Research on Unified Authentication Model based on the Kerberos and SAML

Ding Linhua[1, a], Wang Jiuru[1, b], Wang Xiaojie[1, c]

[1]School of Informatics, LinYi University, Linyi 276000, China

[a]email:private_ding@163.com, [b]email:wangjiuru@lyu.edu.cn, [c] email:wangxiaojie@lyu.edu.cn

Keywords: Unified Authentication; Kerberos; SAML

Abstract. Kerberos protocol is a kind of unified authentication scheme for distributed network environment, which focused on validation functions, not provide complete authorization and access control functions. Security assertion markup language (SAML) is an xml-based framework, which is used to exchange information on authentication and authorization assertions of the subject. But it has not the security protocol for the information exchange between entities. In this paper, an unified authentication model is proposed that improves and simplify the Kerberos protocol, separates the functions of authentication and authorization, and introduces the SAML assertions to this model, in order to safeguard the service provider can be distributed information authorization according to SAML assert.

Introduction

Kerberos protocol provides a unified authentication and single sign-on solution for distributed network environment based on Client/Server network application, but as a result of the HTTP protocol statelessness, Kerberos protocol cannot be directly applied to the world wide web applications based on the Browse/Server (B/S) structure. But the Kerberos protocol focuses on validation functions, there is no complete authorization and access control functions. Security assertion markup language (SAML) is another unified authentication scheme. It is an xml-based framework, is used to exchange information about subject of authentication and authorization assertions. SAML model is simple, universal, but the SAML itself has not the security protocol for the exchange of information between entities, therefore, SAML need combination with other security protocols to provide a safe unified authentication.

Analysis of Kerberos and SAML

Kerberos is an efficient authentication mechanism based on trusted third party put forward by the project team of Massachusetts Institute of Technology (MIT). Its Architecture consists of three parts such as the KDC (Key Distribution Center), Kerberos application server, Kerberos client. When users want to apply for web services, the first Authentication is carried out by KDC Authentication Service (AS) to verify the identity of the user. If the verification success, then AS will distribute to the users a ticket called the Ticket Granting Ticket (TGT), then the users carry their TGT to apply for the KDC authorized Service (Ticket Granting Service, TGS for short), in order to gain Service Tickets (ST) needed for access to the application server. Kerberos protocol use the symmetric key system to encrypt information, through a centralized authentication server to complete two-way authentication between the user and server, provides a unified authentication and single sign-on scheme for traditional distributed network environment based on C/S network application, and has been widely used.

Kerberos protocol architecture and running environment requires encryption calculation on the client, and requests the client maintenance interactions status between the authentication server and application server. Web applications in the world wide web environment rely on HTTP (HTTPS) to host data, and HTTP is an agreement without maintain state, in order to keep the client operating environment (the world wide web browser) is simple to use, Kerberos protocol needs to be improved to apply in the web environment. At the same time the Kerberos authentication and authorization set at a suit (TGS), this approach limits the all service providers must adopt the same authorization model.

SAML is mainly aimed to solve the problem how to use the authentication information for multiple times in the world wide web services security system, can provide users unified authentication and authorization across heterogeneous network and platform. SAML is an xml-based framework that allows exchange their user authentication, authorization and profile information between different institutions, regardless of their safety systems and application platforms. SAML specification is composed by assertions (authentication assertion, authorization decision assertion, attribute assertion), request/response protocol, binding and profile. Unified authentication framework based on SAML usually consists of Entity, Identity Provider (IDP), Service Provider (SP), and provide two unified authentication model such as Browser/an Artifact and Browser/POST.

SAML only defines the document structure of various statement of asserts, itself is not the security mechanism to ensure the security, vulnerable to some malicious attacks such as man-in-the-middle attack, replay attack, information leakage attack, etc. As a result, the SAML needs to be combined with other security agreements or to provide safety unified authentication.

Architecture of Unified Authentication Model based on the Kerberos and SAML

This paper integrates these two kinds of unified authentication model, using the basic idea of Kerberos security agreement, and corresponding improving this security protocol to make it suitable for web services environment. At the same time, this model improves the service ticket token in the Kerberos protocol, separating authentication and authorization function of the system, using SAML to transfer cross-domain identity information, to make the service provider can finally obtain user's SAML assertions according to the service ticket, and use this SAML assertions as a token to flexible customize their access control policy.

The architecture of unified authentication model based on Kerberos and SAML is shown in Figure1 (a), including three systems, the SSO server (including authentication and tickets authorization server), service providers and users.

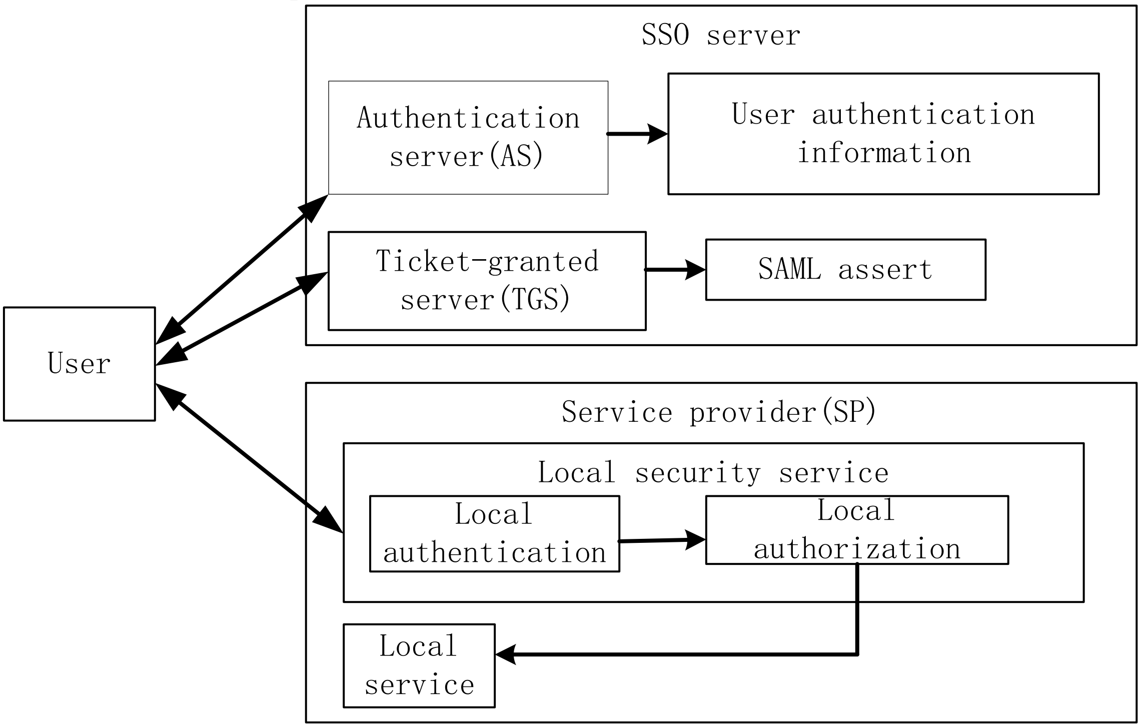

Fig.1. Architecture of unified authentication

SSO server is the core of the whole system, centralized storage and manage user information, service providers and key information, to provide a unified authentication for users and service providers. As Figure1 (b), SSO server includes AS and TGS. AS is responsible for the global user verification, issue TGT. TGS generates SAML assertions for legitimate users throughout successful validation, produces the session key to exchange information with service providers, and issues ST (including SAML assertions of reference) needed for accessing service provider application. Information exchanged between TGS and AS is encrypted with Shared key. As Figure1 (c), Service provider SP is involved in the unified authentication, provides the service for users via the World Wide Web site(WWW). SP exchanges information with SSO server through the WWW redirection, and completes the user authentication, completes authorized work according to the final user SAML assertions.

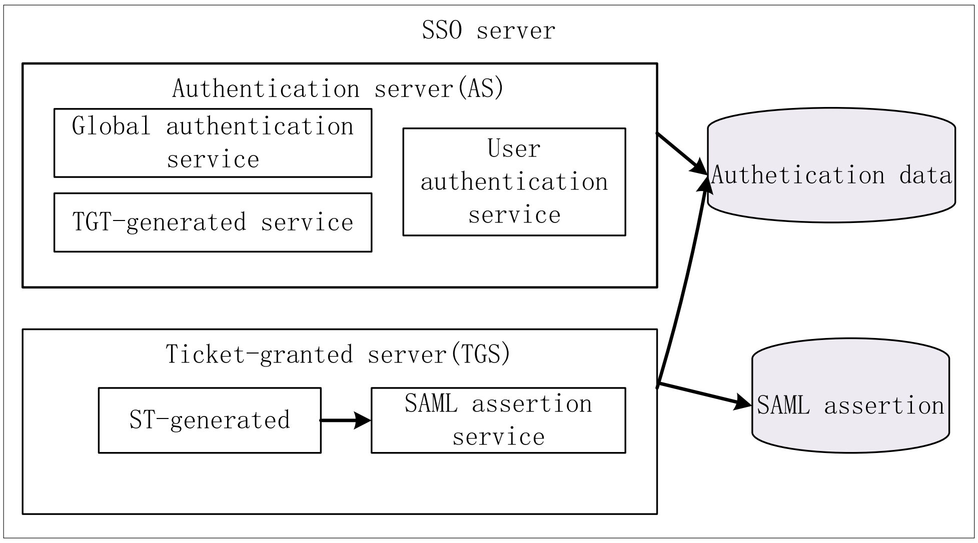
SSO server
Authentication server(AS)
Global authentication service
User authentication service
TGT-generated service
Authetication data
Ticket-granted server(TGS)
ST-generated
SAML assertion service
SAML assertion

Fig.2. Framework of SSO server

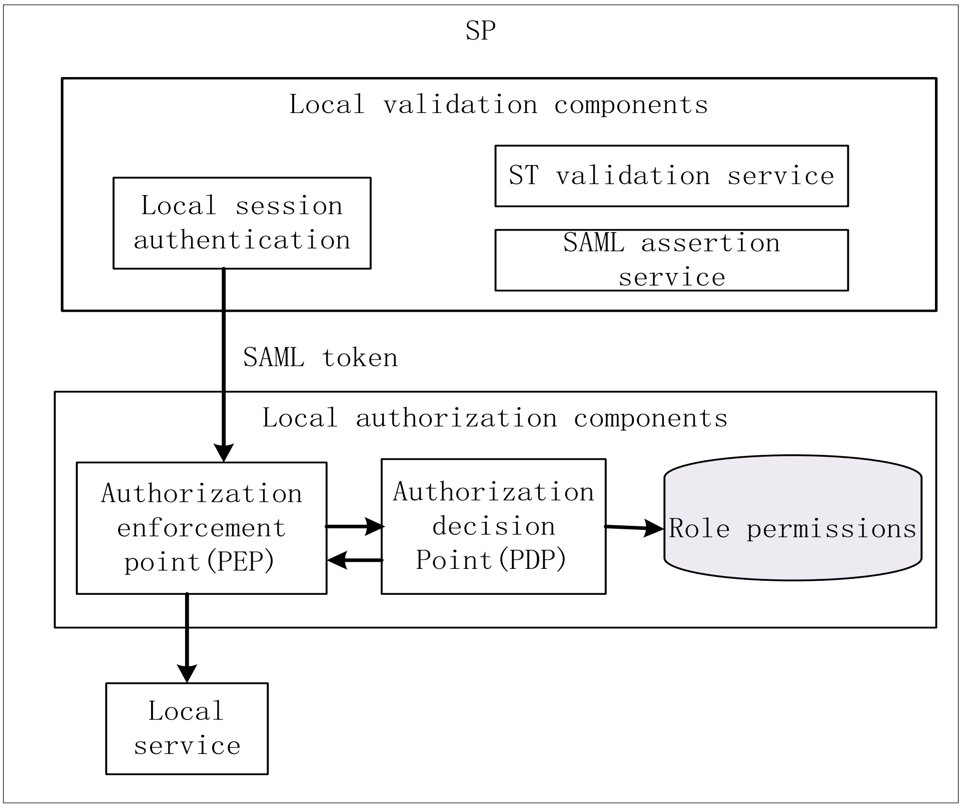
SP
Local validation components
ST validation service
Local session authentication
SAML assertion service
SAML token
Local authorization components
Authorization enforcement point(PEP)
Authorization decision Point(PDP)
Role permissions
Local service

Fig.3. Framework of SP

Authentication Process

In the following work flow, use the following notation. IDx is the identity of the x. Kx represents public key. Kx,y is a shared key or session key between X and Y. The {}K represents encrypting the data using the key K; Symbol || represents a join operation. The first login process is as follows.

Step 1: The user accesses the protected services of SP through a browser.

Step 2: Local session authentication of SP finds that users do not have a local session, and there is no local TGT, then will redirect the user's browser to the AS, in the form of a query string passing its identity.

SP-> AS：ID_{sp}

Step 3: The global session management of AS intercepts the user's request, finds that users have not global validation, then saves the received SP identity, establishes SSL security connection with the user to return the user login page, and requires the user to enter the global user account and password information.

Step 4: Users submit authentication information containing global accounts and password information to the AS via HTTPS security based on SSL connection.

Step 5: AS calculates password message digest of users, and compares it with digest saved in the database. If equal, it is a legitimate user. Then AS saves the user account in session created by the server, sets the global session lifecycle, generates TGT, queries SP site URL according to the identification of the SP, and passes the TGT to SP in the form of a query string.

AS->SP：TGT

Here, TGT={ ID_{tgs}|| $ID_{session}$|| ID_{user} }$K_{as,tgs.}$ ID_{tgs} is the identity of TGS known only by AS and TGS. $ID_{session}$ is the session identity of user. ID_{user} is the global account of user. $K_{as,tgs}$ is the shared key known only by AS and TGS.

Step 6: SP stores TGT in local, and passes its own identity to TGS in the form of a query string for applying service ticket ST.

SP->TGS：TGT|| ID_{sp}

Step 7: TGS verifies the TGT. TGS decrypts received TGT using the shared key between AS and TGS, compares included IDtgs in decrypted TGT with their own identity. If they are equal, TGS confirms the TGT is issued by a legitimate AS. It creates a SAML assertion for the user and save it to the database, generates assertions an one-time quoted Artifact, saves mapping relationship of the Artifact and IDsession, creates the session key Ktgs,$_{SP}$ between TGS and SP, takes out the public key of SP according to its identification IDsp, generates ST structure and passes it to SP in the form of a query string.

TGS->SP：ST

ST={ $K_{tgs,sp}$||Artifact||ID_{sp} }K_{sp}. Here K_{sp} is the public key of SP.

Step 8: SP verifies ST. It decrypts the received query string using its private key. According to the IDsp it confirms whether message is coming from legal TGS, then generates a random string, generates SAML request assertions samlRequest, and sends it to TGS in the form of a query string.

SP->TGS：samlRequest

samlRequest={ random||ID_{sp}|| Artifact } $K_{tgs,sp}$. here $K_{tgs,sp}$ is the session key between SP and TGS.

Step 9: TGS verifies SamlRequest by decrypting received query string using the session key. If success, it searches IDsession according to the mapping relationship between the Artifact and IDsession, then searches SAML assertions database according to the keyword IDsession, after getting the SAML assertions, deletes the mapping relationship between Artifact and IDsession, generates samlResponse and passes it to SP in the form of a query string.

TGS->SP：samlResponse

samlResponse={ random||ID_{sp}||SAMLAssertion||ID_{user} }$K_{tgs,sp}$.

Step 10: SP verifies SamlResponse. It decrypts received query string using the session key, confirms whether message TGS is coming from legal TGS according to the IDsp. It compares receive random string with local saved random string. If consistent, it save SAMLAssertion and IDuser to local session, and removes random string saved locally.

Step 11: SP completes local authorization using SAML assertions. It gets the user role from the assertion, queries access library according to the characters to decide whether to provide service for the user.

Performance analysis

This paper designs a unified authentication model which combines the advantages of both of the Kerberos and SAML and makes the corresponding simplification and improvement on Kerberos. Safety performance analysis of this model is as follows.

Firstly, this protocol can ensure the security when the user authentication information is submitted to the server. this protocol receives the user account and password directly through the secure HTTPS based on SSL connection, calculates MD5 message digest of the user's password to match with the user authentication information in the database, which makes the attacker cannot get the user authentication information through listening technology, and avoids storing the plaintext of user password on the server, to ensure the safety of transmission and storage of the user authentication information.

Secondly, this protocol can ensure the security of key. SSO server stores the user's key calculated MD5 message digest and the public key of SP. TGS generate a session key when it exchanges information with SP, encrypts this random key by the public key of SP and transmits it to SP in a safe way. Then exchanged information between TGS and SP is encrypted by this session key. The life circle of this session key is short. As a result, that greatly reduces the possibility of revealing password and key.

Thirdly, this protocol can ensure the security of TGT and ST. TGT is encrypted through Shared key, as long as guarantee the Shared key don't leak, can guarantee the security of TGT. ST is encrypted by public-key of, only the legal SP having the corresponding private key can encrypting information successful.

Finally, this protocol can prevent replay attacks. TGT contains a session identifier of global-authentication user. This identifier is the only. Whenever TGS receives the TGT, it will verify whether the identifier coming from legitimate users according to the session identifier. So this protocol can prevent the TGT replay attacks.

Conclusion

This paper studies the current two kinds of unified authentication scheme, analyzes the advantages and disadvantages of the two schemes, and puts forward a unified authentication model based on Kerberos and SAML. In the improved model, on the one hand, it adopts the idea of uniform authentication from the Kerberos, on the other hand, it improves the Kerberos token format in the model, to make it can be applied to B/S structure. At the same time, it uses SAML to complete cross-domain identity information transmission, so that the service provider can do access control according to the final gained SAML assertions.

Acknowledgement

In this paper, the research was sponsored by the Natural Science Foundation of Shandong Province (Project No. ZR2014FL012), Achievements Transformation Major Projects of Shandong Province (Project No. 2014ZZCX02702) and Social Sciences Planning Project of LinYi City(Project No.2014LX073).

References

[1] S. M. Bellovin and M. Merritt. Limitations of the Kerberos Authentication System. In Proc. of the Winter 1991 USENIX Conference, page(s):253--267

[2] OASIS Standard.Security Assertion Markup Language(SAML) V2.0 Technical Overview. October 9,2006.http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[3] OASIS Standard.SAML V2.0 Executive Overview.April 12,2005.

http://www.oasis-open.org/committees/documents.php?wg_abbrev=security

[4] SR Kale, ME Scholar, PD Soni. Secure Cloud Computing Based On Mobile Agents. International Journal on Recent and Innovation Trends in Computing and Communication.2015,3(3): 1728 - 1732

[5] MMH Farooqui, KU Koche. A Review on Identity and Access Management for Multitier Cloud Infrastructure by usingKerberos. International Journal on Recent and Innovation Trends in Computing and Communication.2015,3(2):436-439

[6] X Fengguang, H Xie. Networked Automatic Test System based on Message-oriented Middleware. International Journal of Control and Automation.2015,8(3):147-160