WebSeA: A Secure Framework for Multi-site Knowledge Representation in Software Engineering

Muhammad Ilyas[1], Ahmad Ali[2], and Josef Kueng[1]

[1] FAW Institute, University of Linz, Altenberger Str. 69, A-4040 Linz, Austria
[2]Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad, Pakistan
{milyas,jkueng}@faw.uni-linz.ac.at, engr.ahmadali@yahoo.com

Abstract. Multi-site software engineering is one of the most extensively used mean of sharing and communicating information of "software projects" to remotely located stake holders. It involves different domains and large number of users. This requires different security measures, to interact and protect relevant data sources. That is why, the issue of securing the data from unauthorized access is very critical. This research work elaborates a secure framework, named WebSeA, to counter the security measures of multi-site software engineering. WebSeA application and WebSeA services are also developed for the practical implementation of proposed WebSeA framework.

Keywords: Multi-site software engineering, WebSeA, Security measures.

1 Introduction

Multi-site software engineering is an approach dealing with software projects that are carried out by multiple teams over multiple sites where team members use different tools, methods and platforms. Exchange of semantics among team members can be complicated if software engineering principles and discipline are not understood and followed exactly. They could use a particular text as their personal guide, and when they share, their own terminology and knowledge-base could be inconsistent in the perception of software engineering theories and practices. As a result, multiple practical issues arise that need to be explored.

Handling the shortcomings linked with remote communication is a question in multi-site software engineering. A common or unique communication language is necessary for knowledge sharing. This enables efficient ways of reaching an agreement of understanding which is of useful to remote team members in a multi-site software engineering. Successful secure communication and coordination among multiple sites is very important for worldwide software development. Due to rapid increase of business at global level, software engineering projects demonstrates importance while dealing with multi-site project development as well as multi-lingual project management. But as here internet is used as a communication medium, there must be preventive measure in terms of security of such communication. Users with mal-intentions may alter such data and create in-consistencies in mutually agreed

J. Suzuki and T. Nakano (Eds.): BIONETICS 2010, LNICST 87, pp. 682–686, 2012.

project information. To handle such potential vulnerabilities, we have given an idea of WebSeA, a framework for a secure and authentic solution for web based applications. Moreover, we have developed WebSeA application and its services, and the practical implementation of WebSeA framework.

Section 2 gives some background information. Section 3 presents the WebSeA framework, WebSeA application and WebSeA Service, where as Section 5 focuses on conclusion and future work.

2 Background

Sidharth et. al. [1] has worked on web based security issues and presented an integrated application and protocol-based framework. IAPF approach based framework provides protection against vulnerabilities in the UDDI/ WSDL protocol, and prevention against DoS/ DDoS based attacks.

Singh [2] has addressed security requirements of grid services and presented a layered grid security model which deals with web services security specifications. This is a five layered model which provides advanced security features like dynamic trust establishment, privacy enforcement, authorization, secure logging, management of certificates, audit trails and key distribution etc. Provision of these features is based on policies like WS-Policy, WS-Trust, WS-Federation and WS-Secure Conversation specifications. The Security Application Layer provides security services are provided by security function so that other domains can also access these features.

Similarly Zhang [3] has presented an integrated security framework for web services. They have focused on different threats to web services like loss of confidentiality, principal spoofing, falsified messages, forged claims and services denial etc. In their model, they have given the concept of usage of Role-based access control, attribute-based access control and risk-adaptive access control respectively.

3 WebSeA Framework

WebSeA framework focuses on techniques to safeguard the web repository to ensure its consistency i.e. use of spam control pictures, alpha-numeric passwords, user identification and authentication, password aging and password social engineering, cryptography in security, personal identity verification, electronic authentication and user authentication on web. Figure 1 represents the WebSeA framework.

This framework supports three types of users. First type is internet users, who just view or browse available web resources. These users do not require registration to view the available web resources. Second type of users requires registration through WebSeA framework to view and participate for the improvement of web repository. Once registered, the user can raise issues which after categorization and filtrations are directed to respective think tanks for further evaluation. However, to prevent un-authorized and computer-based DDOS attacks, we propose in WebSeA framework that each raised issue must accompany spam control image data.

Third type of users is most privileged being software team members working on software projects on multiple sites. Baseline privileges of these users are similar to that of the second type of users discussed above. However, these users may also request for the updating, deletion and append rights on the web repository.

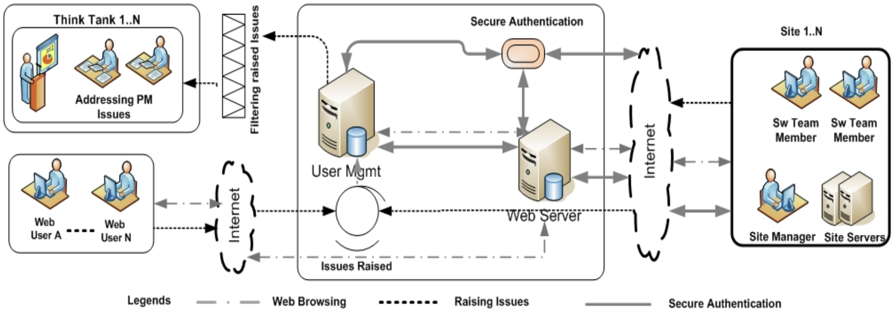


Fig. 1. WebSeA Framework

Here, figure 2 shows the proposed Authentication process of WebSeA framework. The secure authentication process is explained below:

- S-1 Privileged signed-in Member Requests for Admin Rights followed by a spam controller
- S-2, S-3 Generate Dynamic UID and PWD, Encrypt UID, PWD and Session Duration using User's Public Credentials and email to members registered e-mail.
- S-4 Member Get and decrypt UID, PWD and Session Duration and again sign in with new parameters.
- S-5 Server Create a session with admin rights and Connects to Web Repository in editable mode.
- S-6 User is connected to Web Repository Server in editable mode.

Here second and third step are the key innovation in WebSeA framework. For the implementation of WebSeA framework, we have developed an application. WebSeA Application is a web base application, implementing all the processes discussed in WebSeA framework, however, WebSeA Web Service is the backbone of WebSeA Application. Privileged users request for editing rights, these requests are listened and entertained by WebSeA Web Service.

Any user can access web repository by accessing WebSeA Website, however, only registered users can raise issues. These issues are categorized and after getting filtered sent to respective category think tanks for be resolved.

The privileged users, like software project teams can also request for appending, editing and deleting web repository data. However, this access is granted by sending encrypted access key to the user's email box. These users have decrypting application on their remote sites. Figure 3 shows the screen shot of decrypting application.

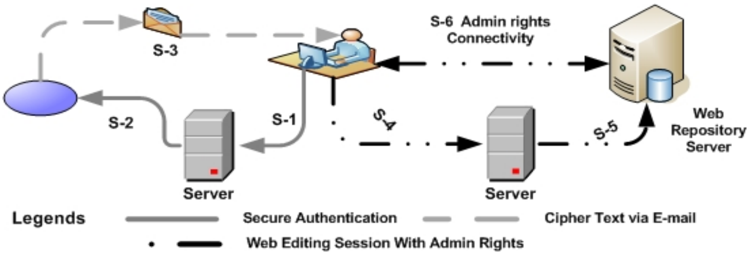
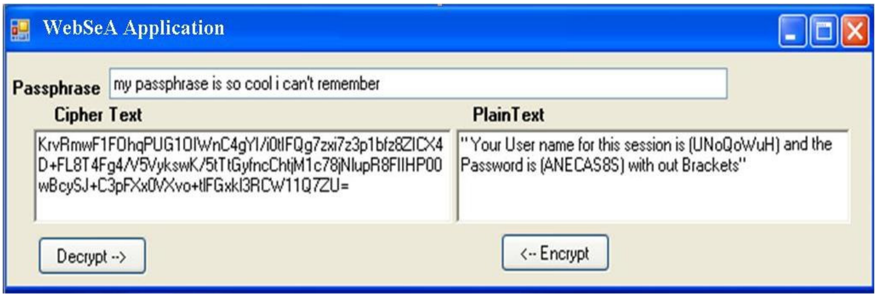


Fig. 2. WebSeA Secure Authentication Process



Passphrase: my passphrase is so cool i can't remember

Cipher Text

```
KrvRmwF1FOhqPUG1OIWnC4gYI/i0tIFQg7zxi7z3p1bfz8ZICX4
D+FL8T4Fg4/V5VykswK/5tTtGyfncChtjM1c78jNlupR8FIIHP00
wBcySJ+C3pFXx0VXvo+tIFGxkI3RCW11Q7ZU=
```

PlainText

"Your User name for this session is (UNoQoWuH) and the Password is (ANECAS8S) with out Brackets"

Fig. 3. WebSeA Decryption Application

Users after receiving encrypted key via email use decrypting application and their pass key can get dynamically generated username and password, however, age of this username and password is also very limited, generally 10 to 20 minutes (or as decided by the organization). This username and password will no more be valid once that session gets expired. Moreover, user must also have to pass through the same spam image control check each time he/she requests for editing rights.

4 Conclusion and Future Work

WebSeA framework has been introduced as a mean of secure web based knowledge representation. Usage of spam control images, dynamic generation of usernames and passwords for a limited time, usage of non-dictionary words as usernames and passwords, sending of encrypted key via email and decrypting application are the features used by remote site users under the supervision of site manger. User needs encrypted key and passkey to execute the required action. All the above mentioned features have been implemented in WebSeA framework against authentication vulnerabilities. Currently, WebSeA framework is based on symmetric encryption methodology. In future, we plan to implement the same by using Asymmetric encryption methodology.

References

1. Sidharth, N., Jigang, L.: A Framework for Enhancing Web Services Security. In: 31st Annual International, COMPSAC 2007, July 24-27, vol. 1, pp. 23–30 (2007)
2. Singh, S., Bawa, S.: A Framework for Handling Security Problems in Grid Environment using Web Services Security Specifications. In: SKG 2006, pp. 68–68 (2006)
3. Wenjun, Z.: Integrated Security Framework for Secure Web Services. In: 2010 Third International Symposium on IITSI 2010, April 2-4, pp. 178–183 (2010)