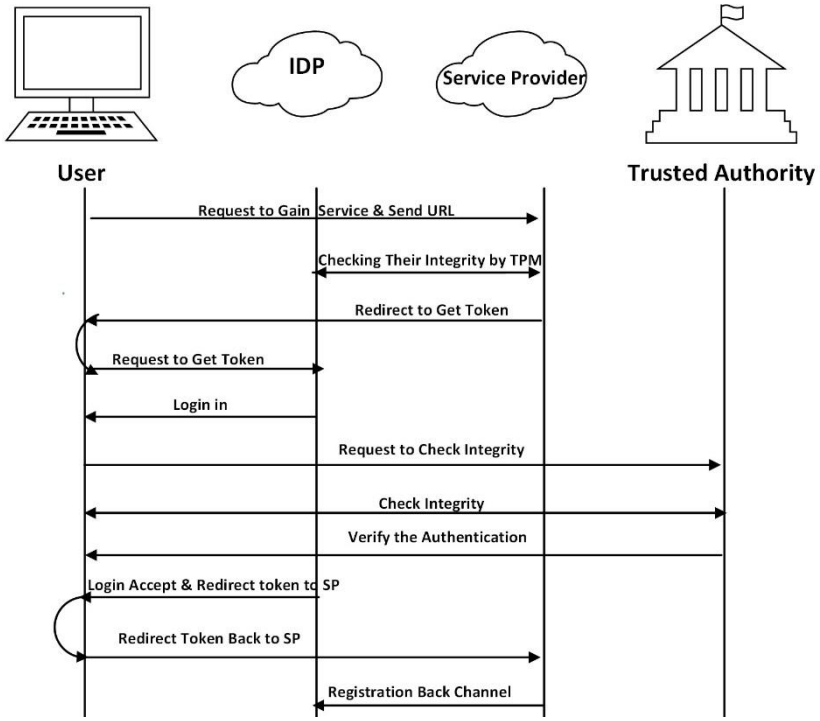

Figure 2: Model Work Flow Architecture

In Figure 2 the work flow steps of the conceptual model are illustrated to itemise the interactions. It assumes the user has already performed the OpenID registration process and is simply requesting a cloud service. This process can be intentional or automated but goes through the same audit steps to assure validity. In Figure 2 these communications are described with one and two way message flow arrows. In Table 1 an analysis of the proposed model is made by subjecting it to theoretical attacks. These attacks have been extracted from the literature cited for specific threats in the Cloud and in the situation where a user is requiring a single logon. Four attacks are chosen to be indicative of vulnerabilities and sufficient to show the proposed model has performance advantages over others. In designing our model were aware of these threats and consequently deliberately designed to secure the system. The adoptions made in Figures 1 and 2 provide a secure environment while considering the user requirements for seamless experience. The testing can be pushed further for in practice testing but we stayed within our research scope of theory.

Table 1: Proposed Solution Threat Analysis

Title	Insider Attack	MITM	Phishing Attack	DNS Poisoning
Ding & Wei, 2010			*	*
You & Jun, 2010			*	*
Feng et al., 2011		*	*	
Thibeau & Reed, 2009			*	
Urien, 2010		*	*	
Nor & Jalil, 2012		*		
Latze, 2007		*	*	
Huang et al., 2011	*		*	
Leicher et al., 2012			*	
Leandro et al., 2012	*			
Hodges et al., 2008			*	*
Proposed Model	*	*	*	*

*Indicates the model is resistant to this attack

TRUSTING BEHAVIOUR

Trust is a two way event that the user and the system formulate through interaction. The system retains a defensive posture based on multiple feedback loops, learning and risk based decision criteria. The system will always act in the best interest of the system by optimising beneficial activities and minimising potential failures. The user retains a recollection of the interaction experience, the process steps and expectation satisfaction. The user will develop negative attitudes when their personal satisfaction is affected by adverse or unexpected consequences. For example if the utility is perceived too low, privacy is breeched, and so on. Unfortunately the compromise of an identity is not usually known until the negative consequences materialise. The user too will often act against the best interest of the system by interacting to their own satisfaction and level of operational ability. The beneficial relationship between the user and the system is optimised in learned behaviours. However there is a strong tension between learning with positive consequences and learning with negative consequences when the perceived risk is heightened. In the use of Cloud services personal, valuable and private information is transacted through multiple agencies. The user tolerance for negative feedback in learning is lower in such a context and the tolerance for puzzling interfaces lower. In simple terms the user is quite nervous about sharing their information and often worried by the thought of potential system failures. An information owner usually has higher expectations for security than a custodian or a general user of the information and hence the tension between the service and the user expectation is heightened.

In the proposed model we have integrated a trusted computing system with the Cloud services of agency and authorisation in order to address the technical concerns of communication. The user confidence has been discussed under the five properties of the usability criteria. Here the expectation is set that a user requires all five properties to deliver in their favour with zero negative feedback. In practice however two other factors come into play that we have structured to mediate positive and negative feedback and importantly, to place the user in a negotiated position that balances the system expectation with the user expectations. In such a context the user can be expected to modify their behaviour in keeping with managed and minimalistic system demands. The user may have a SSO seamless experience for many Cloud services but they are expected to enrol in OpenID, comply with a TPM operating and computing system and occasionally reregister as different Cloud architectures are required or a non-affiliated service is requested. This is part of the trust contract a user is to experience and to accept for service in our proposal. Consequently in our models we have built in technical trust so as to minimise negative feedback and management services to enhance the user confidence levels and ease of behavioural modification.

CONCLUSION

In this research we set out to answer the question: What are the optimal behavioural expectations for a Cloud service information owner? We assumed that there are many users but some users hold a rightful ownership responsibility for the information transacted in a Cloud. We have also assumed that human behaviour fits the five properties in the cited usability literature and hence expectations can be established in relation to the criteria. Other parties involved with the Cloud transaction of information are custodians and as such they hold other expectations. Together the parties must trust one another within the designated roles of system and perform as expected. All parties must expect to negotiate and give up some of their maximum requirements to gain a satisfying user experience. Behaviour and protection from failure is optimised in such a negotiated situation.

REFERENCES

Abbasi, A., Albracht, C., Vance, A. and Hancon, J. 2012. "MetaFraud: A Meta Learning Framework for of Financial Fraud," *MIS Quarterly* (36:4), 1293-A12.

Abbadi, I. and Martin, A. 2011. "Trust in the Cloud," *Information Security Technical Report* (16:3-4), pp 108-114.

Clarke, N. and Furnell, S. 2007. "Advanced user authentication for mobile devices," Computers & Security (26:2), 109-119.

Ding, X. and Wei, J. 2010. "A scheme for confidentiality protection of OpenID authentication mechanism," in *Proceedings of the International Conference on Computational Intelligence and Security* (CIS'10), pp.310–314, Nanning, China.

Faulkner, P. and Runde, J. 2012. "Technical Objects, Social Positions, and the Transformation Model of Social Activity," *MIS Quarterly* (37:3), 803-818.

Feng, Q., Tseng, K., Pan, P., Cheng, T. and Chen, C. 2011. "New anti-phishing method with two types of passwords in OpenID system," in *Proceedings of the 5th International Conference on Genetic and Evolutionary Computing* (ICGEC '11), pp. 69–72, Xiamen, China.

Gupta, A. and Zhdanov, D. 2012. "Growth and Sustainability of Managed Security Services and Networks: An Economic Perspective," MIS Quarterly (36:4), pp 1109-A7.

Hess, T., McNab, A. and Basoggln, A. 2014. "Reliability Generalisations of Perceived Ease of Use, Perceived Usefulness and Behavioural Intentions," *MIS Quarterly* (38:1), 1-A29.

Hocking, C., Furnell, S., Clarke, N. and Reynolds, P. 2011. "Authentication Aura – A Distributed Approach to Authentication," *Journal of Information Assurance and Security* (6:2), 149-156.

Hodges, H. and Johansson, M. 1980. "Towards Kerberizing Web Identity and Services". Kerberos Consortium.

Huang, C., Ma, S. and Chen, K. 2011. "Using one-time passwords to prevent password phishing attacks," *Journal of Network and Computer Applications* (34:4), pp. 1292– 1301.

Jalil, K., Nor, F. and Manan, J. 2012. "Mitigating man in-the-browser attacks with hardware-based authentication scheme," *International Journal of Cyber-Security and Digital Forensics* (1:3), p.6.

Khalil, I., Khreishah, A. and Azeem, M. 2014. "Consolidated Identity Management System for Secure Mobile Cloud Computing," *Computer Networks* (65) pp 679-686.

Latze, C. and Ultes-Nitsche, U. 2007. "Stronger authentication in ecommerce: how to protect even Na¨ıve user against Phishing, pharming, and MITM attacks," in *Proceedings of the International Conference on Communication Systems, Networks, and Applications* (CSNA'07), pp.111–116.

Leandro, M., Nascimento, T., dos Santos, D., Westphall, C. and Westphall, C. 2012. "Multi-tenancy authorization system with federated identity for cloud-based environments using Shibboleth," in *Proceedings of the 11th International Conference on Networks* (ICN'12), pp.88–93, IARIA.

Leicher, A., Schmidt, U. and Shah, Y. 2012. "Smart OpenID: A smart card based OpenID protocol". *Information Security and Privacy Research*, (376), pp.75–86.

Madsen, P., Koga, Y. and Takahashi, K. 2005. "Federated Identity Management for Protecting Users from ID Theft," in *Proceedings of the Workshop on Digital Identity Management*, pp 77-83.

Preece, J. and Keller, L. (Eds), 1990. *Human Computer Interaction Selected Readings*, Prentice Hall: London.

Rivard, S. and Lapointe, L. 2012. "IT Implementers Response to User Resistance: Nature and Effects," *MIS Quarterly* (36:3), pp 897-A5.

Shackel, B. 1990. "Human Factors and Usability" in Preece, J. and Keller, L. (Eds), Human Computer Interaction Selected Readings, Prentice Hall: London, pp 27-41.

Sloan, K. 2009. "Security in a virtualised world," *Network Security* (9:2), 15-18.

Sun, H. 2012. "Understanding User Revision When Using Information Systems: Adaptive System Use Triggers," (36:2), pp 453-478.

Sun, S., Pospisil, E., Muslukhov, N., Dundar, K., Hawkey, K. and Beznosov, K. 2011. "What makes a user refuse web single sign on?: An empirical investigation of OpenID," in *Proceedings of the 7th Symposium on Useable Privacy and Security*. pp 4-13.

Sun, S., Boshmaf, Y., Hawkey, K. and Beznosov, K. 2010. "A billion keys but few locks: The crisis of web single sign on," in *Proceedings of the 6th Symposium on Useable Privacy and Security*. pp 61-71.

Thibeau, D. and Drummond, R. 2009. "Open trust frameworks for open government: Enabling citizen involvement through open identity technologies". Tech. Republic: OpenID Foudation and InformationCardFoudation.

Urien, P. 2010. "An OpenID provider based on SSL smart cards," in *Proceedings of the 7th IEEE Consumer Communications and Networking Conference* (CCNC'10), pp.1–2.

Yan, L., Rong, C and Zhao, G. 2009. "Strengthen Cloud Computing Security with Federated Identity Management Using Hierarchical Identity based Cryptography," in *Proceedings of the International Conference on Cloud Computing*, Beijing, China, pp 167-177.

You, H. and Jun M. 2010. "A mechanism to prevent RP phishing in OpenID system," in *Proceedings of the 9th IEEE/ACIS International Conference on Computer and Information Science* (ICIS '10), pp.876–880.

Wang, K. and Shao, Q. 2011. "Analysis of cloud computing and information security". In *Proceedings of the second International Conference on Frontiers of Manufacturing and Design Science*. Pp. 3810-3813, Taichung Taiwan.