Business Horizons (2016) xxx, xxx—xxx

Available online at www.sciencedirect.com

ScienceDirect

KELLEY SCHOOL OF BUSINESS
INDIANA UNIVERSITY

www.elsevier.com/locate/bushor

Evaluating single sign-on security failure in cloud services

Brian Cusack*, **Eghbal Ghazizadeh**

Auckland University of Technology, 55 Wellesley Street East, Auckland 1142, New Zealand

KEYWORDS
Cloud services;
Internet security;
User behavior;
SSO;
Device security failure

Abstract Business use of cloud computing services is motivated by ease of use and 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 of cloud computing also bring optimization challenges for the information owners who must assess service security risks and the degree to which new human behaviors 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) authorization, asking: What are the optimal behavioral expectations for a cloud service information owner? Federated identity management provides well-developed design literature on strategies for optimizing human behaviors in relation to the new technologies. We briefly review the literature and then propose a working solution that optimizes the trade-off between disclosure risk, human user risk, and service security.

1. Cloud single sign-on demand

The problem of user authentication in the cloud environment has arisen as a usability issue, in that users object to repeating logon behavior multiple times, for multiple identities, for many different services and service providers (Shackel, 1990; Wang & Shao, 2011). Similarly, users may be using multiple devices to access services simultaneously and independently. The problem is accentuated in the cloud computing environment when the layers of complexity are reduced and the risk of unauthorized access to services increases. One of the broad research areas providing solutions to the problem has been that of federated identity management. Such solutions include single sign-on (SSO), OpenID, One Time Passwords (OTP), and other innovative designs that facilitate the ease of human behavior while hardening the technology protection (Gupta & Zhdanov, 2012; Hocking, Furnell, Clarke, & Reynolds, 2011). Each solution has usability strengths and weaknesses but also security risk and effectiveness trade-offs. In this article our interest is in the management of risk around an identity. All parties must accept that sufficient precautions are taken to

* Corresponding author
E-mail addresses: brian.cusack@aut.ac.nz (B. Cusack), eghaziza@aut.ac.nz (E. Ghazizadeh)

0007-6813/$ — see front matter
http://dx.doi.org/10.1016/j.bushor.2016.08.002

prevent theft by an unauthorized party while allowing a seamless user experience for legitimate beneficial parties (Hess, McNab, & Basoglu, 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, Rong, & Zhao, 2009). Current challenges relate to the proprietary nature of many services and the lack of general standardization for interoperability (Leandro, Nascimento, dos Santos, Westphall, & Westphall, 2012). To some extent the problem is addressed in independent authorization agencies to whom each service provider refers user authentication. The scope of authorization 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, Koga, & Takahashi, 2005). It is up to the authentication service user to determine the use of the authorization for matters of access control. 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 if multiple sets are used (assuming differentiation). The problem is accentuated if user identity is compromised or if a service is left open for long periods of time (Huang, Ma, & Chen, 2011). In both instances, user expectation presents technical and design challenges for information security. If the risk management requires a user to provide identification every two—three minutes to keep the service active or if each service or device activated requires a fresh authentication of identification, then the user must adopt new behaviors. The user may resist the new behaviors and forgo the service (Rivard & Lapointe, 2012). Both breach and non-use of a system are failures, hence the optimization of human behavior against a robust security design requires innovation and scoping for cloud environments (Sun et al., 2011).

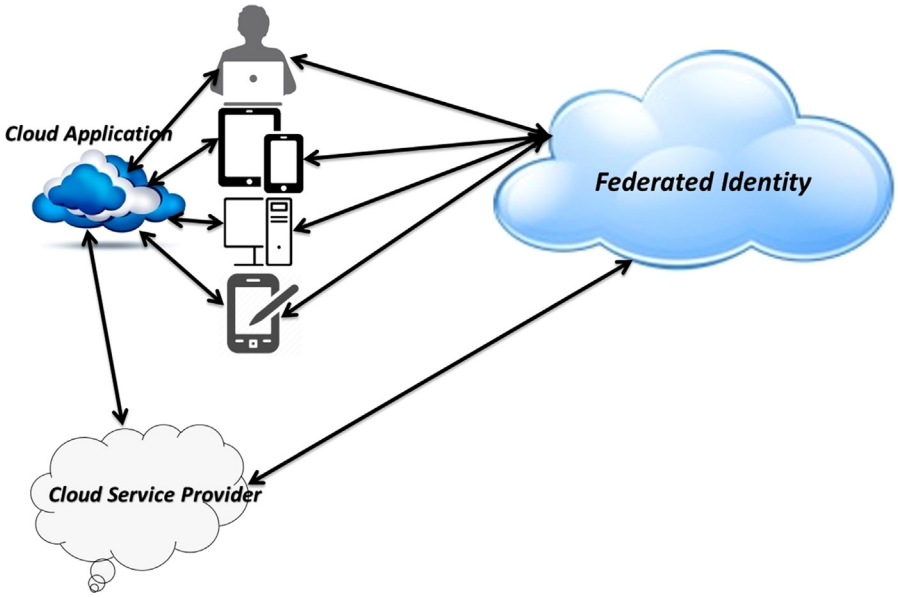
This article is structured to introduce the cloud identity problem and then to elaborate potential solutions. The following section briefly introduces federation theory and the SSO opportunity. The issues of risk and behavioral modification are discussed in terms of potential system failure. It is assumed humans prefer SSO as a behavioral solution but the challenge is to match this behavior with a secure architecture. The literature analysis shows that there is no model that 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 article concludes with a discussion of trust as a utility facilitator in socio-technical security systems.

2. Cloud identity management system

In this section we discuss popular identity management technologies and solutions that allow end users to manage their personal attributes required for accessing certain services. These approaches highlight benefits of each in regards to the cloud identity system access. A general view of the cloud identity management system and process is shown in Figure 1. The federation establishment requires that providers exchange metadata; such metadata contains identifiers, public key certificates, and service attributes. These are used for the location and secure communication between providers' services. This decoupling between providers enables identity providers to support many service providers in a distributed fashion, and also to focus on managing identities, accessing control policies, and issuing security tokens.

OpenID as a part of the SSO today is commonly used between cloud service providers. OpenID 2.0 is a security assertion markup language (SAML) protocol determined by the same necessities for web space and web SSO, but the design goal is different. In particular, the main idea of OpenID is that a user can authenticate via URL and subsequently exhibit their preferred OpenID provider. OAuth defines a protocol in order for clients to access server resources on behalf of a resource owner. This provides a means for end users to authorize third-party access to their server resources without sharing their credentials. Windows CardSpace—also known by its codename, InfoCard—is the Microsoft client or identity selector for the identity metasystem, a system connecting multiple identity systems within one interface. Taking into consideration that end users may have different identities depending on the context in which they are interacting, the challenge of this approach is to allow end users to create, use, and manage their diverse digital identities in an understandable and effective way. The idea behind Windows CardSpace is that end users could manage their digital identities, along with their related attributes, in a way similar to how they manage their cards in their wallets.

Figure 1. Cloud entity relationship model



U-Prove is a cryptographic technology that presents a type of credential or token to encode end user attributes in such a way that the issuance and the presentation of such tokens remains unlinkable. The U-Prove technology makes use of zero-knowledge proof methods to issue the tokens. Zero-knowledge proof is a way for end users to prove possession of a certain piece of information without revealing it. That is, an end user can provide an assertion containing a set of attributes, revealing nothing beyond the validity of such an assertion and the attributes. Similar to U-Prove, Identity Mixer (Idemix) is an anonymous credential system following the protocols in order to allow the end users to control the dissemination of personal information and preserve their privacy. An end user can obtain credentials containing attested attributes from identity providers and prove to a service provider the validity of such attributes without revealing any other information (Tormo, Mármol, & Pérez, 2014).

Higgins is an open source identity framework designed to enhance the end user experience by integrating identity profiles and social relationship information across multiple sites. A personal data service (PDS) is a cloud-based service that works on behalf of the end users, giving them a central point for controlling their personal information. It not only manages end users' attributes, but it also manages data flows to external businesses and to other end users' PDSs. The certification program for OpenID Connect was launched on April 22, 2015. OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify end user identity based on the authentication performed by an authorization server, as well as allowing clients to obtain basic profile information about the end user in an interoperable manner.

Researchers' in-depth analysis of various cloud-based integrated database management systems (IDMSs) reveals most systems do not offer support to all the essential features of cloud IDMS. The ones that do have their own weaknesses. None of the techniques heuristically cover all of the security features. Moreover, they lack compliance with international standards, which understandably undermines their credibility. Although identified features are worth considering, they are not mandatory as security and business requirements vary from one organization to the other.

In order to preserve privacy, some systems avoid direct communication between service providers and identity providers, so the latter cannot trace end users' accesses. However, this can result in difficult implementation of other features or requirements. For example, OAuth and Higgins issue authorization tokens to allow the service providers direct access to user information under certain conditions, instead of sending the information directly into the token. Hence, the identity provider and the service provider could exchange information even if the end users go offline. Furthermore, attribute revocation is hard to achieve when using systems like U-Prove or Idemix where end users can present attributes without involving the identity provider. Additionally, since the identity provider cannot trace end users' accesses, the end users are completely anonymous to the service provider; this

makes it difficult to provide these systems with accurate audit mechanisms.

Nevertheless, some of the defined requirements are not properly managed by any of the presented systems—attribute aggregation, for example. SAML, OpenID, and OAuth are focused on having a unique identity provider manage all identity-related end user information, so attribute aggregation is not considered. In turn, CardSpace, Higgins, U-Prove, and Idemix support credentials and attributes from different identity providers, having an information card from each of them. However, they do not allow presenting information asserted by different providers at the same time. Identity management systems also assume that trust relationships are established, so they usually require that end users attributes are asserted by a reliable entity.

3. Single sign-on risks

Federated authorization relies on the existence of mechanisms beyond an organization or domain to cooperate for the authentication of users (Yan et al., 2009). In cloud environments the ideal is to have transparent and global mechanisms that permit general authorization regardless of service, device, or location. The current challenge is the level of cooperation that must be gained for mechanisms to communicate with different systems and yet retain the integrity of the authorization process (Leandro et al., 2012). A general solution is to take the responsibility for authentication away from any system and instead to refer it to an external authority. Such an architecture introduces the concepts of trust and a trusted third party (Abbadi & Martin, 2011; Thibeau & Reed, 2009). The independence of the third party permits single enrollment 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 also can gain information about the user from other MASPs, as well as from 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 of messaging, data processing, and data storage. These benefits are passed to the user by way of minimal behavioral modifications for cloud services (Faulkner & Runde, 2012). The ideal behavior for a user is to perform a single sign-on for all services.

SSO opportunity has implications for system architecture and the management of risk levels associated with system failure. Failure, in this sense, 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, negative consequences occur. The level of risk in these instances impacts the objectives of the system and requires mitigation (Rivard & Lapointe, 2012; Sun, 2012). A SSO opens the system to a number of attacks (see Figure 3) that may eventuate in user identification being compromised. Madsen et al. (2005) describe identity theft as being exploitation of another user's individual information to perform fraud. Federated identity management (FIM) simplifies authorization for users by removing repetition and layers of complexity that would usually be barriers to an intruder's attack. 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 authorization to much more than if they had hacked a domain- and device-specific authorization (Sun, Boshmaf, Hawkey, & Beznosov, 2010).

The SSO FIM requirements also open the user identity to both intentional and unintentional misuse. In the case of intentional misuse, the federated arrangements in a cloud environment pass the user identity and information to various parties that are often beyond user control and knowledge. The information exposure can include cross-jurisdictional matters, misaligned SLA arrangements, and different information security standards (Yan et al., 2009). For example, carefully embedded identification marking and cryptographic measures may not pass from the user to each service supplier without spoliation. In terms of unintentional misuse, different service suppliers may have different standards for the reuse of identification information, the supply of service, and privacy rules. This can result in the user receiving 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 usability of a system frame a user's expectation for experience: ease of learning, efficiency, ease of recollection, error recovery, and user satisfaction. The degree to which an SSO failure impacts the user experience may be observed in behavioral changes. Unfortunately, the misuse of an identity is usually only detected after a security breach and in association with an unplanned event,

which may be frightening, threatening, and financially costly. Effective error recovery, for example, may regain a user's trust in a cloud service and help put emotional and financial risks into perspective. However, successive negative feedback across the five usability properties leads to risk aversion and user resistance to the cloud services (Faulkner & Runde, 2012; Rivard & Lapointe, 2012; Shackel, 1990).

4. Trust computing

While security might be the dominant term when it comes to protection of sensitive data, trust is a much stronger concept that goes beyond the basic security pillars of confidentiality, availability, integrity, and nonrepudiation. Trust tries to formulate a good-faith relationship between computing machines, as well as between users. From an IT perspective, trust is not only about securing the communication channel or authenticating the data sender, but also about trusting that the sent information is legitimate, that it does not include malicious codes, and that it will not harm the receiver in an unforeseen way. In other words, trust extends to the sender itself by believing that they will obey specific communication rules and will not abuse communication by exhibiting non-responsiveness or selfish behavior (Fournaris & Keramidas, 2014).

Trust is a complex concept for which there is no universally accepted scholarly definition. As a psychological state, trust is comprised of the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another (Pearson, 2013). Moreover, trust is a broader notion than security as it includes subjective criteria and experience. There exist both hard (security-oriented) and soft trust solutions; hard trust involves aspects like authenticity, encryption, and security in transactions, whereas soft trust involves human psychology, brand loyalty, and user-friendliness. An example of soft trust is reputation, which is a component of online trust that is perhaps a company's most valuable asset (Wang & Lin, 2008).

People often find it harder to trust online services than offline services because of the absence of physical cues in the digital world and, possibly, a lack of established centralized authorities. The distrust of online services can even negatively affect the level of trust accorded to organizations that may have been long respected as trustworthy. Some would argue that security is not even a component of trust and that the level of security does not affect trust (Pearson, 2013).

In general, trust management can include security measures focused on either policy-based measures or soft trust relationships and reputation-based measures. Policy-based approaches define permissions, obligations, norms, and preferences for an entity's actions and interactions with other entities. These approaches can also be defined as sets of rules and practices describing how an organization manages, protects, and distributes sensitive information at several levels. However, both policy-based and soft trust management approaches address the problem of establishing trust among interacting parties in distributed and decentralized systems. Reputation can be established for entities like web communities' users, services, or software agents (Alnemr, Koenig, Eymann, & Meinel, 2010). A cloud provider has to address trust issues in a meaningful way for its tenants. These needs translate into a set of foundational usage models for trusted clouds that apply across the three infrastructure domains (Yeluri & Castro-Leon, 2014).

5. A proposed solution

The review of current literature suggests that the positioning of an external authorization power 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 these 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 lower layers that are out of sight to users. The proposal is presented as a conceptual relationship model (Figure 2) for ideal relationships. A workflow model (Figure 3) itemizes the steps in a SSO process, and an architectural model captures the relationships and information flows. Finally, the proposed solution is subjected to 11 theoretical attacks identified from the literature and assessed against other alternative SSO opportunities (Table 1). Process steps depicted in Figure 2 are summarized as follows:

- Step 1: OpenID provider (IDP) allows the user to sign in to websites using a single identifier in the form of a URL.

Figure 2. Cloud conceptual relationship model

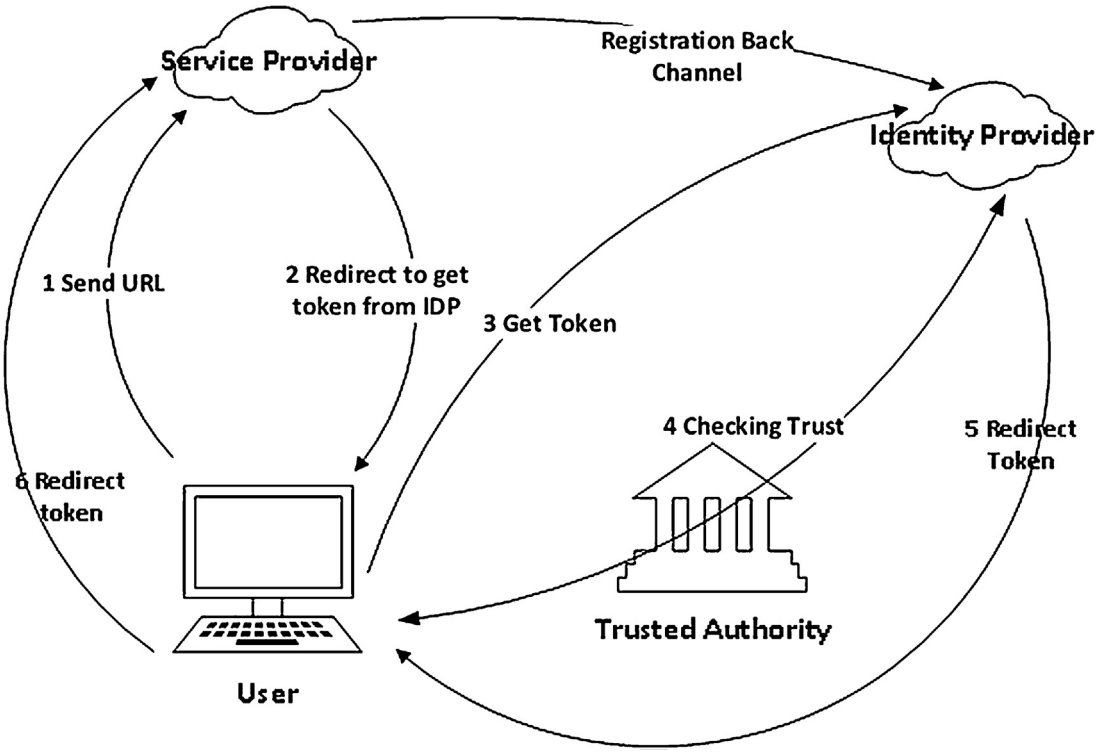


Figure 3. Workflow architecture

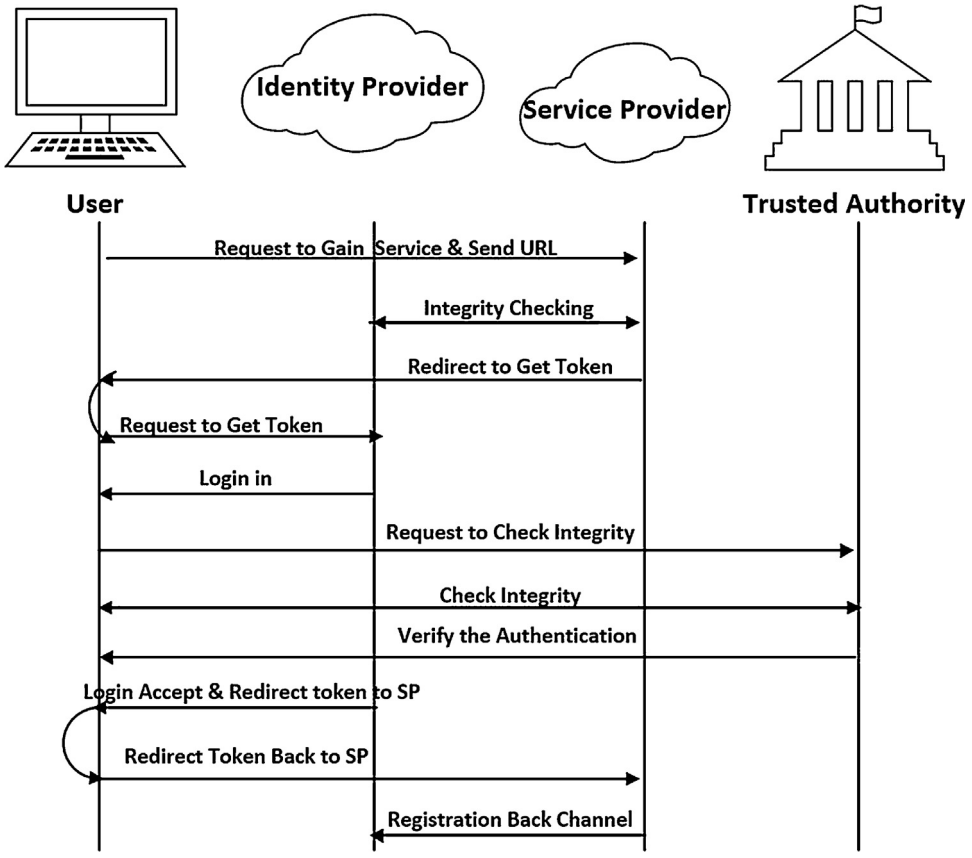


Table 1. Proposed model resistance to attack

Title	Insider Attack	MITM	Phishing Attack	DNS Poisoning
Ding and Wei (2010)			*	*
You and Jun (2010)			*	*
Feng, Tseng, Pan, Cheng, & Chen (2011)		*	*	
Thibeau and Reed (2009)			*	
Urien (2010)		*	*	
Nor, Jalil, & Manan (2012)		*		
Latze (2007)		*	*	
Huang et al. (2011)	*		*	
Leicher, Schmidt, & Shah (2012)			*	
Leandro et al. (2012)	*			
Hodges, Howlett, Johansson, & Morgan (2008)			*	*
Proposed Model	*	*	*	*

*Indicates the model is resistant to this attack

- Step 2: The service provider (SP) locates the user's location and creates an authentication token. SP asks the user to prove their identity.
- Step 3: The browser proceeds with token exchange based on SAML protocol.
- Step 4: Using trusted authority (TA) as the core, the user's browser, relying party (RP) or SP, and IDP must prove their identities based on a mutual attestation process using their TPM-enabled platforms and be verified by the TA.[1]
- Step 5: If, and only if, the mutual attestation process has been successful (i.e., the user and IDP have confidence in each other) then the IDP will deliver the SAML token to the user's browser.
- Step 6: IDP sends an encrypted token by the user's public key that shows the 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 SP, and the IDP. In addition, an 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 communication is 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 verification (the 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 the first component needs to measure the second component and the trusted second component then needs to measure the third component, continuing in this way 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 trustworthy to the trust authority (the verifier).

In Figure 3 the work flow steps of the conceptual model are illustrated to itemize the interactions. The model 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 3 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 the situation wherein a user requires a single logon. Four attacks are chosen to be indicative of vulnerabilities and sufficiently show that the proposed model has performance advantages over others. In designing our model, we were aware of these threats and

[1] This is the most critical step of our proposed OpenID trust-based federated identity architecture.

therefore deliberately designed to secure the system. The adoptions made in Figures 2 and 3 provide a secure environment while considering user requirements for a seamless experience. Testing can be pushed further in practice testing, but we stayed within our research scope of theory.

6. Security failure

The advantages of delivering cloud services with computing resources that have a demonstrated chain of trust rooted in hardware include reducing risks, preventing unsafe transit, and maximizing and scaling operational efficiency. Reducing the risks for co-residency ensures the infrastructure is trusted and has demonstrable integrity, preventing the launch and execution of untrusted components. This method not only protects against malware but also against benign conditions such as the improper migration or deployment of virtual machines. Preventing the unsafe transit of secure virtual machines means that virtual machines arriving from an unsecured platform are not allowed to move to secured platforms, and virtual machines originating on secured platforms are not allowed to move to unsecured ones. Once platform trustworthiness can be measured, cloud providers can put such measurements to use by building trusted pools of systems, all with identical security profiles, which means maximization and scale of operational efficiency. Hypervisors can then make more efficient use of secure clouds, moving virtual machines with similar security profiles within zones of identically secured systems for load balancing and other administrative purposes (Yeluri & Castro-Leon, 2014).

Through the TPM mechanisms, the trust state of a system can be reliably measured and recorded. To achieve a quantified trust state, every part of the computer system from hardware level to application level is measured from boot time. This authenticated boot sequence measurement guarantees the system is not compromised and can be trusted. The TPM platform configuration registers (PCRs) play an important role in the above boot sequence. The authenticated boot measurement follows a daisy chain approach, meaning that each component is measured and compared with existing known good value on the SML. In this way, measurement integrity is retained and the boot sequence can be trusted, meaning that no system component has been compromised (Arthur, Challener, & Goldman, 2015).

The TPM chip is capable of storing a wide variety of information in a secure way. Such information can be divided into asymmetric cryptography keys and symmetric cryptography keys or data. Secure storage follows a protected object hierarchy in which higher-level keys are used for signing/protecting lower-level keys within this hierarchy. The root of the key hierarchy is the storage root key (SRK), which is an asymmetric key pair (2048 bit RSA keys) generated using the endorsement key (EK) at the first TPM power-on. The TPM can be used in order to provide secure sealing functionality (Fournaris & Keramidas, 2014).

Moreover, TPM is able to provide TPM host system trust attestation reports to external third parties, thus proving the system can be trusted. The attestation operation should be unique and undeniable for each TPM host computer system. The TPM can be uniquely identified using the EK values. However, the need to protect the TPM identity and its host's anonymity dictates that this approach cannot be used in practice (Proudler, Chen, & Dalton, 2015). The attestation process, denoted as remote attestation, involves a specific attestation identity key (AIK) pair, a TPM-specific state that provides a captured instant of the PCR's values, and a series of nonce numbers (Yang & Guo, 2015).

7. Trusting behavior

Trust is a two-way event 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 optimizing beneficial activities and minimizing 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 if, for example, the utility is perceived as too low, privacy is breeched, and so on. Unfortunately, any identity compromise is not usually known until the negative consequences materialize. Also, the user 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 optimized through learned behaviors. However, there is a strong tension between learning with positive consequences and learning with negative consequences when the perceived risk is heightened. Personal, valuable, and private information is transacted through multiple agencies when cloud services are used. The user tolerance for negative feedback in learning is lower in such a context, as is the tolerance for puzzling interfaces. 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, causing the tension between the service and the user expectation to be heightened.

In our proposed model, we have integrated a trusted computing system with the cloud services of agency and authorization in order to address the technical concerns of communication. User confidence has been discussed under the five properties of the usability criteria, with the expectation that a user requires all five properties to deliver in their favor with zero negative feedback. In practice, however, two other factors—technical trust and management services—come into play, which we have structured to mediate positive and negative feedback. Importantly, these factors place the user in a negotiated position that balances system expectations with user expectations. In such a context the user can be expected to modify their behavior in keeping with managed and minimalistic system demands. The user may have a seamless SSO experience for many cloud services but they are expected to enroll 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 must experience and accept for service in our proposal. Consequently, in our models we have built in technical trust, so as to minimize negative feedback, and management services to enhance user confidence levels and ease of behavioral modification.

8. Conclusion

In this research we set out to answer the question: What are the optimal behavioral expectations for a cloud service information owner? We assumed that there are many users but that some users hold a rightful ownership responsibility for the information transacted in a cloud. We have also assumed that human behavior fits the five properties in the cited usability literature and therefore 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 the 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. Behavior and protection from failure is optimized in such a negotiated situation.

References

Abbadi, I., & Martin, A. (2011). Trust in the cloud. *Cloud Security: Information Security Technical Report, 16*(3/4), 108—114.

Alnemr, R., Koenig, S., Eymann, T., & Meinel, C. (2010). Enabling usage control through reputation objects: A discussion on e-commerce and the internet of services environments. *Journal of Theoretical and Applied Electronic Commerce Research, 5*(2), 59—76.

Arthur, W., Challener, D., & Goldman, K. (2015). *A practical guide to TPM 2.0: Using the new trusted platform module in the new age of security.* New York: Springer.

Ding, X., & Wei, J. (2010). A scheme for confidentiality protection of OpenID authentication mechanism. In *Proceedings of the 2010 International Conference on Computational Intelligence and Security* (pp. 310—314). Piscataway, NJ: IEEE.

Faulkner, P., & 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, J., Cheng, P., & Chen, C. (2011). New anti-phishing method with two types of passwords in OpenID system. In *Proceedings of the 2011 International Conference on Genetic and Evolutionary Computing* (pp. 69—72). Piscataway, NJ: IEEE.

Fournaris, A. P., & Keramidas, G. (2014). From hardware security tokens to trusted computing and trusted systems. In N. Sklavos, D. Goehringer, M. Hübner, & P. Kitsos (Eds.), *System-level design methodologies for telecommunication* (pp. 99—117). New York: Springer.

Gupta, A., & Zhdanov, D. (2012). Growth and sustainability of managed security services and networks: An economic perspective. *MIS Quarterly, 36*(4), 1109—1130, A1—A7.

Hess, T., McNab, A., & Basoglu, K. (2014). Reliability generalisations of perceived ease of use, perceived usefulness, and behavioural intentions. *MIS Quarterly, 38*(1), 1—28, A1—A29.

Hocking, C., Furnell, S., Clarke, N., & Reynolds, P. (2011). Authentication aura — A distributed approach to authentication. *Journal of Information Assurance and Security, 6*(2), 149—156.

Hodges, H., Howlett, J., Johansson, M., & Morgan, R. L. (2008). Towards Kerberizing web identity and services. *MIT Kerberos Consortium*. Available at http://www.kerberos.org/software/kerbweb.pdf

Huang, C., Ma, S., & Chen, K. (2011). Using one-time passwords to prevent password phishing attacks. *Journal of Network and Computer Applications, 34*(3), 1292—1301.

Latze, C., & Ultes-Nitsche, U. (2007). Stronger authentication in ecommerce: How to protect even naïve users against phishing, pharming, and MITM attacks. In *Proceedings of the 2007 IASTED International Conference on Communication Systems, Networks, and Applications* (pp. 111—116). Anaheim, CA: ACTA.

Leandro, M., Nascimento, T., dos Santos, D., Westphall, C. M., & Westphall, C. B. (2012). Multi-tenancy authorization system with federated identity for cloud-based environments using Shibboleth. In *Proceedings of the 2012 International Conference on Networks* (pp. 88—93). Wilmington, DE: IARIA.

Leicher, A., Schmidt, A., & Shah, Y. (2012). Smart OpenID: A smart card-based OpenID protocol. In *Proceedings of the 2012 IFIP Information Security and Privacy Conference* (pp. 75—86). New York: Springer.

Madsen, P., Koga, Y., & Takahashi, K. (2005). Federated identity management for protecting users from ID theft. In *Proceedings of the 2005 Workshop on Digital Identity Management* (pp. 77—83). New York: ACM.

Nor, F. B. M., Jalil, K. A., & Manan, J. A. (2012). Mitigating man-in-the-browser attacks with hardware-based authentication

scheme. *International Journal of Cyber-Security and Digital Forensics, 1*(3), 204—210.

Pearson, S. (2013). Privacy, security, and trust in cloud computing. In S. Pearson & G. Yee (Eds.), *Privacy and security for cloud computing* (pp. 3—42). London: Springer.

Proudler, G., Chen, L., & Dalton, C. (2015). *Trusted computing platforms: TPM 2.0 in context*. Cham, Switzerland: Springer.

Rivard, S., & Lapointe, L. (2012). Information technology implementers' responses to user resistance: Nature and effects. *MIS Quarterly, 36*(3), 897—920, A1—A5.

Shackel, B. (1990). Human factors and usability. In J. Preece & L. Keller (Eds.), *Human-computer interaction: Selected readings* (pp. 27—41). Upper Saddle River, NJ: Prentice Hall.

Sloan, K. (2009). Security in a virtualised world. *Network Security, 2*, 15—18.

Sun, H. (2012). Understanding user revision when using information system features: Adaptive system use and triggers. *MIS Quarterly, 36*(2), 453—478.

Sun, S-T., Boshmaf, Y., Hawkey, K., & Beznosov, K. (2010). A billion keys but few locks: The crisis of web single sign-on. In *Proceedings of the 2010 New Security Paradigms Workshop* (pp. 61—71). New York: ACM.

Sun, S-T., Pospisil, E., Muslukhov, I., Dindar, N., Hawkey, K., & Beznosov, K. (2011). What makes a user refuse web single sign-on? An empirical investigation of OpenID. In *Proceedings of the 2011 Symposium on Useable Privacy and Security* (pp. 4—13). New York: ACM.

Thibeau, D., & Reed, D. (2009). *Open trust frameworks for open government: Enabling citizen involvement through open identity technologies* [White Paper]. Available at http://openid.net/docs/Open_Trust_Frameworks_for_Govts.pdf

Tormo, G. D., Mármol, F. G., & Pérez, G. M. (2014). Identity management in cloud systems. In S. Nepal & M. Pathan (Eds.), *Security, privacy, and trust in cloud systems* (pp. 177—210). New York: Springer.

Urien, P. (2010). An OpenID provider based on SSL smart cards. In *Proceedings of the 2010 IEEE Consumer Communications and Networking Conference* (pp. 1—2). Piscataway, NJ: IEEE.

Wang, K., & Shao, Q. (2011). Analysis of cloud computing and information security. In *Proceedings of the 2011 Second International Conference on Frontiers of Manufacturing and Design Science* (pp. 3810—3813). Enfield, NH: Trans Tech.

Wang, Y., & Lin, K-J. (2008). Reputation-oriented trustworthy computing in e-commerce environments. *IEEE Internet Computing, 12*(4), 55—59.

Yan, L., Rong, C., & Zhao, G. (2009). Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography. In *Proceedings of the 2009 First International Conference on Cloud Computing* (pp. 167—177). Berlin: Springer.

Yang, B., & Guo, H. (2015). Remote attestation on trusted cloud computing. *Applied Mechanics and Materials, 696*, 161—166.

Yeluri, R., & Castro-Leon, E. (2014). *Building the infrastructure for cloud security*. New York: Springer.

You, J-H., & Jun, M-S. (2010). A mechanism to prevent RP phishing in OpenID system. In *Proceedings of the 2010 IEEE/ACIS International Conference on Computer and Information Science* (pp. 876—880). Washington, DC: IEEE Computer Society.