

Evaluation of Unified Security, Trust and Privacy Framework (UnifiedSTPF) for Federated Identity and Access Management (FIAM) Mode

Zubair Ahmad Khattak
Dept. of Comp. & Info. Sci.'s,
Uni. Teknologi PETRONAS,
31750 Tronoh, Perak, Malaysia

Suziah Sulaiman
Dept. of Comp. & Info. Sci.'s,
Uni. Teknologi PETRONAS,
31750 Tronoh, Perak, Malaysia

Jamalul-Lail Ab. Manan
Adv. Anal. & Modeling Cluster,
MIMOS Berhad,
57000 Kuala Lumpur, Malaysia

ABSTRACT

Federated identity and access management systems such as Shibboleth may symbolize a boost: (i) to bring the efficiency and effectiveness in collaboration for governments, enterprises and academia, and (iii) conserve the home domain user's identity privacy in a privacy-enhanced fashion. However, the consternation is about the absence of a trusted computing based mutual trust and security establishment in the Shibboleth infrastructure. The Trusted Computing based mutual attestation notion may assist to add-on the mutual trust and security but raises bidirectional platform privacy concerns. Therefore, to enjoy effectively the federated identity and resource (service) access by the home and foreign domain organizations it is necessary to provide an access control that may coalesced at least some security, trust and privacy aspects in a cohesive fashion. The objective of the work appearing in this paper is to provide a viable and feasible unified security, trust and privacy framework access control solution for federated identity and access management systems by fusing the Shibboleth authentication and authorization access control with the trusted computing based trustworthy mutual attestation.

General Terms

Attestation, Identity and Access Management, Privacy, Security and Protection, Trust

Keywords

Access Control, Anonymity and Pseudonymity, Federated Identity & Access Management, Mutual Attestation, Security, Trust, Trusted Computing, Trusted Platform Module

1. INTRODUCTION

Federated Identity and Access Management (FIAM) systems enable organizations to share their users' Authentication (AuthN) and Authorization (AuthR) information among themselves for the purpose of the user's legitimacy and resource (service) access in a distributed mode. The federated identity sharing and resource (service) access in Shibboleth may symbolize a boost: (i) to bring efficiency and effectiveness into electronic business operations and collaboration for governments, enterprises and academia, and (ii) provide the users' identity privacy conservation to the Home Domain (HD) organization at the Foreign Domain (FD) organization.

Government, enterprises and academic institutions such as the eSchool initiative, an element of the e-Government effort in Greece [1], Nuxeo's integrated document management tool in Shibboleth [2], and SAGE Journals established country level

federation [3], respectively. All these organizations use FIAM systems for sharing their users' AuthN and AuthR information among their partners for resource (service) collaboration.

The heart of a FIAM system is the "federation" establishment. The federation is established when different organizations come together and agree on common rules. The notion of the federation assists the participating groups in the organizations to establish trust among themselves to collaborate safely in the identity federation and resource (service) access operation. The federation also allows the HD users to be authenticated only once with the HD and then they can use the resource (services) of the FD organization members of the federation exclusive of repeating the AuthN process.

However, there is consternation about the absence of the trusted computing based mutual trust and security establishment in the Shibboleth infrastructure. Therefore, on one hand, Shibboleth brings the advantages of the identity and resource (service) availability to every organization in the federation; on the other hand, it raises concerns about the HD client and Identity Provider (IdP) machine platform's state (i.e., infected with any malevolent attack such as malware, Trojans, virus).

The Trusted Computing Group (TCG) [4] describes trust as "Trust signifies anticipation which shows a machine's or device's behavior that: (i) It will always act in a particular way and (ii) For a precise intention" [5]. This is further elucidated by Alam et al. [6] as follows: (i) Particular way concerns "How a job is anticipated to be carried out?" and (ii) Precise intention regards a specific job or scenario. To realize trust in a machine platform, the TCG introduced the notions of "Remote Attestation" and "Trusted Platform Module (TPM)" [7].

However, the Trusted Computing tamper-resistant based mutual attestation notion may assist to add-on the mutual trust and security, but, conversely, it may raise machine platform privacy worries. Therefore, to effectively utilize the identity and resource (service) collaboration by the HD and FD organizations in a federation it is necessary to construct a cohesive STP access control solution.

The aim of this paper is to construct a feasible cohesive STP framework using Trusted Computing potencies for the FIAM setting. The main idea is to show that the Trusted Computing and Shibboleth [8, 9] standards may be used by the HD and FD organizations to construct a practicable unified STP access control scheme for the federated environment.

The main contributions in this paper are as follows:

- It constructed a feasible cohesive STP framework for the federated environment. The STP unification is carried out as follows: (i) Merged HD user AuthN (i.e., username/password) with the HD IdP and client platform bidirectional attestation, (ii) Bidirectional trust and security formation among the HD IdP and client machine, and (iii) Mutually attested HD client and IdP platform measurement safeguarding.
- It extended the remote attestation to a mutual attestation for federated scenarios.
- The framework viability was validated by a test-bed prototype using the standard FIAM and TCG solutions.
- A new MODULE-DATACONNECTOR (DC), such as the MUTUALPLATFORMINTEGRITY (MPI), Provider was created and added to the HD Shibboleth IdP. This entity performs the HD IdP and client bidirectional attestation only if the HD user is successfully authenticated using his/her basic credentials.
- The resource or service access AuthR decision at the FD was linked to the HD IdP's and client's successful bidirectional attestation.

The remainder of the paper is arranged as follows. Section 2 presents the background. Section 3 presents the related works. Section 4 illustrates the motivational scenario. Section 5 discusses the problem. Section 6 explains the framework architecture. Section 7 discusses the result analysis. Section 8 concludes the paper with the future works.

2. BACKGROUND

2.1 Federated Identity and Access Management

To overcome the credential (UN/PWD) management issues for web services, the WSSO FIAM solutions have been proposed. Shibboleth is one of them and is a key WSSO FIAM system.

2.1.1 Shibboleth

Shibboleth is an open source WSSO FIAM software package. Shibboleth is based on the standard SAML protocol. This means Shibboleth uses the SAML for AuthN assertion and attribute exchange. The "Internet2" is a recognized body working on the identity federation with Shibboleth. The aim of the Internet2 is used to construct the federation of the identity for academic institutions and their partners. The entities in Shibboleth are as follows:

- The HD user is a resource (service) consumer.
- The HD IdP architecture is drawn from the SAML. The HD IdP entity is responsible to accept the AuthN and AuthR challenges from the FD Service Provider (SP) entity to authenticate the HD user and to assert the authenticated user assertion and attributes. The latter may be used by the FD SP in the AuthR operation.
- The "mod_shib" at the FD SP is an Apache web server "plug-in" and enables access regulation to a protected resource or service. This module also makes the AuthR decision on the basis of user attributes. In addition to that, the Shibboleth SP also consists of a daemon "shibd" and Apache module "httpd" which listens to AuthR requests from a web server.
- The SP, when it receives a resource request, redirects the user to the IdP to select the trusted IdP through the

Discovery Service (DS). The DS consists of a "Pool of IdPs" that belongs to the federation.

2.1.2 How Shibboleth Works

A typical resource sharing scenario in a Shibboleth system is such that: an HD user requests a resource or service sited at the FD SP. If the requested resource is a protected one, then the client is redirected to the DS by the FD SP. The DS prompts the HD user with a pool of registered HD IdP machines to select the respective HD IdP machine. Upon selecting a particular HD IdP machine, the DS redirects the HD user to his/her selected HD IdP machine for the AuthN process.

The HD IdP can use any AuthN mechanism (e.g., username/password, biometrics, smartcards etc.). In the proposed architecture, the UN/PWD based AuthN mechanism has been used. Continuing the scenario, the HD IdP presents a login screen for the HD user to enter his/her UN/PWD pair. If the HD user is successfully authenticated using the information provided, a specific session is created for that HD user by the HD IdP. Subsequently, the HD IdP also creates a handle (i.e., AuthN token) and sends this handle to the HD user's browser. Afterwards, the HD user is redirected to the specific FD SP machine and the HD user's browser presents its handle to the FD SP. This handle is then used by the FD SP in order to request the HD user's specific attributes from the HD IdP. The process through which the FD SP machine sends the attribute request and the session handle to the HD IdP machine to request the HD user's attributes is known as the Attribute Lookup.

At the HD IdP end, a special module known as the Attribute Resolver is used to search for the HD user's attributes requested by the FD SP machine. The Attribute Resolver first searches for the particular attributes, then verifies whether the HD user's privacy policy residing at the HD IdP authorizes the release of the requested attributes to that particular FD SP. The privacy policy is known as the Attribute Release Policy (ARP). If the privacy policy allows the release of these attributes only then will the HD IdP machine release the attributes to the FD SP machine. At the FD SP machine end, the attributes received are mapped to different variables and can be used by different applications at the FD SP. These attributes are then used in the access decision making process (i.e., to grant or deny access).

2.2 Trusted Computing

The initiative was taken by the Trusted Computing Group (TCG), previously known as Trusted Computing Platform Alliance (TCPA) [10, 11], to bring in hardware based security and trust solutions (e.g., TPM) for devices) in desktop, server and mobile platforms.

2.2.1 Trusted Platform Module

The TPM is a small coprocessor chip that can perform mixed security functionalities such as private key protection, Random Number Generator (RNG), and Platform Configuration Registers (PCRs). In addition to that, the TPM has some necessary components which are used in the "Remote Mutual Attestation". These components include the Endorsement Key (EK) which is a manufacturer built-in key and uniquely locates a particular platform. However, making use of the EK for data signing raises privacy concerns. Therefore, the Attestation Identity Key (AIK) and a pseudonym key are generated and used for signing the data.

The TPM PCRs are used to prove the state of a target platform configuration to the validator (i.e., challenger). Each PCR is

competent to stock a broad-range of units, for instance BIOS, Boot-Loader, Kernel and Application measurements. The measurements of the units are stored in “Cryptographic Hashes” formed by applying an SHA-1 algorithm [12]. The manipulation of a PCR may be performed through the PCR_Extend as follows: (i) First, the Value, which needs to be amassed in a selected PCR, is its Hash added with a current PCR Value and (ii) Second, the resulting structure SHA-1 is stocked rear into an identical PCR.

2.2.2 Mutual (Bi-directional) Attestation

To perform the attestation of a computing device platform (i.e., the hardware’s and software’s) electronically, the Trusted Computing provides a remote attestation concept. The remote attestation technique affirms to the challenger that the target machine platform contains a genuine TPM and its platform integrity is secured or in a trustworthy state. The objective of the remote attestation technique is to let the remote machine (i.e., the challenger) determines the “degree of trust” of the target machine platform on the basis of the target machine’s platform integrity health.

The TCG introduced the first remote attestation protocol. However, the limitation in the TCG’s technique is that this method is restricted to gauging only the Software loaded earlier than the Operating system (Os), for example BIOS, Boot-Loader etc. To overcome the TCG’s limitation, Sailer et al. [13] initiated a remote attestation technique based on the Integrity Measurement Architecture (IMA). The IMA exploits the Loaded-time Measurement technique to verify the platform integrity of a remote device. The IMA was the first method to expand the “TCG method” inside the Os by gauging all the Libraries and Executables using the SHA-1 loaded through and later than the LINUX Os’s Boot process. However, the limitation in all remote attestation schemes is that they cannot perform the mutual attestation of both communicating machine platforms (e.g., client and server) in a FIAM system.

In this paper, the authors extended the IMA based remote attestation technique to the mutual attestation technique for the federated environment. The extended technique will establish bi-directional trust among the HD IdP’s and the client’s platforms. To form the bi-directional trust, the authors configured a Linux kernel with the IMA for the HD client’s and IdP’s machines. The advantage of this is that the Linux Kernel sustains a measurement list at the StoredMeasurementLog (SML) in a Securityfs of the Linux system that symbolizes the History of the burdened procedures and the libraries. Every burdened file is managed by obtaining the SHA-1. One of its parts is appended to the Measurement List whereas the second part is aggregated into the TPM PCR (e.g., PCR-10). In response to an attestation request triggered from a HD IdP, the SML entries and the TPM-QUOTE of an attested machine (i.e., client and IdP) is reported to the validator (i.e., IdP). The validator then validates the client and IdP platforms’ reported SML and TPM_QUOTE to establish a trust decision.

3. RELATED WORK

Trust in existing FIAM modes are achieved in different styles. The Liberty Alliance (LA) [14] defines a Circle of Trust (CoT) to which the FD SPs and HD IdPs adhere by signing a business agreement in order to support secure transactions among the CoT members [15]. In an OpenID, the trust association like CoT is missing [16] and moves trust from the application level to a social level [17]; so in the OpenID, in order to trust a person, the OpenID provider must verify that

the person is really the one who he/she claims to be. Whereas, in Shibboleth: (i) the SP trusts the IdP user AuthN and AuthR data and (ii) the user trusts the IdP that it will authenticate the user securely. The idea behind the Shibboleth design is to ease the formation of federations and collaborations between the participating organizations. The advantage of the Shibboleth over other FIAM modes is the privacy conservation at the FD SPs [18].

Lutz and Campo introduced the identity token (IDToken) concept in Multi-domain-Federations (MdfFs) to bridge the gap between security and privacy in order to solve the security and privacy problem in the MdfFs. Therefore, whenever users wish to use the token, each time it will [19]: (1) Increment the serial number and (2) Generate a new random number. It uses the pseudonymity technique to conserve the user’s privacy in the MdfFs. This will ensure that no private information will be kept at the FD.

Oey and Weis proposed a privacy enhanced scheme for the OpenID federated login scheme. The concern is that the HD IdPs may possibly link the user’s identity and track their visits across multiple sites [20]. The authors solved the privacy problem in the OpenID federated login scheme through a blind signature [21] scheme. The scheme allows the user to be anonymous and his/her transactions unlinkable via pseudonymity and unlinkability.

To overcome the security concerns in the machine platforms, the TCG introduced a hardware based security solution. Watanabe and Tanaka proposed a federated AuthN scheme using a cellular phone [22]. Their scheme improves ID assurance and a secure AuthN in an OpenID. The authors solved the security and privacy problems in the current OpenID scheme.

A trustworthy AuthN scheme was introduced in [23, 24]: (1) It was designed on the OpenID concept and (2) It made use of a remote attestation technique to measure, report and validate the integrity of a target machine. However, the OpenID concept was different than in other IAM systems. The OpenID IdPs issue “global identifiers” to their users through which the users then login to any SP. However, the problem of using a “global identifier” is that it does not support anonymity and unlinkability [25].

Ali et al. provided the trustworthy approach for the federated identity management system. The authors integrated a remote attestation technique in Shibboleth to strengthen the client machine security [26]. However, in the federated environment, a dishonest HD IdP machine may raise serious security concerns because: (1) The Home Domain IdP is always present online, (2) It performs the HD user AuthN and (3) It affirms the HD user AuthN and AuthR (i.e., attributes) assertion to the FD SP. Therefore, in such a case, it is not wise to leave the HD IdP machine open to the invaders.

To bring the STP in a single framework, Khattak et al. initiated a step to build a practicable Unified Security, Trust and Privacy Framework (UnifiedSTPF) for the federated environment. For this, the authors exemplified the STP threats in the federated environment by a threat model. The initiated threat model covers [27]: (1) Weak AuthN, (2) Absence of mutual trust formation among the HD clients and the IdP machines’ platforms and (3) The Home Domain clients and IdP machines’ platform privacy-conservation in the mutual attestation protocol at the FD SPs. On the basis of specified threats, two different frameworks are identified: (1) the

Emergent STPF which does not include a TTP [28, 29] and (2) the Practicable UnifiedSTPF which includes a TTP [30].

4. MOTIVATION SCENARIO

To reveal the STP unification challenge in a federated setting consider a federated research collaboration scenario which consists of two organizations: (i) The Department of Defense (DoD) and (ii) The Department of Research (DoR). The DoD and DoR organizations are also known as the HD and FD, respectively. This scenario is based on assumptions such as: (1) The DoD and DoR are managed autonomously, (2) The HD is responsible for user registration, AuthN and attributes assertions, and (3) They possess privacy conserving related policies. The HD consists of an entity called the IdP which is responsible for performing the user AuthN and AuthR attribute assertion. The FD may be a resource provider organization.

Deem the user to be in a weak trust association with the FD in a federated environment and he/she is about to expose his/her private information and revealing this private information to the FD may lead to privacy concerns. For this, the authors assumed that all of the user's private information is stored in the HD which is trusted strongly by the user.

However, the STP concerns in the federated scenario are as follows: (1) A weak AuthN mechanism instead of an integrated AuthN such as UN/PWD with the HD IdP and client machine platforms' mutual attestation, (2) The absence of mutual platform attestation among the HD IdP and the client machines' platforms, (3) The absence of the TC technology based bi-directional trust and security in the federated setting, (4) The resource AuthR decision in the FD is not linked to the HD IdP and client machine platforms' successful mutual attestation outcome (i.e., Trusted Attribute) or (5) The mutually attested machines' platform security credential privacy conservation; releasing of the machines' platform security credentials raises platform privacy concerns.

5. PROBLEM

The mutual trust, security and privacy anxieties in a FIAM system and TC remote attestation are as follows:

5.1 Mutual Trust and Security Concerns

The mutual trust, security and privacy anxieties in the FIAM:

5.1.1 Deceitful Home Domain IdP

In the FIAM, the HD IdP is always available online to authenticate the HD user and to pass on the HD user AuthN and AuthR information (e.g., attributes) to the FD SPs. However, in a worst case scenario, it may be possible for the HD IdP machine to be tampered with by a malevolent program such as Trojans and Rootkit programs. Therefore, such an infected HD IdP machine behaves malevolently which may lead to HD user credential theft and the attacker may misuse the credentials to access sensitive resources.

5.1.2 Deceitful Home Domain Client

The FD SP redirects the HD user to the HD IdP whenever he/she requests a protected resource or service at the FD SP. However, the HD IdP and FD SP do not have beforehand knowledge about an HD client machine's platform integrity (i.e., trusted or not). Therefore, such un-trusted HD user machine may lead to the HD user credential theft.

5.1.3 Resource/Service Access Concern

The resource or service access in the FD SP is not on the basis of the HD IdP and client machine platforms' mutual attestation. Therefore, the absence of "mutual trust" in the

machine platforms generates anxiety such as to whether both of the HD machines' platforms are in a trusted state or not.

5.2 Remote Attestation Shortcomings

The shortcomings of the trusted computing "Remote Attestation" scheme are as follows:

5.2.1 To Perform Bidirectional Attestation

The traditional trusted computing remote attestation scheme cannot perform the machine platform mutual attestation in a federated scenario. Therefore, an extension is required in the "remote attestation" in order to perform the machine platform mutual attestation.

5.2.2 Privacy Concern

However, extension to the remote attestation will introduce machine platform security credential privacy concerns in the mutual attestation scheme.

6. FRAMEWORK ARCHITECTURE

The main entities included in the proposed practicable cohesive STP architecture are the FD SP and HD IdP organizations. In the cohesive STP architecture, the HD organization is the core organization for major configurations such as the establishment of mutual attestation and the integration of mutual attestation with the user basic AuthN mechanism (e.g., UN/PWD).

6.1 Home Domain Modification

The HD organization consists of IdP and client machines. The modifications that the authors have made are as follows:

6.1.1 Home Domain Pre-requisites

The major nuts and bolts for the HD client's and IdP's machines are given below, which were carried out only once in the entire development phase:

- The HD IdP and client machines' TPMs have to be enabled, activated and owned by the HD user and/or by the HD administrator.
- Both the HD client and the IdP machine platforms require a particular "Attestation Identity Key (AIK)". The AIKs are created later than the TPM ownership.
- The newly generated AIKs then have to enroll with a TTP such as a PrivacyCA according to the TCG specification [5]. The enrolling process with the TTP helps to accomplish the TPM authenticity. This may be achieved by setting-up a personal PrivacyCA and enrolling the newly generated AIKs.
- In turn, to employ the AIKs in a mutual attestation scenario, the secret values of the AIKs have to be available to the Attestation_Presenter-Daemon called the Attestation Collector(AC)-Daemon running on both of the HD client's and IdP's machines.

6.1.2 HD IdP to Accomplish Mutual Attestation

In the proposed architecture, the authors have chosen the HD IdP to perform the mutual attestation operation because of the following reasons:

- Both the client and the IdP are in a strong trust link with members of the internal network so it is not sensible from the HD machine platform privacy perspective that the HD IdP transport the HD IdP and client machine platforms' measurements to an external network entity such as the FD SP in our scenario.

- It is also not sensible from the privacy perspective for the HD IdP “big brother” to share its platform security credentials with the HD clients.
- Also, the FD SP is not feasible to carry out the mutual attestation because of the following reasons: (1) The FD SP has its own security procedures and authorization policies and (2) The weak trust link between the HD clients and FD SP because the FD SP is an external network for the HD users.
- Maintaining and checking the honesty of trusted hashes is a tedious operation in diverse networks. To overcome this issue in the proposed architecture, the authors make liable the HD IdP to carry out the internal network HD clients’ and its own (i.e., IdP) machine platform attestation. Therefore, in such cases, the HD IdP machine retains the imprints of the confined amount of the potential platform security credentials. This probably diminishes the intricacy issue because the HD organization potentially possesses less measurement space.

6.1.3 HD Client and IdP Machine Modification

To measure and report the HD organization’s machine platform integrity measurement, the following modifications were made to the HD client’s and IdP’s machines:

- At both the HD IdP’s and the client’s machines, to measure the executables loaded for execution at the boot-time and reporting it to the HD IdP machine, a JAVA based AC-Daemon was developed. The tasks to be performed by the daemon are as follows: (1) Listening for attestation requests from the Corroboration Service (CS) located at the HD IdP’s machine, (2) Requesting for the TPM to perform the TPMQUOTE operation, (3) Reading of the SML, and (4) Processing of the attestation request and response in SAML formats.
- A specialized entity such as the Corroboration Service (CS) located at the HD IdP’s machine was developed. This entity performs the HD IdP and client machine platform mutual attestation on behalf of the HD IdP machine. This entity also conserves the HD IdP’s and the client’s machines because it is located in the internal network.
- In the current Shibboleth IdP architecture, there is no mutual integrity resolver or data-connector. Therefore, the new MutualIntegrity-Resolver (MI-R) and the MutualIntegrityProvider-DataConnector (MIP-DC) were created for implementation by the authors. The MI-R communicates with the MIP-DC to populate the MutualPlatformIntegrity-Attribute (MPI-A). The MPI-A contains mutual platform attestation outcomes (e.g., “true”).
- To validate the attestation responses received from either the HD client’s or the IdP’s machines, the authors created the unlike AttestationValidation (AV)-Components such as follows: (1) the ValidationofReceived-Nonce (VR-N), (2) ValidationofReceived-PCR (VR-PCR), (3) ValidationofReceived-SML (VR-SML) and (4) ValidationofReceived-Certificate (VR-Certificate).

6.1.4 Complete Framework Architecture Protocol

The complete framework architecture protocol is as follows:

- The HD user, via a browser, requests a protected resource sited at the FD. The FD forwards the HD user to the Discovery Service (DS) to choose his/her HD IdP (list of several IdPs). So, after the selection of his/her HD IdP, the DS forwards the user’s agent to the selected HD IdP (Steps 1, 2, 3 & 4).
- The above step brings the HD user to a chosen HD IdP sign-in portal. The HD user then inputs his/her credentials (UN/PWD). The HD IdP next validates the user the input against the LDAP entries (Steps 5 & 6).
- If the outcome of the above step is positive, then the log-in handler’s facility at the HD IdP creates a session for this user and pushes a “handler” to the user’s agent. (Steps 7 & 8).
- The user’s agent pushes the “handler” to the module-mod_shibd present at the FD. This is the user’s successful AuthN proof (Step 9).
- The module-mod_shibd then pushes a query to the Shibboleth daemon-shibd part of the FD for attribute requests from the HD IdP (Step 10).
- The daemon-shibd pushes a request to the module-Attribute Resolver at the HD IdP to provide the HD IdP and client mutual attestation attributes (Step 11).
- The Attribute Resolver then contacts the new MIP-DC for the MPI-attribute (Step 12).
- The MIP-DC then pushes an Attestation Request (AR) to the CS to carry out the HD client’s attestation (Step 13).
- The Module-AttestationRequester (AReq.) at the CS (i.e., part of an HD IdP) creates a “NONCE” and an attestation request and pushes them to the AC-Daemon present at the HD-client (Step 14).
- The AC-Daemon then initiates the AttestClientPCR and AttestClientSML to assemble the PCR10 & SML from the HD-client’s TPM. The AC-Daemon then pushes the collection back to the Module-AReq. at the CS (Step 15-16).
- The CS then initiates the VR-PCR and VR-SML to confirm the HD client trustworthiness as follows the certificate legality with the PrivacyCA; it validates the SML-hashes against Good-hashes in the Database, the PCR value and the VR-N against the sent nonce. (Step-17).
- The CS merges the results and encodes them as an XML node and then returns it to the MIP-DC at the HD IdP (Step 18).
- However, if the outcome of the above step is “false”, it means that the HD client’s platform is not trustworthy; then, the HD IdP attestation will not be performed and (Steps 20-25) will not be carried out (Step 19). If the outcome is “true”, it means the HD client’s platform is trustworthy; then, the MIP-DC pushes an attestation inquiry to the CS to mutually validate the HD IdP’s platform integrity (Step-20). The HD IdP’s attestation will be performed similarly as the client’s in Steps14-20.

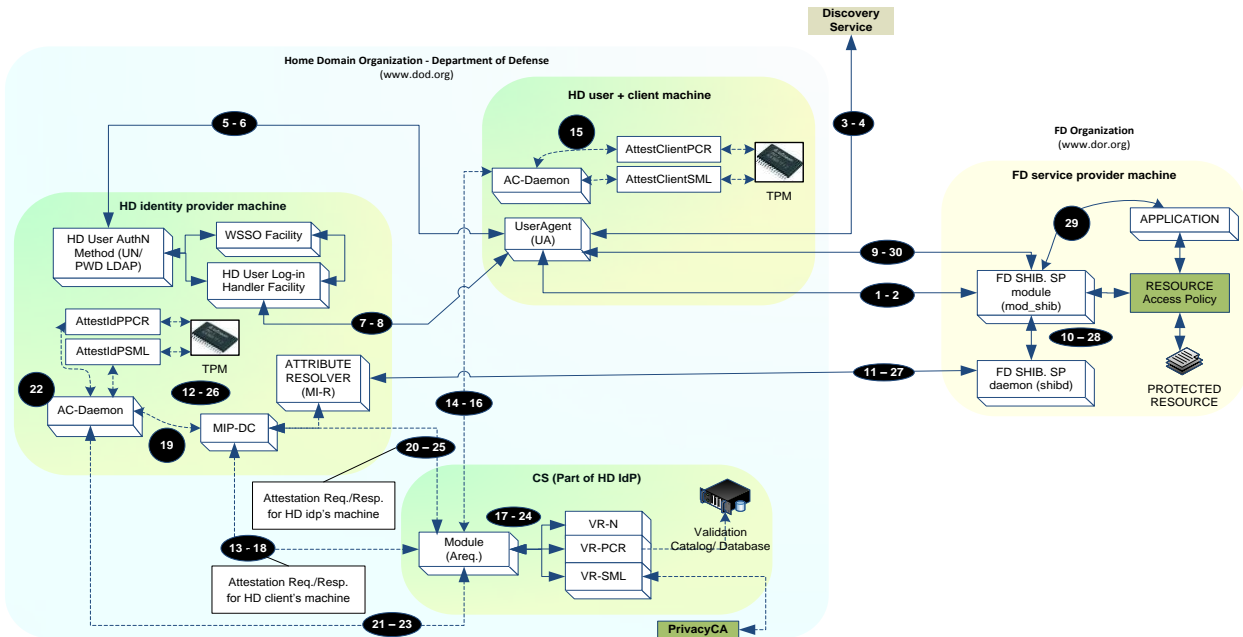


Fig 1: Unified security, trust and privacy framework (Unifiedstpf) architecture

- The MIP-DC gathers the outcome of the mutual attestation and forwards the outcome to the Attribute Resolver at the HD IdP (Step 26).
- For the HD organization’s mutual attestation, the MI-R populates the MPI-attribute with the outcome of the mutual attestation and pushes the attribute to the Shibboleth daemon-shibd in the operation at the FD (Step 27).
- The daemon-shibd then passes it to the FD Shibboleth module-mod_shibd. This module applies its policies and checks the values of the acquired attributes against its policies (Step 28).
- The module-mod_shibd then applies the organizational policies to the attribute values (e.g., false or true). This module then communicates with the application which is shielding the critical resource either to let or refuse the release of the resource on the basis of the HD machine’s mutual attestation result (Steps 29-30).

6.2 Foreign Domain Modification

The FD SPs protect critical resources (services) by enforcing organizational level policies. Therefore, at the FD, the changes made to the SP are limited to the SP application side and the SP central modules are not customized. In the proposed implementation, the web server is responsible for enforcing these policies and making decisions such as to allow or deny. Therefore, the FD releases the resource only after checking that the HD client and IdP machines’ mutual attestation is successful (i.e., true).

7. RESULTS AND ANALYSIS

The results and analysis are as follow:

7.1 Mutual Attestation Performance

Figure 2 shows the “round trip” mutual attestation time for the HD IdP and client platforms. This includes sending and receiving the attestation request and response, validation of the Nonce, SML, PCR and Certificate. The graph data is

obtained by merging the HD client and HD IdP machine platforms’ attestations. The No. of measurements’ and attestation time’s association shows that when the “No. of Measurements” in the SML increases, then the attestation time also increases. This is equally true for the “Round-trip Att. time (in ms) plus the Network overhead” as given in Figure 2.

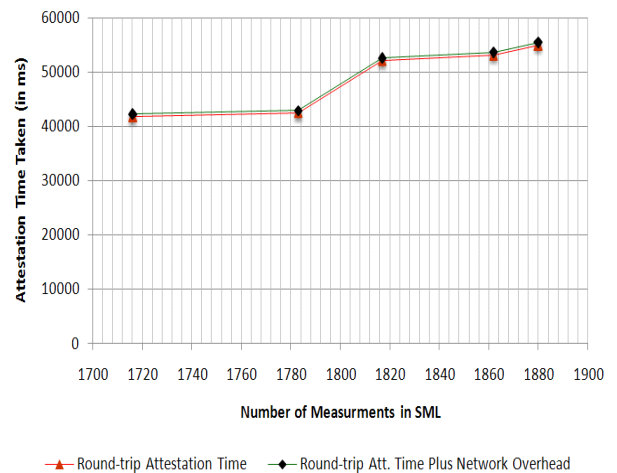


Fig 2: HD machines attestation roundtrip-Attestation-time + network overhead

7.2 Security and Trustworthiness Test

7.2.1 Insecure and Untrustworthy Client Platform

In this scenario, the HD client’s platform integrity breakdown demonstrates an unknown “hash:eog” found which shows that the signature of the original “eog” is already altered. The alteration indicates that a malevolent action has replaced the original “eog” with a malicious type as given in Figure 3. This scenario demonstrates that the client’s platform is not trustworthy or is already infected by a malevolent action.

```

1. 13:03:31.686 - DEBUG [VRPCR:140] - Unknown hash:eog-
C6B21365d43217e00543x5v3215h44398754sw10
2. 13:03:31.686 - INFO [tbed.pustpf.ima.net.avagent.Target:137] - ! ----- Unknown hash
is located. Validation is unsuccessful.
3. 13:03:31.686 - DEBUG [tbed.pustpf.ima.net.avagent.Target:156] - Time Taken (ms):1301
4. 13:03:31.687 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:71] -
Attestation acknowledgement reply about HD client's machine integrity from CS: false
5. 13:03:31.687 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:73] -
HD client's machine platform integrity is not validated, so HD IdP attestation is not carried out.
6. 13:03:31.687 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:97] -
Mutual attestation unsuccessful because of HD client or IdP machines platform integrity
validation breakdown
    
```

Fig 3: HD client platform attestation failure

7.2.2 Client Platform Not Configured with IMA

Figure 4 shows that when the attestation collector agent at the HD client is not running, it means that the client is not equipped with a TPM or configured for mutual integrity validation. Therefore, the CS then assumes that the HD client's integrity is false.

```

1. 12:57:12.884 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:47] -
Attributes construction begins.
2. 12:57:12.884 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:48] -
Generating Mutual integrity attribute: MutualPlatformIntegrity
3. 12:57:12.887 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:62] -
Calling CS for Mutual attestation of HD IdP at idp.dod.org and HD Client at 192.168.0.2
4. 12:57:12.887 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:64] -
Carrying out HD client's machine platform attestation at 192.168.0.2
5. 12:57:12.887 - DEBUG [tbed.pustpf.ima.net.avagent.Target:43] - Establishing connection to
HD target machine on port 4444
6. 12:57:12.889 - ERROR [tbed.pustpf.ima.net.avagent.Target:53] - Couldn't get I/O for the
connection to: 192.168.0.2
7. 12:57:12.890 - ERROR [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:69] -
ACDaemon couldn't be contacted. Assuming bad integrity.
8. 12:57:12.890 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:71] -
Attestation acknowledgement reply about HD client's machine integrity from CS: false
9. 12:57:12.890 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:73] -
HD client's machine platform integrity is not validated, so HD IdP attestation is not carried out
10. 12:57:12.891 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:97] -
Mutual attestation unsuccessful because of HD client or IdP machines platform integrity
validation breakdown
    
```

Fig 4: HD client not configured with IMA/no TPM

7.2.3 Insecure and Untrustworthy IdP Platform

In this scenario, the HD IdP's platform integrity failure demonstrates that an unknown "hash: idp.war" is detected. This shows that the signature of the "idp.war" has been changed as shown in Figure 5. This means a malicious action has replaced the original "idp.war". The unknown hash detection illustrates that the HD IdP's platform is no longer trustworthy or protected.

```

1. 13:10:18.682 - DEBUG [VRPCR:140] - Unknown hash:idp.war :
56c2346b3476877e374p83532041b2311s64210qa
2. 13:10:18.682 - INFO [tbed.pustpf.ima.net.avagent.Target:137] - ! ----- Unknown hash
is located. Validation is unsuccessful.
3. 13:10:18.683 - DEBUG [tbed.pustpf.ima.net.avagent.Target:156] - Time Taken (ms):12778
4. 13:10:18.683 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:86] -
Attestation acknowledgement reply about HD IdP's machine integrity from CS: false
5. 13:10:18.683 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:88] -
HD IdP's machine platform integrity is not validated.
6. 13:10:18.684 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:97] -
[Mutual attestation unsuccessful because of HD client or IdP machines platform integrity
validation breakdown
    
```

Fig 5: HD identity provider platform attestation failure

7.2.4 Secure and Trustworthy HD Client and IdP Platforms

Figure 6 shows the HD client and IdP platforms' successful mutual attestation. After the successful mutual attestation, the attribute is derived and transmitted to the FD SP for the access decision.

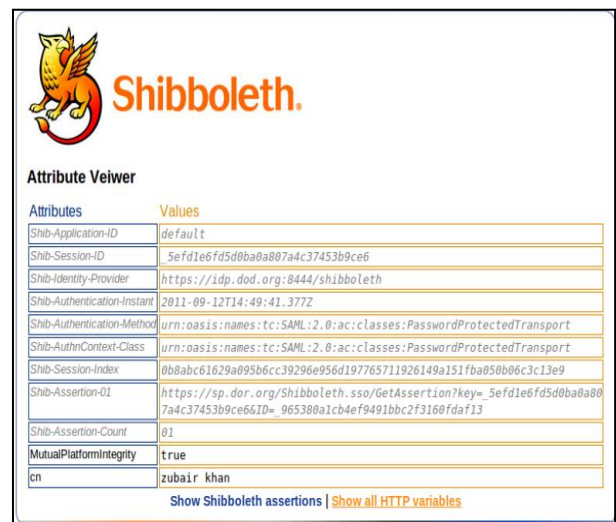
```

1. 14:59:52.791 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:48] -
Generating Mutual integrity attribute: MutualPlatformIntegrity
2. 14:59:52.794 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:62] -
Calling CS for Mutual attestation of HD IdP at idp.dod.org and HD Client at 192.168.0.2
3. 14:59:52.795 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:64] -
Carrying out HD client's machine platform attestation at 192.168.0.2
4. 14:59:52.795 - DEBUG [tbed.pustpf.ima.net.avagent.Target:43] - Establishing connection to
HD target machine on port 4444
5. -----
6. 15:00:21.165 - INFO [tbed.pustpf.ima.net.avagent.Target:147] - * ----- Validation of
SML is successful
7. 15:00:21.166 - DEBUG [tbed.pustpf.ima.net.avagent.Target:156] - Time Taken (ms):28371
8. 15:00:21.166 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:71] -
Attestation acknowledgement reply about HD client's machine integrity from CS: true
9. 15:00:21.166 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:80] -
Carried-out HD IdP's machine platform attestation at idp.dod.org
10. 15:00:21.167 - DEBUG [tbed.pustpf.ima.net.avagent.Target:43] - Establishing connection to
HD target machine on port 4444
11. -----
12. 15:00:45.025 - INFO [tbed.pustpf.ima.net.avagent.Target:147] - * ----- Validation of
SML is successful
13. 15:00:45.025 - DEBUG [tbed.pustpf.ima.net.avagent.Target:156] - Time Taken (ms):23858
14. 15:00:45.026 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:86] -
Attestation acknowledgement reply about HD IdP's machine integrity from CS: true
15. 15:00:45.026 - DEBUG [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:94] -
HD Mutual attestation resulted in "true".
16. 15:00:45.026 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:101] -
Mutual attestation attribute insertion: MutualPlatformIntegrity
17. 15:00:45.027 - INFO [tbed.pustpf.pustpsub.MutualIntegrityProviderDataConnector:103] -
Sending back the Mutual integrity attributes.
    
```

Fig 6: HD idp and client mutual attestation is successful

7.3 HD Platforms Privacy Conservation

Figure 7 shows the populated "MPI-attribute" with the successful mutual attestation result (i.e., true). The FD SP cannot guess what the HD IdP's and client's platform measurements are so the HD IdP and client machines' platform privacy is protected at the FD SP.



The screenshot shows the Shibboleth Attribute Veiver interface. It features a logo of a phoenix and the text "Shibboleth." and "Attribute Veiver". Below the logo is a table with two columns: "Attributes" and "Values".

Attributes	Values
Shib-Application-ID	default
Shib-Session-ID	5efd1e6fd5d0ba0807a4c37453b9ce6
Shib-Identity-Provider	https://idp.dod.org:8444/shibboleth
Shib-Authentication-Instant	2011-09-12T14:49:41.377Z
Shib-Authentication-Method	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-AuthnContext-Class	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Shib-Session-Index	0b8abc61629a95b6cc39296e956d19765711926149a151fa050b06c3c13e9
Shib-Assertion-01	https://sp.dor.org/Shibboleth.sso/GetAssertion?key=_5efd1e6fd5d0ba0807a4c37453b9ce6&ID=965380a1cb4ef9491bbc2f3160fda13
Shib-Assertion-Count	01
MutualPlatformIntegrity	true
cn	zubair.khan

At the bottom of the interface, there is a link that says "Show Shibboleth assertions" and "Show all HTTP variables".

Fig 7: HD platform privacy conservation via MPI

8. CONCLUSION AND FUTURE WORK

This paper provided a viable and cohesive STP framework for FIAM systems. The STP framework combined the potencies of standard technologies such as Trusted Computing based mutual attestation, SAML Inter-domain AuthN and AuthR information sharing and Shibboleth privacy-enhanced features. The concept was evaluated by constructing a test-bed prototype of the system using standard technologies. The results demonstrated that the solution is practicable and feasible in real environments.

To bring mutual trust and security into the FIAM, the authors compromised on the performance as shown in Figure 2. The STP framework is fully flexible and can accommodate any new attestation scheme [6, 31 and 32] in the future. To carry out the mutual attestation between the HD IdP and the FD SP machines, the IMA may not be a good choice because of privacy concerns. Therefore, in such cases, the PBA or attestation schemes formed upon the PBA may conserve the attested platform privacy.

9. ACKNOWLEDGMENTS

This work was funded by the Universiti Teknologi PETRONAS (UTP) Postgraduate Assistantship Scheme and MIMOS Berhad, Malaysia.

10. REFERENCES

- [1] Zisis, D., Papadopoulou, A-E., and Lekkas, D. 2008. Enhancing security in the integration of e-Government: The e-School initiative. In Proceedings of the 4th International Conference on Web Information Systems and Technologies, vol. 2, 495-502.
- [2] Nuxeo-Shibboleth @ Integration.
- [3] SAGE Library News. 2012.
- [4] Trusted Computing Group (TCG). <https://www.trustedcomputinggroup.org>
- [5] TCG. 2007 Trusted Computing Group (TCG) Specification Architecture Overview revision 1.4, Technical Report. 11-12.
- [6] Alam, M., Zhang, X., Nauman, M., Ali, T., Seifert, J-P. 2008. Model-based behavioral attestation. In Proceeding of the 13th ACM symposium on Access Control Models and Technologies. ACM Press, New York. pp. 175-184.
- [7] Bajikar, S. 2002 Trusted Platform Module based Security on Notebooks PCs. White Paper. Mobile Platforms Group Intel Corporation.
- [8] Cantor, S. 2005 Shibboleth architecture, protocols and profiles. Technical Report.
- [9] Morgan, B et al., "Federated security: The shibboleth approach," Journal of Educause Quarterly, vol. 27, 2004.
- [10] TCPA. 2002 Trusted Computing Platform Alliance (TCPA): TPMe protection profile ver. 1.9.7
- [11] Pearson, S. 2002 Trusted Computing Platforms: TCPA Technology in Context. Prentice-Hall.
- [12] Eastlake, D., Jones, P. 2001 US secure hash algorithm-1 (SHA-1). RFC 3174 (2001).
- [13] Sailer, R., Zhang, X., Jaeger, T., Doorn, L. 2004. Design and implementation of a TCG-based Integrity Measurement Architecture (IMA). In Proceedings of the 13th Conference on USENIX Security Symposium, vol. 13, pp. 223-238.
- [14] Cantor, S et al. 2005 Liberty identity Federation Framework (ID-FF) architecture overview v1.2. Technical Report.
- [15] Fragoso-Rodrigu, U et al. 2006. Federated identity architectures. In Proceedings of 1st Mexican Conference on Informatics Security.
- [16] Helenius, K. 209 OpenID and identity management in consumer services on the Internet. Presented at the Current Internet Trends Seminar on Internetworking.
- [17] Culloch, F. 2008. OpenID and SAML. Technical Report.
- [18] Chadwick, D. W. 2009. Federated identity management. In Foundations of Security Analysis and Design V, vol. 5705, Springer-Verlag, pp. 96-120.
- [19] Lutz. D. J., Campo, R. 2006. Bridging the gap between privacy and security in multi-domain federations with identity tokens. In Proceeding of 3rd Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, pp. 1-3.
- [20] Dey, A., Weis, S. 2010. PseudoID: Enhancing privacy for federated Login. In Proceedings of 3rd Symposium on Hot Topics in Privacy Enhancing Technologies, Berlin, Germany, pp. 95-107.
- [21] Chaum, D. 1982. Blind signature for untraceable payments. In Proceedings of Advances in Cryptography, pp. 199-203.
- [22] Watanabe, R., Tanaka, T. 2009. Federated authentication mechanism using cellular phone - collaboration with OpenID. In Proceedings of 6th International Conference on Information Technology: New Generations, Las Vegas, USA, pp. 435-442.
- [23] Klenk, A., et al. 2009. Preventing identity theft with electronic identity cards and the trusted platform module. In Proceedings of the 2nd Workshop on System Security, New York, USA, pp. 44-51.
- [24] Leicher, A., et al. 2010. Trusted computing enhanced OpenID. In Proceedings of International Conference on Internet Technology and Secured Transaction, London, UK, pp. 1-8.
- [25] Pashalidis, A., Mitchell, C. 2011. Privacy in identity and access management. In Digital Identity and Access Management: Technologies and Frameworks, IGI Global, pp. 316-328.
- [26] Ali, T., et al. 2010. Scalable, privacy-preserving remote attestation in and through federated identity management frameworks. In Proceedings of International Conference on Information Science and Application, Seoul, South Korea, pp. 1-8.
- [27] Khattak, Z. A., et al. 2010. A study on threat model for federated identities in federated identity management system. In Proceedings of International Symposium on Information Technology, KL, Malaysia, pp. 618-623.
- [28] Khattak, Z. A., et al., "Analysis of open environment sign-in schemes: privacy-enhanced and trustworthy approach", Journal of Advances in Information Technology, vol. 2, 2011, pp. 109-121.
- [29] Khattak, Z. A., et al., 2011. Proof of concept implementation of trustworthy mutual attestation architecture for true single sign-on. In Proceedings of the 10th Int. Conference on Security and Management, Las Vegas, Nevada, USA, pp. 721-724.
- [30] Khattak, Z. A., et al., 2011. Security, Trust and Privacy (STP) framework for federated single sign-on environment. In Proceedings of the 5th International Conference on Information Technology and Multimedia, Kuala Lumpur, Malaysia, November 2011, pp. 1- 6.
- [31] Jager, E T., Sailer, R., Shankar, U. 2006. Policy-Reduced Integrity Measurement Architecture (PRIMA). In Proceedings of 11th ACM Symposium on Access Control Models and Technologies, pp. 19-28.
- [32] Sadeghi, A-R., Stuble, C. 2004. Property based attestation for computing platforms: Caring about properties, not mechanisms. In Proceedings 4th Workshop on New Security Paradigms.