E-Transactions by using secure web services

Govinda.K[1] T.Amith Kumar[2] L. Karunakar[3]
[1]Assistant Professor
[1, 2, 3] SCSE, VIT University

Abstract--- Due to the growth of Internet, millions of users are using internet for various cases such as online shopping, banking etc. Hence it is necessary to provide security to transactions done by the users. In the modern economy, information is critical both as input and output. The Security can be provided by providing security during e-business transactions and web services. There are many options to make web service secure. We can pick any alternatives from conventions based, policy based or message based security. There are various threats are present to web services and e-business transactions such as unauthorized access and disclosing of data. It is essential to provide security to code during designing and developing the web service. The web administrations are playing a crucial role in online transactions.

Key words: - web services, e-business, Online transactions, Security.

I. INTRODUCTION

The first purpose behind the Internet is to move documents around computers, to empower simple remote access to PC's and its use for business purposes has increased since the advancement of the World Wide Web.Accessibility and usability were the prime motive for designing the Internet.Web Service is a product framework intended to help machine-to-machine collaboration over a system.Web service provides distributed computing for creating, publishing, discovering and consuming the services over web.

While there are distinct possible results to represent with Web Services, SOAP is considered as the genuine standard. SOAP messages are constantly sent to administration endpoints recognized by resource identifiers, to manage some data and sending a SOAP response holding data or error codes. This can basically be SOAP over HTTP or even a SOAP message exchanged by SMTP.

To be efficient in business scenarios, Web Services must be suitable for secure communication. Yet the first SOAP determination holds no answers for take care of the security issue. Different methods as SSL or SOAP header in web service calls give standard transport security. The issue: a SOAP association starting with one endpoint to the end point will be seen as a coherent association, abstracting from the physical foundation past. Consistently being an end-to-end association, the physical layer can include various middle people sending SOAP messages. So throughout this procedure of accepting and sending messages, security data can be defined on transport level, the way i.e. SSL makes up to expected marks, can without much of a stretch get lost. Hence any beneficiary needed to depend on the security treatment of his physical association point forerunner, and also its treatment of the information trustworthiness and privacy. A way out is to tag security data on message level.

II. LITERATURE REVIEW

Security can be provided by using the following elements for web services. The six elements are as follows

- Confidentiality.
- Integrity.
- Availability.
- Legitimate use (identification, authentication, and authorization).
- Traceability.
- Nonrepudiation.

A. Confidentiality: Confidentiality includes making data accessible to only authorized parties, or confining data access to unauthorized parties. Doing business over the Internet has been increased under the circumstances.

To administer the confidentiality of Web client's data, organizations need to discover approaches to keep the data from unauthorized view. From an operational perspective, that means data that is saved must be secured in a manner that it can just by entered by authorized parties. Similarly, data in travel must be kept from view of unauthorized parties and that it is recovered just by authentication

B. Integrity: Transmitting data over the Internetis like sending a package by mail. The package may travel various trusted and untrusted systems before arriving at its destination. It is possible for the information to be captured and changed while in travel. This adjustment could be the work of a hacker, system administrator, government agents; it could additionally be unintentional.

The necessity for accuracy of data in information driven society can't be expressed. Regularly, data is either stored at a given location or being passed starting with one point then onto the next. It is possible that way, the essential sympathy toward data respectability is that it remain in place so nothing is included nor taken from it that is not expected or approved. The great instance of absence of data is the point at which an entire database is lost or displaced with something else. Between these extreme cases are situations where information is corrupted either negligibly or fundamentally such that major repairs must be carried out to make it useable once more.

C. Availability: Availability means that systems, information, and different resources are usable when required. Lack of availability is basically misuse of utilization. The most usually known reason for availability issues is Denial of Service (DOS) assaults despite the fact that there are other normal causes, for example, outages, network issues, or host problems. The objective is to ensure that system components give continuous service by preventing failures that could come about because of accidents or attacks. From a security point of view, availability is improved through measures to avoid malicious denials of service.

Closely related to availability and very important to e-businesses are reliability and responsiveness Reliability refers that a system performs practically. Responsiveness is a measure of how rapidly service could be restored after a system failure. As such, it is a measure of system survivability. One advantage for e-businesses is that the Internet, being a distributed system, affords a greater opportunity for building redundancy into systems so as to mitigate denial of service problems. In fact, system survivability is at the heart of the design of the Internet and appropriate use of it should result in minimal availability problems. Nevertheless, there are still real threats to availability.

D. Legitimate use: Legitimate consists of three segments: identification, authentication and authorization. Identification includes a procedure of a client decidedly distinguishing itself to the server that it wishes to lead a transaction with. The most widely recognized strategy for building character is by method for username and password. The process to identification is authentication. Without authentication, it is possible for the system to be gained entrance to by an impersonator. Authentication has to work both ways: for clients to verify the server they are reaching, and for servers to distinguish their customers. Authentication normally requires the element that introduces its identity to affirm it either with something the customer knows something the customer has. Authentication has been turned out to be the most exact method for confirming a client's personality.

The methodology to authentication that is picking up acceptance in the e-business world is by the use of digital certificates. A digital certificate holds unique data about the user including encryption key values. These public/private encryption key sets might be used to create hash codes and digitally sign information. The authenticity of the digital certificate is attested to by a trusted outsider known as a "Certificate Authority." The entire process constitutes Public Key Infrastructure.

Once an entity is certified as uniquely identified, the next step in establishing legitimate use is to ensure that the entity's activities inside the system are limited to what it has the right to do. This may include access to files, control of information, changing system settings, etc. A secured system will establish very well defined authorization policy together with a means of detecting unauthorized action.

E. Traceability: From an accounting point of view, traceability is the procedure of authoritatively looking at records. Essentially, in an e-business security connection, traceability is the procedure of analyzing transactions. Trust is enhanced if clients could be guaranteed that transactions might be followed from starting to finish. If there is a discrepancy or dispute, it will be conceivable to work again through each one stage all the while to figure out where the issue happened and, most likely, who is responsible. Order confirmation, receipts, sales slips, etc. are examples of documents that enable traceability. In a well-secured system, it should be possible to trace and recreate transactions, including every subcomponent, after they are done. An effective auditing system should be able to produce records of users, activities, applications used, system settings that have been varied, etc., together with time stamps so that complete transactions can be reconstructed.

*F. Non-repudiation:*Non-repudiation is the capacity of an originator or beneficiary of a transaction to demonstrate to an third party that their partner completed. Hence the sender of a message ought to have the capacity to demonstrate to an third party that the expected beneficiary got the message and the beneficiary should be able to prove to a third party that the originator did actually send the message. This necessity demonstrates handy to check asserts by the gatherings concerned and to allot obligation is instances of risk. Clearly, this is a pivotal prerequisite in any business transaction when requests are put and both purchasers and dealers requirement to be certain that not just are they managing the suitable gatherings additionally that they have verification to help the cases of any movement taken all the while.

III. ARCHITECTURE

The following architecture describes soap messages and headers:

1. WS-Security describes about SOAP extensions to implements the authentication of client, integrity and confidentiality on messages based services. Therefore it's not the goal of WS-Security to invent new methods, but to know how to use existing security solutions with SOAP. It specifies the formats for authentication and encryption mechanisms. One major benefit is WS-Security works in addition with many other Web Service extensions.
2. The <Security> Header the starting point to WS-Security is a SOAP header element it is called `<Security>`. It contains the security-related data and information needed to implement mechanisms like security tokens, signatures or encryption. This element can be represented multiple times to enable focusing different receivers. The target of a `<Security>` header is announced by use of the `<role>` element. To make safe security information for different receivers you can implement that information in different header blocks, each specifying a different`<role>` value. It's important that no two headers should not have the same `<role>` value or omit the `<role>`. A header without a `<role>` value can be consumed by anyone. Recognize the fact that no two security headers can use the same role. So as we can see only the header element of the SOAP message is altered to add WS-Security. All security elements are placed inside the `<Security>` element. Identity is the major challenge in web services transactions. Without hesitation most services see the importance to know who is requesting services, and whether to give the rights to the message sender access to their services. Authentication is done using security tokens. WS-Security allows us to use any security token we like to use. Explicitly defines as username and password authentication. The first option is customer authentication using username and password validations. WSS defines an element called `<Username Token>` it provides help of this

purpose.<Username Token> among all things having the following elements:

- /Username
  username contains with this token
- /Password
  password of the username contains with this token
- /Created
  details of time and when it was created.

There are variety ways of using the <Username Token> dependent on the way the <Password> element is defined. The easiest way of finding would be just to carry a username and left the password.Tags.<UsernameToken> <Username>MyName</Username></UsernameToken>the WS-Security makes us the means to implement a good security. Conveying the <password> element as a part of the <Username Token> element, the first approach to secure authentication would be done, since an identity could now be proven.<Username Token><Username>My Name </Username> <Password Type="Password Text">My Pass</Password></Username Token>

1) When we talk about time synchronization issues, WS-Security supports the <Timestamp> header. It can be useful to show creation and expired time of a message. This is very worthful for message creation, receipt and doing process. So with the <Security> header, many <Timestamp> elements are identified and focused to many roles. The schema for the <Timestamp> element is defined as
<Timestamp><Created></Created><Expires></Expires></ Timestamp>

IV. Conclusion

The problem of data security in today's networked world is presented together with current basic results applied to solve it. It is argued that the purely technological methodology is not sufficient to produce trust or minimize chance in order to cause companies and their clients to convey e-business with confidence. A risk management approach is presented. With the implementation of this methodology, new money related security markets will emerge to handle the evaluating and exchanging of this type of danger. Demand and supply of e-business hazard insurance will lead to price discovery and market efficiency.

Two conditions are necessary for this new approach to become effective: industry standard needs to be set for what constitutes best practices in e-business security and a new type of "Certification Authority" will have to be instituted to certify that an association adjusts to a set of best practices. These best practices and their certification will then become the standard whereupon market prices for e-business insurance will be set.

References

[1] www.w3.org
[2] http://www.w3.org/TR/2002/WD-ws-arch-20021114/
[3] www.codeproject.com
[4] http://msdn.microsoft.com/en-us/library/ff648643.aspx # c12618429_010
[5] http://www.ibm.com/developerworks/webservices/library/wssec1/index.html
[6] http://technet.microsoft.com/enus/library/cc700820.aspx
[7] http://www.net-security.org/article.php?id=949&p=2
[8] www.4GuysFromRolla.com
[9] http://dev.mysql.com/tech-resources/articles/guide-to-php-securitych3.pdf
[10] http://msdn.microsoft.com/en-us/library/ff649371.aspx

