2010 3rd International Conference on Advanced Computer Theory and Engineering(ICACTE)

User Requirement Model for Federated Identities Threats

Zubair Ahmad and Jamalul-Lail Ab Manan
Cyber Security Cluster
MIMOS Berhad
Technology Park Malaysia, Kuala Lumpur, Malaysia
zubair.khattak@mimos.my, jamalul.lail@mimos.my

Suziah Sulaiman
Department of Computer and Information Sciences
Universiti Teknologi PETRONAS
Bandar Seri Iskandar, 31750 Tronoh, Perak, Malaysia
suziah@petonas.com.my

***Abstract*—Federated identity management system interconnects distributed island of identity management systems with federated identity standards with single sign-on facility. In an open environment, such as those of a federated identity management system a user single sign-on credentials, can easily fall prey to identity theft, or unlawful information gathering. It may use either existing account or new account fraud. In this paper, we present scenarios related to identity theft, unlawful information gathering and tracking. We show the main issue of lack of platform trust in platforms involve in federated systems and discussed the consequences of respective threats on them. In an effort to present a holistic approach to handle security, trust and privacy, we propose a user requirement model involving these core issues for federated identities. These requirements include system trustworthiness, hardware protected key generations, usability, efficiency, identity information validity, privacy, accountability and system robustness. In our proposed model, Trusted Platform Module (TPM), is the fundamental component which ties and binds all communicating platforms together in authentication, verification and trustworthiness of the platform.**

Keywords-identification infromation; identity theft; platform trust; privacy; security; trusted platform module

I. INTRODUCTION

Federated Identity Management System (FIMS) is an example application for Federated Environment (FE) that facilitates organizations to share resources based on business agreements, cryptographic trust, and user identifiers or attributes across security domains.

The three main entities in FIMS [1] include user, Identity Provider (IDP), and Service Provider (SP). The popular single sign-on (SSO) scheme that allow a user to logon only once using his/ her username and password and then access multiple services without reauthentication. In SSO systems, user credentials concern such as identity theft [2] that can use by the adversary to obtain the user confidential information that can invade user privacy.

A. Identity Theft

According to Gonzales and Majoras [3], Identity theft is the misuse of another individual's personal information to commit fraud. Identity theft can be subcategoriseds in two: existing account fraud, which, attacker takes charge over existing account; and new account fraud, where the attacker uses personal information to create new accounts on victim's name. Latest trend in new account identity theft the adversary/ predator may a victim's identity two methods. The first is a Low- tech method, by diving rooting through garbage for personal information, and the second is a Higher-tech method, by hacking into corporate computer systems, stealing a laptop containing identity information, phishing, and use malicious computer code to obtain the user or system information.

The FIMS is at risk if single-sign-on username and password are compromised to the identity theft and opens the doors to the rest of organization information, such as in [4]. For example, the Microsoft Live ID (Federated Identity System) is hotmail services that allow the user to sign- in once and have access to multiple services such as hotmail, messenger, Xbox live, office online, Skydrive and bing have been compromised to the phishing attacks. The author in [4] showed that's a single phished email username/ password could result in user business data being compromised, backed up documents or business documents being exposed, as well as search result being visible. This further could lead to financial disaster if Xbox live account is compromised. It shows that if SSO password is most vulnerable and once compromised it will open the doors to the rest of personal information.

B. User Identification Information Gathering

To determine the existing link between data breaches and identity theft is challenging because ID theft victims often do not know how their personal information was acquired [5]. The study conducted by panda security [6] found that Trojans, designed to steal personal identifiable or financial information that lead to identity fraud rose by 800 present from the first half to the second half of 2008. Further, researcher forecast based on the previous 14 months analysis that this rate would increase 336 percent per month throughout 2009.

The Identity theft and user information gathering can happen in the presence of weak cryptography where IDPs and SPs collude with each other. The IDPs and SPs in our case are the entities that gathering user information, therefore we assuming the term user identification information instead of personal identification information.

Our paper is structured as follows. In Section II, we discuss the related work. In Section III, we present threat analysis with scenarios. In Section IV, we discuss security, privacy and trust relationship and its effect on identified problems. In Section V, we propose a user requirement

978-1-4244-6542-2/$26.00 © 2010 IEEE

model for federated identities and we conclude with an outlook on future work in Section VI.

II. FEDERATED IDENTITY MANAGEMENT SYSTEMS

The most discussed FIM model in literature are Kerberos, Liberty Alliance, OPEN ID, Windows Live ID. In this paper we discuss only the first two with SAML. Microsoft Federated Identity Management System uses SSO facility. Two approaches exist to achieve SSO functionality such as close and open environment [7]. We talk only on open environment SSO issues in Kerberos, SAML, and Liberty alliance.

The Kerberos is an interdomain 'network authentication system' [8]. Kerberos security infrastructure is based on symmetric cryptography where every user and SP shares a long-term secret key with Authentication Server to perform encryption operation that is privacy risk. Some limitations specified in [9], Kerberos is not effective against password guessing, requirement of trusted path for password (insecure in the case of Trojan horse, man-in-the-middle attack).

Liberty Alliance [10] consists of a federation of over 140 companies. In [11] it is demonstrated that a man-in-the-middle attack against the Liberty-enabled client and proxy profile: a dishonest service provider could interpose itself between a Principal and an honest service provider (or even simply pretend to be the Principal without an initial request from the Principal) and then request authentication to the SP. In Liberty Alliance, user privacy can be compromised in various ways such as.

- IDP knows all user identifiers and SPs collude with IDP to link the user pseudonym.
- SPs possibly able to associate SSO identities based on user network address.
- Profiling, individual SPs may maintain the user information for instance telephone numbers, shopping habits, credit card numbers that could use to link the identifiers.

In addition to identity theft (security) and user identity information gathering (privacy), entity trust is also an important aspect. Defining trust relative to security architecture methodology is a set of principles [12] such as

- Trust binding unique attributes to a unique identity
- Trust is enabler of confidence that some thing will occur in predictable manner
- Trust is a binary or set of compound binary relationship based on individual identity or unique characteristic validation

According to ITU-T X5.09 Section 3.3.54 trust is defined as follows: "Generally an entity can said to "trust" a second entity when it makes the assumption that the second entity will behave exactly as the first entity expects [13]." In FE trust can either be direct, indirect and multidimensional (recommendation, past experience, reputation and belief). However, trust that we define in our research is for a platform only, and will not include trust for user. We emphasize that for user, we need to ensure authentication is being used instead.

The Trusted Computing Group (TCG) initiate Trusted Platform Module (TPM) [14] that provides many hardware and software properties that remotely attest the platform hardware or software configuration to vouch trustworthiness of hardware devices in distributed environment, it supports hard-ware based software integrity reporting, secure storage, temper resistance, theft deterrence, platform authentication, integrity measurement. Therefore, the hardware trust can elevate bring more security and privacy in federated system entities. Later we will show in Section IV why trust is important.

III. ATTACK ANALYSIS

Threat is a potential violation of the system security and the effects may appear in the form of some negative impacts. The following threat model first appeared in [15]. The reason of the threat analysis to show the conventional platforms are lacking in handling the following threats.

- Threat 1: User web based SSO credential (user name, password) can easily compromised via man-in-the-middle attack in open network (Internet). Attacker can use the theft ID to access confidential information (user identification information).
- Threat 2: IDP and SP could misuse user identity information via user registration or serving with authentication services. In reality, Federated Environment, some potentially malicious IDP, SPs could misuse user identity information to share it with other SPs or third parties.
- Threat 3: In reality, there is no platform trust between the communicating platforms. Most of the current trust is relying on the digital certificates (containing public key, serial number, etc.) issuing by CA.

A. Scenario 1: Man-in-the-Middle Attack

In this attack, adversary uses the well-known weakness that who controls the Domain Name Service (DNS) can impersonate. We present a man-in-the-middle attack in which adversary (Adversary) (a proxy) between browser (Browser) and source site (Source-site), such as (Browser)←→(Adversary)←→ (Source-site).

- Prerequisites: Suppose an adversary (Adversary) that can crack the DNS and the adversary then can act with a hostname not belonging to him/ her and can impersonate certain URLs. Additionally we assume that the source site (Source-site) have no protection against man-in-the-middle attacks.
- The Attacker: Adversary (Adversary) crack the DNS, uses its ability, to impersonate inter-site transfer URL #ist-url#Source-site of source site (Source-site) to browser (Browser). (Adversary. Source-site): impersonate the source site (Source-site) #ist-url#Source-site to browser (Browser). So, → #ist-url#Source-site (Browser) = #ist-url#Adversary
- Browse → Adversary. Source-site: finish redirect (Note: In the above step, profile does not claim authentication)

- Adversary. Browser→ Source-site: finish redirect, The adversary (Adversary. Browser) impersonates browser (Browser) to (Source-site); (Adversary): Adversary acts as man-in-the-middle between (Browser) and (Source-site), due to the lacking of user-tracking system of (Source-site) have no resistant against man-in-the-middle attacks, as a result (Adversary) can forward all communication between (Browser) and (Source-site) during the user tracking.
- Source-site → Adversary. Browser: forward redirect request to #ar-url#Destination-site. This contains e.g. SAML artifacts for (Browser) that could readable by (Adversary.Browser). Therefore (Adversary. Browser) starts to impersonate (Browser) to destination site (Destination-site).
- Adversary. Browser → Destination-site: close down redirect to #ar-url#Destination-site. So adversary (Adversary. Browser) impersonate (Browser) to (Destination-site). For instance, redirect contains SAML artifices and allows (Adversary. Browser) to act as using the permissions of (User).
- Adversary → Browser: send redirect request to #ist-url#Sourc-site. So the original redirect sends, by Adversary (Adversary), to browser (Browser). Therefore, profile assumes user already has been authenticated to (Source-site). So in the end adversary re-initiate a normal protocol to run (Browser) with maximum probability that the user would not notice rest of the protocol running.

B. Scenario 2: User Information Gathering

Privacy threats result from poor data gathering, handling practices, centralized data, excessive data collection, leaky channels, and linkability are chief perpetrators. In Liberty Alliance, protocols pass information in URLs, if not following proper mechanism it can compromise user privacy such as if the IDP login form is embedded within service provider page. Therefore, seamlessness contact submits the user credentials back to identity service provider. In this mechanism user potentially revealing his IDP credentials to SPs in clear-text, thus privacy of user IDP account could compromised, the rough SPs can now use those credentials and impersonate the user.

- Prerequisites: Suppose SPs (Service. Providers) Collude with IDP (Identity.Provider) to link user (User) pseudonyms (Pseudonyms) and taking note of user behaviors. Therefore, the colluding (Service.Provider OR identity.Provider) can possible sell it to third party for advertising purposes or sell to hackers to get financial benefits. Additionally we assume that there is no Privacy Enhancing Technology (PET) deployed.
- The Attacker: Colluding/ Malicious/ Suspicious SP (Service. Provider) get access to user identifiers (User.Identifiers) or perform Profiling (Profiling) such individual SP (Service.Provider) maintain for instance telephone numbers and credit card numbers.
- User (User) belonging to xyz (xyz. Bank) customer, where xyz Bank is in federation with Telecom abc (abc. Malaysia) and Air pqr (Air. pqr)
- User (User) request for Air pqr (Air.pqr) service, who xyz (xyz.Bank) customer so only (xyz.Bank) have user authentication data that stored in (xyz.Bank.Database). Therefore, user (User) redirected to **xyz**.Bank (xyz.Bank) Login page.
- After User (User) enter his/ her (Username/Password) and if successfully login the User (User) identification/ authentication assertion is forward to Air pqr (Air.pqr) as they are in federation so it should trust the authentication assertion and response with Air pqr service (Air.pqr)**.** The same customer move to Telecom abc Malaysia (abc.Malaysia) and Paid (Paid) his landline or mobile Billing (Billing) using xyz Credit/ Debit card (xyz.Bank.Credit/Debit.Card)
- We assume that Air pqr (Air.pqr) and Telecom abc Malaysia (abc.Malaysia) holds xyz Bank (xyz.Bank) customer (User) credit card/ debit card numbers (Credit/Debit.Card), mobile number (Mobile. No.) and may use these for advertising or other purposes.

C. Scenario 3: No Platform Trust

In this attack, adversary uses the known weaknesses of the user platform to install Trojan horse, activate worms, and run remote key loggers to get control of the user system. We present an attack scenario where the user (User) is very much concerned about the dynamic updating of antivirus (Antivirus), application (Application), and operating system (Os) on his/her system platform.

- Prerequisites: Suppose an adversary (Adversary) that access to the Hospital record system (Hospital), to fetch patient, doctor's etc. records. Additionally we assume that the Hospital (Hospital) system is not protected with updated antivirus (Antivirus), anti phishing (Phishing), anti worm's application (Application).
- The Attacker: Assuming that adversary is (Adversary) able to successfully access the Hospital (Hospital) system and installed key logger or Trojan horse due to the lacking of a platform trust integrity measurement in a conventional systems.

IV. DISCUSSION

In this paper, we discussed user identity theft and information gathering in open environment. These problems appear in lacking of strong authentication protocols, involvement of the third parties and no platform trust. Therefore, new mechanisms are required to fill the existing gap between (user identification) security, (UIG) privacy and (platform) trust. Interested readers should refer to the pervious work in [15]. In Kerberos issues [8] related to the open network access such as the ticket lifetime, trust in third Parties, and the software integrity running on the workstation.

In federated identity management system, federated identity thefts evaluations and detection have a high risk, so

endpoints identity validation become an important point of action. John [16] gives design techniques such as deployment of reciprocal PKI, identities encapsulation, identity abuse detection, that can help to minimize endpoint-spoofing attacks (hijacking, DNS-attacks etc.).

The method proposed in [17], introduce identity Token concept in multi-domain service environment to bridge the user authentication/ authorization and privacy. The idea on which it is working, not to provide private information relating to user real identity or contractual information to a domain he/ she dose not trust. The contradiction between security, privacy and trust always exists in digital world. The security and privacy overlapping presented in [18], which means they do not flawlessly equivalent. It is against the hypothetical concept that security should protect privacy. However, security involves protection of physical and virtual realms, while privacy to protect personal information. So, normally electronic sensitive information protected by security, and security measures do not protect personal information. Fig. 1 below shows security, privacy and trust relationship

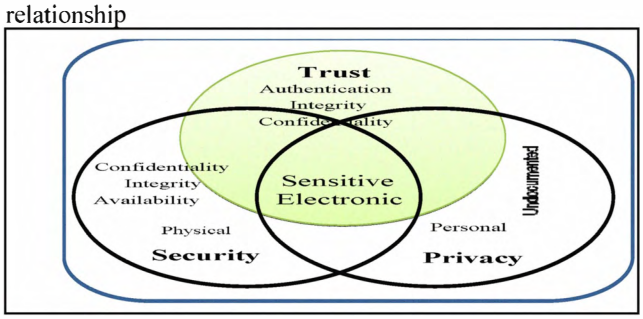

Figure 1. Security, privacy & trust relationship

In addition, as mentioned in [19], information security concerns with the confidentiality: guarantee information share only among authorized person or organization; integrity: guarantee information is consistent and complete, and availability: guarantee systems responsible for delivering.

In [20] the author explored trust models and metrics for public key infrastructure (PKI) systems that tackle authentication between sender and receiver, message integrity, and data confidentiality. All of these are security model feature, which means security and trust are in relationship. Trust is an important factor that can increase the subject confidence and usefulness of the system.

V. USER REQUIREMENT MODEL

The literature reviewed in this paper shows the conventional user platform (system) always in continuous threats. Therefore, the platform security, usability, and protection of user privacy requirements are also changing due to new trends of threats. In this Section, we proposed the user requirement model in Fig. 2 to combat these threats.

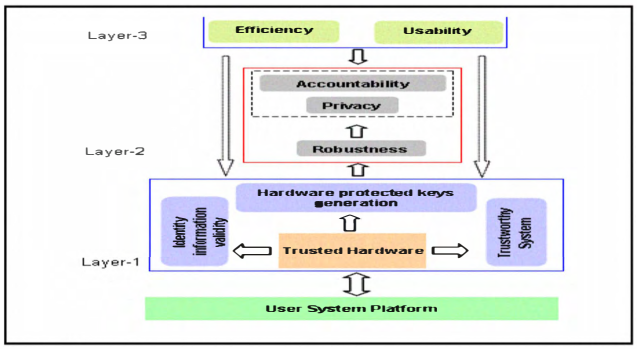

Figure 2. User requirement model (URM)

The Trusted Hardware [14] 'Trusted Platform Module' contain (EK) endorsement key that is 2049-bit RSA key pair (pub and pvt key). The private part always remains in chip where the public key used for attestation and data encryption. In addition it preserves platform privacy via proof of zero knowledge (in DAA scheme); authenticity (security) via platform authentication and platform integrity via platform attestation to check the integrity of the running applications and platform. The three layers in Fig. 2 are described below.

A. *Layer – 1*

- Trustworthy system: In conventional distributed environment, trust is always on the server side. What about the client's platform, applications and operating system that affected from virus, worms, phishing, malicious party or suspicious code attacks? The current mechanisms are lacking to verify remote applications, platform, and software's, integrity measurement.
- Hardware protected key generation and storing: Trusted computing cryptographic chip that generate aliases of key pairs, provide protected storage location, strong encryption and decryption facilities. Compared to the conventional key pair generation methods where the private or public keys can easily compromise to threats we already mentioned in Section IV.
- Identity information validity: The system should be intelligent enough to detect ID theft or suspicious code based on the trusted computing platform authentication mechanism or attestation to close the suspicious applications etc.

B. *Layer - 2*

- System Robustness: The authentication protocols should be robust, even if the user strong identifiers, credentials are compromise to some attacks such man in middle, Trojan horse, and worms, and should have the feature/ mechanism to stop the adversary to impersonate the victim, such as presence of mutual authentication protocols.
- Privacy: The underline authentication mechanism or technology should conserve user or platform privacy, and must have the facility to auto enforce when requiring identifiers on "need to know principle".

- Accountability: The system must ensure users actions and behaviors are accountable, but must anonymous and unlinkable to respect the user identity and identity information. The accountability must not harm user privacy.

C. Layer - 3

- Usability: It means the integrated security mechanisms must not overload the end user with computational expensive operations, involvement in complex authentication operations, or lengthy than the conventional federated identity management systems.
- Efficiency: Must make sure the authentication mechanism is efficient, must reduce the message round trip between the service provider and the user.

VI. CONCLUSIONS

In this paper, we proposed a user requirement model based on trusted hardware functionalities discussed in [15], we present scenarios related to identity theft, unlawful information gathering and tracking. We show the main issue of lack of platform trust in platforms involve in federated systems and discussed the consequences of respective threats on them. This research also creates new direction; the detailed threat model [15] analysis using threat-modeling techniques could help the federated application developers in flawless coding. In our future work, we come up with a model that full fill some of the user requirements described in the proposed model in this paper.

ACKNOWLEDGMENT

This work funded by Universiti Teknologi PETRONAS Postgraduate Assistantship Scheme and MIMOS Berhad, Malaysia

REFERENCES

[1] S. S. Shim, G. Bhalla and V. Pendyala, "Federated identity management," Computer, vol. 38, no.12, Dec. 2005, pp. 120-122.

[2] R. G. Brody, E. Mulig, V. Kimball, "Phishing, pharming and identity theft," Journal of Accounting & Financial Studies, vol. 11, no. 3, 2007.

[3] A. R. Gonzales, D. P, Majoras, Combating Identity Theft: A Strategic Plan, Office of the President: U.S. Department of Justice, 2007.

[4] D. Jevans, "Microsoft Live ID Phishing illustrates the dangerous of Federated Identity," Privacy and Identity Theft, 2009.

[5] D. Wood, Personal Information: Data Breaches Are Frequent But Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown, Washington, D.C.: U.S. Government Accountability Office, 2007.

[6] E. Mills, "Report: ID fraud malware infecting PCs at increasing rates," Security, 2009. http://news.cnet.com/8301-1009_3-10193025-83.html?tag=mncol;title

[7] M. F. Grubb, R. Carter, "Single sign-on and the system administrator," Proc. Twelfth Systems Administration Conference, 1998, pp. 63-86.

[8] J. G. Steiner, B. C. Neuman, J. Schiller, "Kerberos: An authentication service for open network systems," Proc. Winter Usenix Conference, 1988, pp. 191-201.

[9] S. M. Bellovin, and M. Merritt, "Limitations of the kerberos authenication system,".ACM SIGCOMM. Computer Communication Review, ACM Press, vol. 20, no. 5, 1990, pp.:119-132.

[10] Liberty Alliance, Liberty Authentication Context Specification. vol.1.2 - 05, 2003. http://xml.coverpages.org/liberty-architecture-authentication-context-v10.pdf

[11] B. Pfitzmann and M. Waidner, "Analysis of Liberty Single-Sign-on with Enabled Clients," IEEE Internet Computing, IEEE Press, 2003, pp. 38-44.

[12] D. Andert, R. Wakefield, and J. Weise, Trust Modeling for Security Architecture, sun blue prints, 2002.

[13] ITU-T Recommendation X.509| ISO/IEC 9594-8: "Information Technology – Open Systems Interaction- The Directory: Public-Key and Attribute Certificate Framework" 4th ed, 2001.

[14] Trusted Computing Group.http://www.trustedcomputinggroup.org

[15] Z. A. Khattak, S. Sulaiman, and J.Ab-Manan, "A study on threat model for federated identities in federated identity management system," Proc. IEEE 4th International Symposium on Information Technology, 2010, vol. 2, pp. 618-623.

[16] J. C. Checco, Federated Identity Theft, 2006. http://www.checcoservices.com/publications/2006_Federated_Identity_Theft.pdf

[17] D. J. Lutz, R. del. Campo, "Bridging the Gap between privacy and security in Multi-domain federations with identity tokens," in Mobile and Ubiquitous Systems: Networking and Service, pp. 1-3, 2006.

[18] A. Anderson, "Effective management of information security and privacy," Journal of Educause Quarterly, vol. 29, pp. 15-20, 2006.

[19] A. J. A. Wang, "Information security models and metrics," Proc. 43rd ACM Southeast Conference, vol. 2, 2005, pp. 178- 184.

[20] L. J. Hoffman, K. L.-Jenkins, and J. Blum, "Trust beyond security: an expanded trust model," Communications of the ACM, vol. 49, no. 7, 2006, pp. 95-212.