American Research Journal of Computer Science and Information Technology
ISSN: 2572-2921
Volume 3, Issue 1, pp: 1-8

AMERICAN RESEARCH JOURNALS
An Academic Publishing House

Research Article Open Access

A Trusted Computing Solution for Security Threats in Federated Identity Management

Anushika Chauhan[1], Dr. Vijay Kumar Tiwari[2]

Department of Computer Science (Cyber Security), Centre for Advanced Studies, Lucknow, India
17mcs03@cas.res.in; vktiwari@cas.res.in

Abstract: Federated Identity Management (FIM) is a collaboration of different federations coming together for the purpose of sharing each other's resources and providing a Single Sign-On facility to the end user. Despite the profitability there are certain issues, vulnerabilities and security aspects that hinder the widespread acceptance of the FIM. These security issues include Snooping, Modification, Masquerading, Replay Attacks, Denial of Service, Escalation of Privileges, Brute Force and Phishing. We have also explored Trusted Computing Technologies-Trusted Platform Module and Trusted Network Connect. Based on our analysis we provide a Trusted Computing framework which can be used to mitigate all the obstacles for the better functioning and acceptance of FIM.

Keywords: Federated Identity Management (FIM), Threats in FIM, Trusted Computing, TPM, TNC

Introduction

ITU-T X.1252 has defined federation as "An association of users, service providers, and identity service providers". Different organizations having certain level of trust among themselves come together providing services to the user on a single click. Before becoming a federation, the participating organizations must accept a legal agreement, clearly defining each other's roles and responsibilities, way of working, risk factors, different levels of providing service, adding new members, revocation of access, dynamic changes (e.g. a legitimate user may access services from a different location using a different system and at a different time). There must be clearly defined process of making a service request and a service response.

FIM provides Single Sign-On facility to users. It eliminates the need to enter credentials for every service provider (SP); instead a single log-in gives access to different SPs in the federation. Chadwick [1] outlines various benefits of FIM - SSO facility, users' identity attributes managed by trusted identity providers facilitating the SPs to focus on providing better services, scalability. Apart from these FIM also helps in business growth, interoperability, simplified user management, easy audits and risk management.

There are, however, certain challenges, vulnerabilities and security attacks vectors that create problems for the widespread acceptance of FIM.

This paper analyzes these issues and shows how Trusted Computing can provide solutions to the mentioned problems.

This paper is organized as follows: Section II describes current FIM systems, Section III discusses various threats and security issues in FIM acceptance, Section IV presents Trusted Computing features relevant to FIM, in Section V we discuss how Trusted Computing can effectively mitigate the underlined threats and Section VI concludes the paper with the future scope.

Current FIM Solutions

FIM is a set of technologies, protocols and processes that allows dynamic distribution of identity attributes and delegation of identity tasks across security domains [10].

The factors involved in FIM are [11]:

- subject (user), possesses a digital identity and a consumer of services.
- identity provider (IdP), authenticates the user and manages the user information.
- service provider (SP) or resource partner, provides services to the user. An IdP can also be a SP.

The service providers therefore trust the IdP for authenticating the user and accept security tokens issued by IdP on the user's behalf. Authentication in FIM is actually a three-factor authentication. A user must be registered with the IdP. It can then access the SP which will redirect it to the IdP for authentication. The IdP then provides specific identity attributes of the user to the SP for asserting the validity of the user.

OAuth

OAuth 2.0 is the industry-standard protocol for authorization in Web applications, desktop applications, and mobile phones. It enables a third-party application (client) to obtain limited access to a service or resource, either on behalf of a resource owner by obtaining authorization from resource owner, or by allowing the third-party application to obtain access on its own behalf. The Protocol flow is [2]:

- The client requests authorization from the resource owner.
- The client receives an authorization grant, representing the resource owner's authorization.
- The client requests an access token by authenticating with the authorization server and presenting the authorization grant.
- The authorization server authenticates the client and validates the authorization grant, and if valid, issues an access token.
- The client requests the protected resource from the resource server and authenticates by presenting the access token.
- The resource server validates the access token, and if valid, serves the request.

OpenID

OpenID is an open protocol that allows a user to use a URI for authentication purposes. This URI is used as an Identifier.

Reference [3] provided a scenario for Login to a Trusted Web Site using OpenID:

- User submits its URI to Consumer web site.
- The Consumer Web site will locate the user's OpenID server and redirects the user browser to that OpenID server to get credentials.
- OpenID server will provide the necessary credentials for user login.

Facebook Connect

It provides users the facility to login to other websites using their Facebook account.

SAML

Security Assertion Markup Language (SAML), is an XML based framework for authentication and authorization across different security systems.

SAML provides three different types of asssertions -

1. **Authentication assertion**: specifies how and when a subject was authenticated. This type of assertion is provided by identity provider (IdP), which is in charge of authenticating users.

2. **Attribute Assertion**: speficies identity attributes of subject.
3. **Authorization assertion**: specifies the request of the subject for a particular resource is granted or denied.

The Protocol flow is-

- The user submits its credentials to authentication authority.
- The authentication authority provides a SAML Token.
- Resources are accessed using this SAML Token.
- Policy Enforcement Point submits SAML token to Attribute Authority or Policy Decision Point. If Attribute Authority grants the request, it attaches an attribute assertion to the SAML Token.
- Now this token can used to access the resources from different organization in FIM.

Shibboleth

Authentication is always performed by the user's own organization– the identity provider, whereas the Authorization is performed at the service provider (SP) side.

- User makes a service request.
- SP redirects the user to its 'Where are you from' (WAYF) service.
- The user selects its IdP to which it belongs.
- Here the authentication of the user is performed (Authn service of IdP).
- Once the user is authenticated, a random identifier is provided to the user.
- SP sends the attribute request to the IdP (SAML Attribute Query Message).
- The IdP sends a SAML Attribute Response Message containing SAML Attribute Assertion to the SP.
- SP decodes the IdP message, verifies the IdP signature, and grants access to the user.

Security Issues in FIM

So far we have discussed various FIM solutions; one thing is common in every scenario: a user, an identity provider, and a service provider. The user requests a service or resource from the service provider, which in turn redirects the user to the IdP for authentication. When authenticated, the SP grants the service. Different platforms use different protocols, personalized or modified for their purpose. There is no single standard which can fit the ideal position for these scenarios. Also the involvement of heterogeneous organizations marks the complexity for the management. Jensen [13] has provided comprehensive account of various challenges in FIM – a) Huge investment cost, b) Liability of participating federations for proper functioning of FIM and responsibility if something went wrong, c) Assurance of verification of identity data of the individuals enrolled at each IdP, d) Trust requirements between federation partners, e) Knowledge of identity management, f) Data synchronization and consistency between different organizations, g) Security-which we will discuss in detail, h) Interoperability-challenges in working of federations adhering to different standards, i) Lack of practical and effective revocation mechanisms. These complexities often lead to security issues in the system. We have identified such security issues which are obstacles in the widespread acceptance of FIM. These are:

Table1. *Threats with Brief Description*

Security Issues	Description	FIM Context
Snooping	Interception of credentials or messages.	The attacker will listen on the network for unencrypted messages and in an attempt to intercept access token or other identity attributes of the user [12].
Modification	Tempering of data.	An adversary may modify the data-in-transit or stored data in the FIM domain.
Masquerading	Impersonating a legitimate user.	This can be a result of snooping or phishing attacks where an attacker getting access to the identity attributes of the user may impersonate a legitimate user. Also an attacker may impersonate a legitimate SP, a threat to the entire FIM security domain.
Replay Attacks	Capturing a message of user and use it later.	Use of HTTP can allow the attacker to launch a replay attack on the SP server for user authentication. Use of HTTPS would reduce the risk [12].
Denial of Service	For complete shutdown of service; sending bogus requests to the server so that the server crash due to heavy load.	An attacker may send several modified requests which take long time to process to the SP resulting in complete shutdown of its services for a particular time.
Escalation of Privileges	Adversary obtains a higher level of permissions on a system or network.	A case of Automatic Authorization. Certain protocols automatically authorize a user for a particular action they have done before in the same session. An attacker using session hijacking can perform that action without providing authorization credentials [12].
Brute Force	Repetitively trying all possible combinations to crack an encryption.	The attacker may launch a brute force attack for cracking the secure communication between the user and the SP or IdP.
Phishing	Tricking individuals into disclosing confidential information usually through emails or bogus web sites.	The attacker would set up a bogus SP which will redirect the user to the fake IdP (having close resemblance to the original IdP). The user signs in to the fake IdP, giving away its credentials to the attacker.

Trusted Computing Features Relevant To FIM

Trusted Computing (TC) aims at establishing a trust transfer system by improving the security of computer architecture [4].

In this section, we describe two trusted computing technologies:

1. Trusted Platform Module (TPM).

2. Trusted Network Connect (TNC).

Trusted Platform Module (TPM): TPMs are hardware chips securely attached to the motherboard of a PC. Its features are underlined as follows:

Platform Configuration Registers

These are memory registers on the TPM. When the machine is first powered on, they all are set to zero, which can be changed using an 'extend' operation. The extend operation specifies a PCR number and the hash value. The PCR's new value is the new input hash value concatenated with the old PCR hash value [5].

Trusted Boot

This is a daisy chain process. When the system is first started, the control goes to the Root of Trust (RoT). This RoT is a small part of BIOS. It measures which BIOS is used to measure the system before passing the control to the full BIOS. The BIOS measures Boot Loader and passes control to Boot Loader. The Boot Loader records kernel before passing control to it. TPM creates a hash of this information and store it in the PCRs (extend operation). This process is also known as Static Root of Trust Measurement. A history file containing information of extend operation is also maintained and kept outside TPM [5].

Remote Attestation

In this process the integrity of the system is checked (verifying that the concerned system is in the correct state). Osborn, Challener [6] describes the process as- the server creates a cryptographic nonce and sends it to the client. Client software creates a TPM 'quote' request, sending the nonce to the TPM and specifying the identity key. The TPM hashes the PCR values along with the nonce and signs the hash. This hash is send to the server for verification which verifies it with public portion of the identity key.

Dynamic Root of Trust Measurement

Unlike static root of trust measurement which starts at the boot time, DRTM can be performed any time, any number of times. Static root of trust measurement guarantees that the system is loaded in required state whereas DRTM provides run-time guarantee. This is needed as the system state may change at run-time due to inclusion of new software/programs. TPM cannot restrict insecure software from loading; it merely saves the state of the system.

The system software loads the codes to be executed in trusted environment and then triggers the DRTM launch instruction. Instruction is broadcasted to the whole hardware components and all the environmental contexts are saved. DMA, interrupts are disabled. Dynamic PCR in the TPM is reset. System executes the above saved codes and extended into the dynamic PCR. DRTM termination instruction is executed and system state is restored [4].

TPM Identities

A new TPM contains only an 'Endorsement Key' (EK) burned by the manufacturer. The public portion of the key is named as EK-PUB and private portion is EK-PRIV. EK-PRIV remains inside the TPM and never leaves the TPM. It is used for decrypting certain data structure and sent it to the TPM for specific purposes while EK-PUB can be retrieved under certain conditions.

Secure Storage

Symmetric keys can be obtained from the TPM or the data can be presented to the TPM for encryption. In TPM, when a protected object is created, the creator states the software state that must exist for revealing the secret. When TPM unwraps the protected object, the current software state must match the stated software state to access the secret, otherwise the access is denied.

Trusted Network Connect (TNC): TNC is an open, interoperable, standards-based network security solution. According to [7] the aim of TNC is:

- **Platform-Authentication**: verification of identity and integrity of endpoints.
- **Endpoint-Authorization**: verifying the 'trusted' state of endpoint and making authorization decision for getting access to the network.
- **Access Policy**: the user must follow the access policies before connecting to the network.

- **Assessment, Isolation & Remediation**: the system that does not meet the security policy requirement can be isolated from the rest of the network, and if possible an appropriate remediation applied such as upgrading software or virus signature database to become eligible for connection to the rest of the network.

TNC Entities and their Components [7] are given in the following table

Table3. *TNC Entities and their Components*

Entities	Description	Components	Role
Access Requestor (AR)	requests access to a protected network	1. Network Access Requestor (NAC)	Software component of AR that negotiates its connection to a network.
		2. TNC Client (TNCC)	Aggregates integrity measurements from IMCs.
		3. Integrity Measurement Collector (IMC)	Measures security aspects of the AR's integrity.
Policy Enforcement Point (PEP)	Compares the credentials of AR and its security compliance against network access policies and decides for granting or denying access to the AR.		
Policy Decision Point (PDP)	PDP communicates its decision to PEP, which actually grants or denies access.	1. Network Access Authority (NAA)	Decides whether an AR should be granted access based on TNCS Action-Recommendation.
		2.TNC Server(TNCS)	Formulates TNCS Action-Recommendation based on IMV Action Recommendation.
		3. Integrity Measurement Verifier (IMV)	Component that verifies a particular aspect of AR's integrity.

A typical TNC message flow is described as follows [7]:

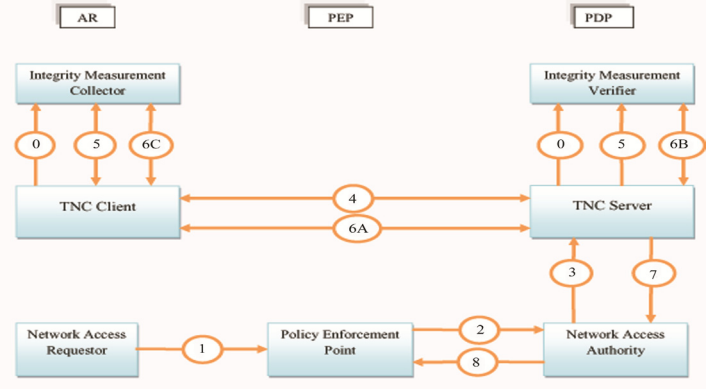

Fig1. *TNC network connection establishment message flow [7]*

0. Prior to begin a network connection, TNCC loads IMC.

1. NAR at AR initiates a connection request.

2. User Authentication between NAA and AR.

3. Upon successful user authentication, NAA informs TNCS of the connection request.

4. TNCS performs mutual Platform Credential Authentication with the TNCC.

5. Upon successful Platform Credential Authentication, TNCS informs IMVs for the new network connection and an Integrity Check Handshake is carried out by TNCS.

6A. Flow of messages between TNCS and TNCC for Integrity Check Handshake.

6B. TNCS passes each IMC message to IMV. IMV provides IMV Action Recommendation to TNCS.

6C. TNCC forwards messages from TNCS to the corresponding IMC.

7. Upon completion of Integrity Check Handshake, TNCS sends its TNCS Action Recommendation to the NAA.

8. NAA then sends its network access decision to the PEP to enforce.

Mitigating the Threats Using Trusted Computing

Here we describe how Trusted Computing can be a successful tool for mitigating all the threats discussed in Section III in FIM.

It is important that the clients, IdPs and SPs are TCG compliant. The participating federations must formulate policies for the effective functioning of the FIM.

We assume that TCG compliant features attestation can be used for accessing critical service or resource. Secure sessions time-durations must be judiciously framed so as to avoid the overhead of authenticating and authorizing the clients multiple times.

In the following table we describe the TC components that can be used for effective threat mitigation.

Table4. *Security Threats and their TC Solutions*

Threats	TC Solution	Description
Brute Force/ Dictionary Attack	TPMs dictionary attack logic [8].	TPM prevents dictionary attack/brute force attack by allowing only a limited number of authorization failures. TPMs have global lockout when too many authorization failures occur [8].
Phishing	TPM Keys	TPM Keys are unavailable outside TPM, so the owner of the keys cannot give the private keys away to phishing attacks.
Snooping	TNC + TPM	TNC provides endpoint security. Messages signed with the TPM keys can only be decrypted by private portion of TPM keys which can be accessed using correct authorization values.
Modification	HMAC + Nonce	For checking the integrity and authentication of the message.
Masquerading	Multifactor Authentication	Passwords, HMACs, State of PCR, State of TPM.
Replay Attacks	Rolling Nonce Protocol	Both the calling process and TPM use fresh nonce in each HMAC computation, and they verify incoming HMACs for integrity and authorization [9].
Denial of Service	TNC	Allow only 'trusted compliance' customers to connect.
Escalation of Privileges	Authorization Protocols	Uses proof of knowledge of authorized data.

Conclusions

In this paper we described various FIM technologies in use today. We also discussed various underlying threats in the FIMs. We described Trusted Computing relevant to FIM and as an effective tool for mitigating mentioned security threats. In our future work we will provide a detailed security framework for the FIMs.

References

1. D.W. Chadwick, "Federated identity management", Foundations of Security Analysis and Design V: Lecture Notes in Computer Science, 2009, pp. 96-120.
2. RFC 6749- The OAuth 2.0 Authorization Framework. https://tools.ietf.org/html/rfc6749
3. Rafeeq Ur Rehman. Get Ready For OpenID. Conformix Technologies Inc. 2008.
4. Dengguo Feng, Yu Qin, Xiaobo Chu, Shijun Zhao. Trusted Computing: Principles and Applications. Tsinghua University Press and Walter de Gruyter GmbH, 2017.
5. David Challener, Kent Yoder, Ryan Catherman, David Safford, Leendert Van Doorn. A Practical Guide to Trusted Computing. IBM Press, 2008.
6. Justin D. Osborn and David C. Challener, "Trusted Platform Module Evolution", Johns Hopkins APL Technical Digest, Volume 32, Number 2, 2013, pp. 536-543.
7. Trusted Computing Group. TCG Trusted Network Connect TNC Architecture for Interoperability, specification 1.1. https://trustedcomputinggroup.org/wp-content/uploads/TNC_Architecture_v1_1_r2.pdf
8. How the TPM mitigates dictionary attacks. https://technet.microsoft.com/en-us/library/JJ889440
9. Liqun Chen, Mark Ryan, "Attack, solution and verification for shared authorisation data in TCG TPM", International Workshop on Formal Aspects in Security and Trust, FAST 2009: Formal Aspects in Security and Trust, pp. 201-216.
10. Eve Maler, Drummond Reed, "The venn of identity: options and issues in federated identity management", IEEE Security and Privacy, vol. 6, no. 2, pp. 16-23, 2008.
11. Zubair Ahmad Khattak, Suziah Sulaiman, Jamalul-Lail Ab Manan, "A study on threat model for federated identities in federated identity maangement system", IEEE 4th International Symposium on Information Technology, 2010, vol. 2, pp. 618-623.
12. Sean Simpson, Thomas Groß, "A Survey of Security Analysis in Federated Identity Management", Privacy and Identity 2016: Privacy and Identity Management. Facing up to Next Steps, pp. 231-247.
13. Jostein Jensen, "Federated identity management challenges ", 7th Int'l Conf. Availability, Reliability, and Security, IEEE CS, 2012, pp. 230–235

Citation: **Anushika Chauhan, Dr. Vijay Kumar Tiwari, "***A Trusted Computing Solution for Security Threats in Federated Identity Management. American Research Journal of Computer Science and Information Technology; vol 3, no. 1, 2018; pp: 1-8.*