World Conference on Technology, Innovation and Entrepreneurship

Security Type Comparison In Service Oriented Architecture Security

Mirsat Yeşiltepe\textsuperscript{a}, Ömer Ö zgür Bozkurt\textsuperscript{b}\textsuperscript{*}

\textsuperscript{a,b}Yıldız Technical University, Beşiktaş, İstanbul - 34349, Turkey.

Abstract

Nowadays more effort has been spending on combining subsystems to form larger systems such as enterprise information management systems rather than simple database management systems. The security of the enterprise system emerges as a growing problem besides the difficulty of the creation of complex systems. One of the major adversities is the wideness of the system coverage area. Especially the concept of cloud computing introduced the notion of coverage without strict borders. The security of this notion also is a research topic. In this study, the security mechanisms and properties of web services as well as the usage areas are explained.

\textsuperscript{*} Corresponding author. Tel.: +90-212-383-4550; fax: +90-212-383-4557.
E-mail address: mirsaty@yildiz.edu.tr

1. Introduction

Nowadays more effort has been spending on combining subsystems to form larger systems such as enterprise information management systems rather than simple database management systems. The security of the enterprise system emerges as a growing problem besides the difficulty of the creation of complex systems. One of the major adversities is the wideness of the system coverage area. Especially the concept of cloud computing introduced the notion of coverage without strict borders. The security of this notion also is a research topic. In this study, the
security mechanisms and properties of web services as well as the usage areas are explained. Access to the data stored in the first when we look at history shows that use of the file. This increases the amount of data structure is disrupted and is open for public use data was encrypted. Then brought the encryption feature to allow user authentication, today is the most important reason to prefer. Access to data in the next step in the use of database systems has been. These methods allow the data to be encrypted and the user has control. But this time, the transmission of this data in a web environment that challenges and difficulties in providing access to data security was a problem. More recently widely used in XML (extensible markup language) are faced with. Despite its name, only the first version with the extended expression as a language, especially in the web world with the emergence of the term cloud environment, such as SOA was insufficient for the upper system. XML contained in the user control, which is the region in which the user (eg, data nodes) to be opened and how much access time cannot be specified due to the lack of a new protocol, such as the need arose. Different problems, especially the XML problems (such as network sharing status) solves the SOAP (Simple Object Access Protocol) use has increased. Data communication problem in the SOA architecture, has been tackled using simple object access protocol. In the next section of the study; the first definition given, as a web service security types are mentioned. Then, transport layer security and message-layer security issues in more detail and handled security types were compared. Finally, where and when to use which type of security are addressed and that the lack of security types are indicated.

2. Types Of Security

Web services security, to ensure the security of web services SOAP extension. Prepared in accordance with the SOAP message schema converted to XML format is transmitted. Web services security, the protection of our minds when we first message with the quality of reliability, confidentiality and authentication is a singularity.

Web services security is examined in three parts: the transport layer security (TLS), message layer security, and application layer security. In this study, application layer security, which is a combination of the first two, not mentioned deeply.

The transport layer security (TLS) over the Internet, the communication between the application and the user is a protocol that provides privacy. Environment has only the client and server although a third component has to do with communication. So message communication is provided by the interaction between client and server only. Best examples of this kind can be given; link to a website to perform as required, when asked on the opposite side of the user name and password authentication is performed by. In this case the client (user) and server (web site) other than the client or the server is not available.

Message layer security, security of information or security information message SOAP message with an attachment that allows the transmission of SOAP messages are included in the appendix. Here not only the communication of messages between the client and server; may be multiple client and server. Even in the environment sometimes unknown. For example, when shopping on e-commerce site's server when you connect to the client's e-commerce website shopping when the amount collected from the bank would be the client. The number of banks may be more than one, and users will also shop at the same time on the site and multi-client multi-server environment is transformed into an environment.

Application-level security is used in certain places these two security type is based on. Who wants to do which is important when transport level connections, message-level security, which the user wants to achieve what data is important for how long. Some of the top systems, one to one relationship between the client and server, and multiple which would be a lot already from the type of security used on the question of where to find a solution is a type of employee safety. It is difficult to provide exact settings of the system, sometimes too little, sometimes it can lead to excessive transportation security elements.
3. Transport Layer Security

Transport layer security, the SSL 3.0 protocol developed by Netscape is a security protocol standardized by the IETF based on. The aim of TLS to authenticate the user as well as for network authentication is to use digital certificates.

Often called TLS, SSL is used instead of the term appears. The reason for this difference between TLS and SSL 3.0 protocols, so it is not obvious. However, TLS 1.0 and SSL 3.0 (TLS 1.0 and SSL 3.0 with backward support mechanism although it can work with) work together. As to the differences between them can give examples. In case of not having to use the server certificate warning message while in TLS, SSL, there is no such a warning message. TLS to encrypt the message and extract key extraction (hash) SSL algorithms using the RSA, SHA uses the symmetric and asymmetric algorithms. TLS certificate verification message during a session with automatically changing the SSL handshake messages, message creation of certificate validation requires a difficult process.

This type of security, usually running on port 80 HTTP (HyperText Transfer Protocol) protocol instead of SSL is running on port 443 prepared by adding HTTPS (Secure Hypertext Transfer Protocol) is used. The main contribution, in HTTP network Anyone who has listened environment to the data as plain text arrives and wants information might be, HTTPS In network Anyone who has listened to the data randomly corrupted (data pieces divided all the data components $\text{GLYLGHGDOOWKHGDWDFRPSRQHQWV}$ $\text{DQVDODUUD\HG}$ $\text{DQGHQFU\SWHGLQDQRUGHUJRDQGJHWLWKDVEHFRPHPRUHGLIILFXOW}$ to use. Https site with a very user name and password used to connect to the event.

In the transport layer security, there are two types of authentication. They are Kerberos and JAAS authentication. Kerberos shared secret key encryption algorithm using traditional trusted third-party authentication service authentication process performs. Different from other means of authentication where the client and server authentication process by asking each other on both sides is to determine exactly who they are. Monitor traffic, even if the seizure of the data in this way will be prevented. The process leading to the description "Kerberos Key Distribution Center" (KDC) should be explained. DC in an Active Directory domain and the users log on to a computer that provides tickets and temporary session keys is a network service. Who want to be included in the system (server or client) first TGT from the KDC (ticket-granting ticket), and a session ticket requests. TGT; about users, which will remain in the group that contains information such as how long a ticket is linked. If authentication fails, then control returns error. Connected to the system if you want to enter the correct password, unencrypted TGT ticket is opened and the connection is performed.

This type of security used in the JAAS authentication is another type of authentication. This is the purpose of authentication and identity authentication. Provides a connection to the authentication system is tested whether the right people, at the authorization identity which users have permission to access to the resources is determined and managed.

4. Message Layer Security

Message-level security, document systems and between business partners digitally signed or encrypted messages enables communication. Unlike TLS signing event and a business partner in this definition does not include the word partners.
Message layer security for authentication in addressing handler (addressing handler) to use. The goal here in the environment, the multiple components (multi-client and multi-server) communication appropriate protocol is used, the address used words (string) check and (extended address word by screening), validation by making contact is to allow. The purpose of the word address to expand the appropriate address to produce new ones. Contact address during the expansion of words, had been allowed to expand. The message-level security is further compounded by complex and an unknown number of servers from one end of the communication when trying to communicate with other servers inoperable after a certain level to come. Address generating word interface, generated address whether its proper format is composed of the functions of controlling.

Transport Level Security, which are described under the heading of JAAS authentication, message-level security is also supported in the security type. Message-level authentication method used in the other one of the proxy (proxy) authentication method. Proxy authentication is specified in the policy file editing is required. The most important advantage of this method is hidden from other servers in the system itself. In this case, the request came from the fact that the impression may think about the confusion, it also tried to enter together as a client or server is not the real goal, the virtual location allows you to reach. Another advantage in the cache (cache) through the mechanism of the servers in the same conditions undisturbed by sending the same request to be prepared for the answers and the top of the system is that it run faster. However, if successful effort to intervene, rather than the actual location where a virtual position is reached it is difficult for the attacker to determine. Today, the encryption system to avoid difficulties due to the excessive functioning of the system preference rate is quite high. In order to implement authentication of access requests in different categories proxy for each URL must use an increasing number. Thus, the server does not respond at the same time increasing numbers in a row and after that puts jobs and / or the data in the cache if there is a direct answer.

Finally SAML authentication method may be employed. SAML (Security Assertion Markup Language) authentication handler that uses the HTTP protocol binding post. Work can be done; "signing and encryption of messages, CRX automatic creation of users and groups, service provider and identity provider authentication is initiated.

SAML is utilized in the authentication servlet. Servlet, the servlet that responds to HTTP request interface is compatible with the working class. Considering the life cycle of the work done will be better understood.
Data security is one of the important issues in the data handler is implemented using sign here, sign the subject. Not all of the data is different from the normal data signing, the signing of the desired section performed. This is the relevant part of the required data to the server or the client will ensure the provision of the signing. In this way, both would rise rapidly as well, never reached to the environment would be unnecessarily redundant data.

 Signing handler details given in the following way: on the client side that can be used to sign requests, responses on the server side also signed. As nodes in an XML document can be signed, only certain items can also be used for signing. As nodes in an XML document can be signed, only certain items can also be used for signing. In the process of a web service, no name or identifier or set an identity component not found a root element; for all the elements in the envelope signed a web service ID is assigned. Any element (identity held by) playing on the server side is done at work may interfere signatures are invalid.

5. Compression Of Security Types

In this section, particular message types security level security (MLS) and the transfer level security (TLS) types will be compared.

TLS only on systems in data communication between client and server while MLS support multiple client and server systems are used. In this way, cloud computing is not certain limits can be considered closer to the MLS.
However, the TS of the MLS and not just to be slower than the communication between the client and server to host due to excessive security measures for implementation of the MLS makes it difficult to choose.

The type of security in both the client (s) and server (s) will be sent encrypted communication between the posts. While the vehicle can operate with MLS as a whole is not accepting TLS tool, when using MLS data on the client and the server, the data is encrypted, the TLS client and server in the data is not encrypted. If you admit TLS tool, maliciously trying to infiltrate into the system, the system cannot be estimated to be within or outside of their own in the message encryption should also differs from that time would be the MLS.

TLS between the client and server platforms and channels using only safe way to transport securing the caller secure authentication, message integrity, message reliability, while the task; any XML messages using transport layer security to transmit data, certificates and digital signatures to use to encrypt messages as there are tasks. MLS data on their own can perform post. So the protocol is independent. So as long as the distortion level of the work environment allows multiple protocol. If the channel is running at TLS protocol-independent (only TCP, IPC, MSMQ, or HTTP) is not. Mutual communication is multi-protocol does not allow messages.

TLS transmission through the HTTPS protocol in the SOAP HTTP configuration need to be realized not only in MLS, web services, and web services are used depending on the specification. TLS in the care of the MLS is better than the performance.

TLS uses the system is relatively easy to attack. It is relatively more difficult to attack using the MLS system. MLS unsafe roads is kept to minimum.

TLS only on systems using communication messages are encrypted as a whole and its sub-systems (client, server) is used as the password. In the MLS system that uses encryption to communicate messages that can be performed all the desired portion of the desired piece of encryption possible.

TLS, the message only to provide security for the transmission line is derived based SSL SSL supports rearwardly; SSL is a part of the message does not support digital signing and encryption are not supported by the MLS.

What is important is that the system in TLS who want to reach. The aim is to communicate with the right client or server That in MLS with whom contacted, as well as how many of those people which data source is given and according to the priority level of requests to be answered as soon as possible provide.

6. Conclusion

Have dealt with types of security protocols that contains client-server architecture supports only HTTP protocol. FTP, SMTP, Telnet is not supported protocols like. Therefore, the TCP / IP running on, directory inquiry services and supports application layer protocol for changing the LDAP (lightweight directory access protocol) is supported. ECC algorithms support has begun to contain some errors. As a result, two security type used in XML encryption algorithms, many symmetric, asymmetric and hybrid algorithms, although ECC algorithms available.

Message-level security with all of the security features of the next TLS also has additional flexibility and features. Message-level security that is for point to point transmission; this means that one or more transmission if the vehicle interior is also secure SOAP messages. Here, you can sign the SOAP message itself except for the connection and / or can be encrypted. Another advantage is that the required elements of the message can be signed separately or can be encrypted. Transfer-level security ensures that only secure the connection. This means that if an intermediary between the client and the web server, if any (distributors), vehicle unencrypted plaintext access to the SOAP message. Agents send a message to the second receiver does not know when the second receiver to the original sender. Traditionally used by TLS encryption "all or nothing" mentality or the entire SOAP message is
encrypted or completely open. So all SOAP messages are encrypted encryption, if desired, a selected portion of the SOAP message (there is no way encryption). Message-level security for authentication may include descriptive icons.

Transport layer security using the client application and the web server with TLS provides security between. TLS to authenticate the other two sides connect over a network to send and receive encrypted data between the application and a secure connection through provides. Optionally verifying a client, a network connection, at the other end application requires a server to authenticate.

References

Abel Wike (2014), Difference between SSL and TLS.
McAfee- Setting Up Authentication Base on URL Categories (2014).
Oracle® Communications Network Integrity Developer's Guid Release 7.1 E23701-03 (2014).