Globus An International Journal of Management & IT
A Refereed Research Journal
Vol 7 / No 2 / Jan-Jun 2016 ISSN: 0975-721X

A STUDY OF WEB SECURITY

*Neha Sharma

Abstract

The researcher discussed about the image stitching that is the process of modifying the perspective of images and blending them, so that the photographs can be aligned seamlessly. The success of web service technology is clearly evident from the usage and adoption of this IT technology. A large number of providers from different sectors of industry are shifting to web service technology. Web services are software components accessible through programmatic interfaces and can perform tasks from simple requests to complex processes. Priority based trust (PB) model presented for service selection in general service oriented environments. It follows Reputation based and Trusted Third Party approach. It overcomes the limitations of Certified Reputation Model. PB Trust model is also getting consumer expectation on trust for individual service attribute.

Keywords: *Web Service Technology, . Priority based trust, Reputation based, Trusted Third Party approach.*

Introduction

Security analysis allows one to delimit the security perimeter of a computer system. In service oriented architectures, such task is intrinsically complex, due to the many architectural layers, technologies and communication protocols involved. The security analysis must also consider the particular implementation for a given SOA. In this deliverable we first introduce different kind of attacks that are related to web-services and embedded devices, to then cover threats that appear in presence of service composition. We also present accepted methodology with proposition of a generic attacker model that can be instantiated for different SOA settings, which allow an analysis of specific categories related to SOA. Finally, we carry out the security analysis of the main CESSA use-cases.

The success of web service technology is clearly evident from the usage and adoption of this IT technology. A large number of providers from different sectors of industry are shifting to web service technology. Web services are software components accessible through programmatic interfaces and can perform tasks from simple requests to complex processes. The heterogeneous nature of web service technology offers advantages like interoperability, usability, use of standardized communication protocol, deplorability, etc. This makes web services technology an ideal candidate for organizations to host and deploy services in order to collaborate with other organizations in a flexible manner.

In order to attain the trust of service users, it is necessary that the system must conform to the performance requirements as it is the most important criteria for evaluating a system. It is therefore necessary to test the system before deployment in order to ensure that the system meets quality of service requirements. Various testing tools have been developed and designed for testing of web services. By using these test tools, web engineers can perform their tasks easily and efficiently, thus improving the quality of the system.

Review of Literature

Web Service is a reusable component which has set of related functionalities that service requesters can programmatically access from the service provider and manipulate through the Web. One of the main security issue is to secure web services from the

*Research Scholar, Kalinga University, Naya Raipur

malicious requesters. Since trust plays an important role in many kinds of human communication, it allows people to work under insecurity and with the risk of negative cost, many researchers have proposed different trust based web services access control model to prevent malicious requesters. In this literature review, various existing trust based web services access control model have been studied also investigated how the concept of a trust level is used in the access control policy of a service provider to allow service requester to access the web services.

Galiziaet.al. presented a trust model for accessing web service. It follows Trusted Third Party based approach for the classification of the web services with the help of Internet Reasoning Service tool.

Surya Nepal et al. (2010) developed a fuzzy based trust management framework for web service. Initially, they developed a data model based on consumer views on QoS attributes that evaluates the reputation of services. Secondly, they proposed the fuzzy based linguistic query model to parse the requested query to evaluate by different query processing algorithm. They have not addressed some issues such as trust bootstrapping, propagation, retaliation, reciprocation and dishonest or biased ratings.

Priority based trust (PB) model presented for service selection in general service oriented environments. It follows Reputation based and Trusted Third Party approach. It overcomes the limitations of Certified Reputation Model. PB Trust model is also getting consumer expectation on trust for individual service attribute.

Honest agent can give the feedback and ask other participants in same domain about the services. The reliability of the service is calculated as average of all the feedbacks from participants. The consumer may give the dishonest about the service to make the reputation value to be decreased. When the trust management center found this dishonest feedback, punishment can be given to the consumer.

Mangling Zhu et al. (2006) designed the social rules on describing the trust relationship between the provider and consumer in the open environments. Self Confidence Rule which rate the self confident of service provider about their providing services. Persistence Rule says that a service provider should be persistent to their goals to achieve better performance. Honest Rule analyze whether service provider is trustworthy in their commitments. Motivation Rule checks for motivation in providing services. Reliance Rule estimates the trust from the reliability of service provider. If an agent was unreliable at previous transactions with a consumer, its trustworthiness will be decreased. Reputation Rule finds whether it has positive or negative feedback about providing services from the other agents in the open environment. If an agent always performed the committed service, then its reliability will increase, consequently reputation will improve. Trust value of an agent will increase based on their reputation and other dimension and also it automatically updates their reputation. Finally, they defined a trust is based on performance, commitments, social attitude and relations of particulars.

Internet Security and Web Computing

Web access has opened new vistas for various sectors of society including businesses. The ability that anyone using (virtually) any device could be reached anytime and anywhere presents a tremendous commercial potential. Indeed, the number of web applications has seen a exponential growth in the last few years. The Internet has undoubtedly introduced a significant wave of changes. The increased electronic transmission capacity and technology further paves a superhighway towards unrestricted communication networks. To provide interworking, the future systems have to be based on a universal and widespread network protocol, such as Internet protocol (IP) which is capable of connecting the various wired and Wireless networks. Web computing environment supports user web, network web, bearer web, device web, session web, service web and host web.

Breaching Information Security

Hacking, cracking, and cyber crimes are hot topics these days regarding information security and will continue to be in near future. When the World Wide Web was mainly used to send e-mail and view remote data, the main concern was amateur hackers devising ways to break into large systems for bragging rights’. Hackers are almost impossible to eliminate. As one group is caught, another replaces them. This thesis will tell how hacking is organised and also about some of the ways hackers use to breach security.

Emerging Trends on Web Security

This study describes the use of different web security techniques. Every now and then hackers are challenging web security measures. We describe the security systems. Its components and various issues involved in the design of security systems for world wide web involving web server access control through password authentication.

Hash Racking and Its Impact on Information Security

One of the most important classes of typographic algorithms in current use is the class of cryptographic hash functions. Hashes functions are ubiquitous in today’s IT systems and have a wide range of applications in security protocols and schemes, such as providing software integrity, digital signatures, message authentication and password protection. In the Crypto 2004 conference one of the big news was that a fundamental technique in Typography i.e. Message Digest 5 (MD5,) had been cracked. Soon after this event, it was announced that the Secure 1-lash Algorithm (SHA-1) had been cracked. Data assurance has come under scrutiny due to attacks on hashing schemes. This thesis will discuss in detail the broken MD5 and SHA-l, which both are reported to have been cracked, and Wi-Fi investigate any impact. This thesis also shows the implications of these recent attacks, and the possible directions for the development of the theory of hash functions.

Information System’s Security by Using Matrices and Graphs

This thesis illustrates that all the projects to design or develop secure information system for processing classified information have had a formal mathematical model like matrices and graphs for security as part of the top level definition of the system. The model functions as a precise description of the behavior desired of the security relevant portions of the system. In this, an attempt is made to explore the matrices models that can be used in the construction of information system’s security.

Conclusion

Image Stitching is the process of modifying the perspective of images and blending them, so that the photographs can be aligned seamlessly. The aim of this research is to web security through achieve seamless image stitching without producing visual artifacts caused by various reasons like changed lighting conditions, vignette effects, severe intensity discrepancy and structure misalignment. The process of image stitching consists of Registration, Calibration and Blending. Image registration is an automatic or manual procedure which tries to find corresponding points between two images and spatially aligns them to minimize a consistent distance measure between two images. Detailed review of SIFT descriptors are given in this research for image registration process as they are considered best invariant to image-scaling and rotation, and partially invariant to changes in lighting. The descriptors are also well localized in the spatial and frequency domains, and so minimize the effects of occlusion, clutter, and noise. RANSAC algorithm is used in this to calculate full homography in the presence of outliers to match the descriptors. RANSAC method counts the inliers based on some threshold value which depends on the noise present in the images. This is done by estimating corresponding models from some randomly drawing data subsets and calculating how many data elements agree with each model. When different images are stitched together, the adjacent pixel intensities may differ and can produce seams. Feathering and Image pyramids are suggested as a measure to remove these artifacts. It explores vital aspects of image stitching and suggests the appropriate methods available for stitching and homography in the process of image blending in web security.

References

1. R. Joseph Manoj, A. Chandrasekar, M.D. Anto Praveena, Gandhi Desai , 2012 ,“AFTAC: Attribute, Feedback and Time Decay based Access Control for web services”, ICCCIT.
2. Hien Trang Nguyen, Weiliang Zhao, Jian Yang, 2010, “A Trust and Reputation Model Based on Bayesian Network for Web Services”, IEEE International Conference on Web Services.
3. V. Mareeswari, Dr. E. Sathiyamoorthy, 2012 “A Survey on Trust in Semantic Web Services” International Journal of Scientific & Engineering Research, Volume 3, Issue 2.
4. Srividya K Bansal, Ajay Bansal, M. Brian Blake, 2010, Trust-based Dynamic Web Service Composition using Social Network Analysis, IEEE Workshop on Business Applications of Social Network, 13th December .
5. Damjan Kovac and Denis Trcek, 2009,Qualitative trust modeling in SOA, Journal of Systems Architecture, 55, pp. 255-263.
6. Donovan Artz and Yolanda Gil, “A survey of trust in computer science and the Semantic Web”.
7. Stefania Galizia, Alessio Gugliotta and John Domingue,2007, A Trust Based Methodology for Web Service Selection, International Conferences on Semantic Computing.
8. Surya Nepal, Wanita Sherchan and Athman Bouguettaya,2010, A Behaviour-Based Trust Model for Service Web, IEEE international Conference on Service Oriented Computing and Applications.