Computer Engineering and Intelligent Systems www.iiste.org
ISSN 2222-1719 (Paper) ISSN 2222-2863 (Online)
Vol.4, No.6, 2013 - Selected from International Conference on Recent Trends in Applied Sciences with Engineering Applications

Security Schemes for Hack Resilient Applications Using "SNHA" (Securing Network, Host, and Application) Service

Kamal Kulshreshtha
M.Tech. (CSE), Department of CS/IT Engineering, Mewar University, Chittorgarh (Raj.)
Tel: +91-9829290520 E-mail: kamalkul@rediffmail.com
Prof. Ajay Sharma
Department of CS Engineering, SRM University, Ghaziabad (UP)
Tel: +91- 01232-234300, 301 E-mail: ajay.kumar@srmimt.net

Abstract
The very nature of web applications - their ability to collate, process and disseminate information over the Internet - exposes them in two ways. First and most obviously, they have total exposure by nature of being publicly accessible. Second, they process data elements from within HTTP requests - a protocol that can employ a myriad of encoding and encapsulation techniques. Any service available on the Internet requires authentication. Simple, one factor authentication schemes are vulnerable to hacking and require lot of discipline among authorized users - in the form of complying with strong password, One Time Password and password salt. The challenges start from making the authentication setup of the network services as secure and as simple as possible. In order to overcome this problem, we will develop a portal and authentication setup to address the problem of the directly making the authentication setup and the web services of the organization accessible from the internet. For our purposes we will concentrate on the combination of web servers and application servers interfacing to provide user authentication as multi-tenant applications.
Keyword: - Network security, Web-Security, Multi tenant, Web-service, SAAS, SOP, WCF, multilevel authentication, one time password (OTP), Salt password.

1. Introduction

Traditionally, security has been considered a network issue, where the firewall is the primary defense or something that system administrators handle by locking down the host computers.
Many organizations today are looking up to security services as an architectural solution to provide a robust computing platform to connect to legacy systems.
The main causes of acceptance of this latest design paradigm are its distinct advantages of reusability ease of maintenance, interoperability, reduced development cost, defined standards and many more.
First and most obviously, they have total exposure by nature of being publicly accessible. This makes security through obscurity impossible and heightens the requirement for hardened code. Second and most critically from a testing perspective, they process data elements from within HTTP requests..
This attention comes with the benefit of it being addressed as a higher priority now, but with the drawback of still being in an emerging area of technology. The current use of most web application security testing tools is still focused on the penetration tester/information security professional, with use being extended for QA and audit professionals.
This approach of distributed computing is not suitable for homogenous IT environment, true real time systems, old legacy systems and systems where tight coupling is required. Besides certain areas where security has not proved to be beneficial there are certain critical aspects that are to be considered. Service versioning, service security, availability, service discovery, unfurnished standards, request change etc. are few of them.
Security has always been a holistic solution, requiring all players and systems to work in concert to form a good defense.

2.0 Literature Survey and Analysis

Literature surveys are important as research tools, especially in emerging areas, with populations that typically yield small samples (e.g., special education research often does), or in areas that represent value-laden positions adopted by advocacy groups.

2.1 Purpose of Literature Survey

The main purpose of a literature review is to describe and establish the theoretical framework on work that has been reported on a subject or field.

Many organizations are turning to SOA to help lower the cost of ownership, maximize IT efficiency, and plan for future growth. A services framework is essential to achieve these goals. A services framework finely tuned to the business needs of a company enables SOA to boost IT efficiency by use — and reuse — of tools across interfaces and business functions [11].

The reuse also decreases redundancy of functionality as services. At the same time, a services framework can help drive down the total cost of ownership. An effective services framework demands an end-to-end analysis of each business process to achieve an actionable understanding of the company's value chain. Through this detailed analysis, the organization also gains crucial insight into its overall applications and technology platform, which enables it to develop and discover affordable and effective services [10].

The use of distributed systems by enterprises has increased exponentially in past few years due to certain factors such as readily accessible internet and World Wide Web (WWW). Software as a Service (SaaS) is a latest computing paradigm that utilizes services as the basic constructs to support the development of rapid, low-cost and easy composition of distributed applications, even in heterogeneous environments [9].

Another area of IT expertise in which many companies are lacking is the ability to create common data models with strong contract and policy definitions, which are essential to ensuring that services are reusable. Organizations typically take shortcuts in building the data model, failing to recognize that the services are, at their essence, nothing more than the sum of their generic information and data models. We also have found that business units within an organization may resist a standardized service approach because they believe their needs have unique requirements that cannot bead dressed by generic services. This shortsighted approach does not take into account SOA's ability to employ extensions to services that make them reusable, yet unique, by division or geographic location [8].

"Security systems typically attempt to introduce barriers (such as passwords or other authentication mechanisms) while human-computer interaction (HCI) designers attempt to remove such barriers."

The above quote is very meaning to the primary reason for conducting this review: security and usability in software development are two important factors that until now have been unable to cooperate in the same development process.

Information systems security is a very important consideration during software application development process. It is just as important as the delivery of the functional requirement.

In the project's initiation phase the environment, operating system, database design and system architecture can be modeled with security built in, ensuring compliance with appropriate legislation, regulations and standards.

The application's architecture should be driven from an agreed security policy for the web application or website. All inter-connected systems must be identified, specified and the dependencies documented.

Functional design analysis and planning and the creation of system design specifications, including the security framework, will provide an understanding of the security issues and methods of negating or minimizing security risks.

2.2 Website threat modeling

The context of a website will affect the types of threats identified. The term website can include intranets, extranets and public sites but there can be a huge overlap of these in the websites of enterprise organisations. Threat modelling vulnerabilities

For websites and web applications (transactional website processes), the following are likely to be the major categories of vulnerabilities:

- input and output data validation
- authentication
- authorization
- session management
- configuration management
- sensitive data
- cryptography
- exception handling
- auditing and logging

Any website or web application which has any form of user interaction will include all of these potential categories.

3.0 Level of security

We started with the in depth study of the subject. In this, we will provide security at three levels [3]:

- Network

Network security is to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

- Host

Web servers are one of the most targeted public faces of an organization, because of the sensitive data they usually host. Securing a web server is as important as securing the website or web application itself and the network around it.

- Application

Application level security is currently receiving a great deal of attention. Poorly protected applications can provide easy access to confidential data and records. Access control/authentication ensures only authorized users are able to access the application.

A weakness at any layer can be exploited by an attacker.

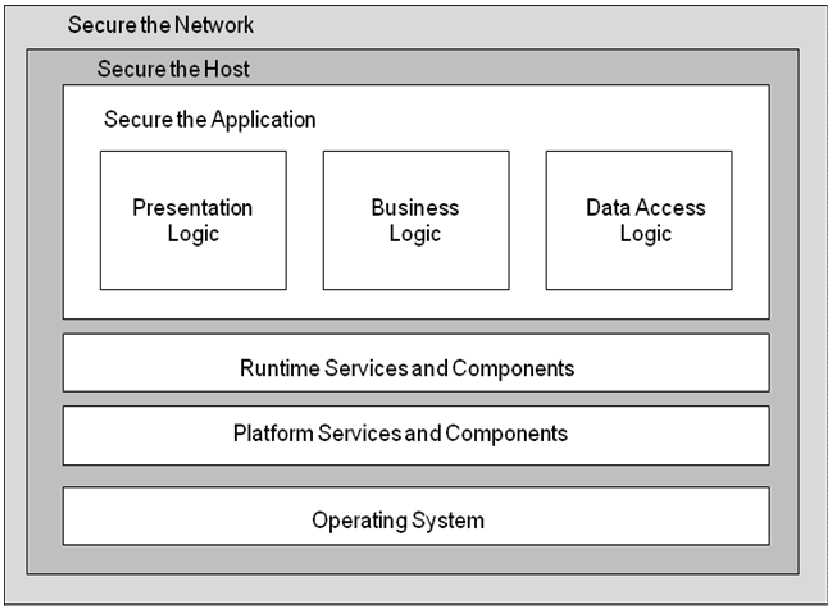

Figure 1: The three-layered approach:
securing network, host and application

4.0 Security Features

- A login will be provided to each user, which authenticates user's identity.
- Role-based Security: Role-based security is an approach to restricting system access to authorized users.
- Strong Passwords: The strong passwords that are complex, are not regular words, and contain a mixture of upper case, lower case, numeric, and special characters.
- Non-reversible Password: Store non-reversible password hashes in the user store.
- Account Locked out: The account locked out mechanism will be enforced for end-user accounts after a set number of retry attempts.
- One-Time Password: The one-time password will be generate & send to the users registered mobile no. when user tries to logged in from unregistered Mac Address.
- Least Privileges: Least Privileges will be given to accounts to connect to the database.
- Parameterized Stored Procedure: We will use parameterized stored procedures for database access to ensure that input strings are not treated as executable statements.
- Exception Handling: we will use of exception handling throughout our application's code base.

These Features are countermeasure for following types of attack:

- Buffer overflows vulnerabilities can lead to denial of service attacks or code injection. A denial of service attack causes a process crash; code injection alters the program execution address to run an attacker's injected code.
- Cross-Site Scripting, An XSS attack can cause arbitrary code to run in a user's browser while the browser is connected to a trusted Web site.
- SQL Injection attack exploits vulnerabilities in input validation to run arbitrary commands in the database.

- Network Eavesdropping, if authentication credentials are passed in plaintext from client to server, an attacker armed with rudimentary network monitoring software on a host on the same network can capture traffic and obtain user names and passwords.
- Brute force attacks rely on computational power to crack hashed passwords or other secrets secured with hashing and encryption.
- Dictionary attacks are used to obtain passwords. Most password systems do not store plaintext passwords or encrypted passwords.
- Disclosure of confidential data can occur if sensitive data can be viewed by unauthorized users
- Data tampering refers to the unauthorized modification of data.

5.0 Tools are required

The Windows Communication Foundation (WCF), previously known as "Indigo", is a runtime and a set of APIs (application programming interface) in the .NET Framework for building connected, service-oriented applications. WCF is meant for designing and deploying distributed applications under service-oriented architecture (SOA) implementation. Clients can consume multiple services; services can be consumed by multiple clients.

Features of WCF

- Service Orientation
- Interoperability
- Multiple Message Patterns
- Service Metadata
- Data Contracts
- Multiple Transports and Encodings
- Reliable and Queued Messages
- Transactions

6.0 Features of "SNHA"

6.1 Multi-tenant

The term multi-tenancy in general is applied to software development to indicate an architecture in which a single running instance of an application simultaneously serves multiple clients (tenants) [6].

6.2 User Authentication

User authentication is a means of identifying the user and verifying that the user is allowed to access some restricted service.

6.3 One-time password

A one-time password (OTP) is a password that is valid for only one login session or transaction.

6.4 Password Salt

In password protection, salt is a random string of data used to modify a password hash.

6.5 Password hashing

Hash algorithms are one way functions. They turn any amount of data into a fixed-length "fingerprint" that cannot be reversed.

6.6 Strong password

A strong password consists of at least six characters (and the more characters, the stronger the password) that are a combination of letters, numbers and symbols (@, #, $, %, etc.) if allowed.

7.0 Future Work

As future work, we will create a security service to make secure network, host and application. We create hack resilient application to define rules and measures to use against the attacks. We also provide secure protection mechanism portals from a high risk of intrusion or fraud by user authentication as multi-tenant applications."

8.0 Conclusions

In this, we propose security services as an architectural solution to provide a robust computing platform. The main causes of acceptance of this latest design paradigm are reusability. The current use of most web application security testing tools is still focused on the penetration tester. Organizations are turning to SOA to help lower the cost of ownership, maximize IT efficiency, and plan for future growth. In the project's initiation phase the environment, operating system, database design and system architecture can be modeled with security built in. There are three levels of security i.e. at Network, Host & Applications. A weakness at any layer can be exploited

by an attacker.

9.0 Acknowledgement:-
The author would like to acknowledge with deep sense of gratitude to my project mentor, Prof. Ajay Sharma, Dept. of CSE, SRM University, Ghaziabad (UP) for his valuable suggestions and guidance.

10.0 References

1. Dr. James H. Yu & Mr. Tom K. Le, "Internet and Network Security", Journal of Industrial Technology, Volume 17, Number 1 - November 2007 to January 2008.
2. eMarketer, "Worldwide Internet Users", URL http://www.emarketer.com/estats/selleglob.html.
3. Bell, Michael, SOA Modeling Patterns for Service-Oriented Discovery and Analysis. Wiley & Sons. pp. 390. ISBN 978-0-470-48197-4, 2010.
4. Erl, Thomas. Serviceorientation.org – About the Principles, 2008–08
5. http://visualstudiomagazine.com/Articles/2011/06/01/pcnet_WCF-and-SOA.aspx?Page=1
6. Research and Evaluation in Education and Psychology, sagepub, Chapter3, p. 89-120
7. L. Srinivasan, "An overview of Service Oriented Architecture, Web Services and Grid Computing", HP(Hewlett Packard) White Paper, November 2007.
8. L. Hancheng, "Design of SaaS-based Software Architecture", International Conference on New Trends in Information and Service Science, 2009.
9. K. Kalaiselvan and P. Venata Krishna, "Grid to Cloud (G2C) - A infrastructure based transition", CSI Journal, February 2010, pp 22-25.
10. Research and Evaluation in Education and Psychology, sagepub, Chapter3, p. 89-120
11. Advisory Services Business Systems Integration http://www.pwc.com/us/en/increasing-it-effectiveness/assets/Framework_for_SOA_Services_Final_v2_7.9.pdf.

This academic article was published by The International Institute for Science, Technology and Education (IISTE). The IISTE is a pioneer in the Open Access Publishing service based in the U.S. and Europe. The aim of the institute is Accelerating Global Knowledge Sharing.

More information about the publisher can be found in the IISTE's homepage: http://www.iiste.org

CALL FOR PAPERS

The IISTE is currently hosting more than 30 peer-reviewed academic journals and collaborating with academic institutions around the world. There's no deadline for submission. **Prospective authors of IISTE journals can find the submission instruction on the following page:** http://www.iiste.org/Journals/

The IISTE editorial team promises to the review and publish all the qualified submissions in a **fast** manner. All the journals articles are available online to the readers all over the world without financial, legal, or technical barriers other than those inseparable from gaining access to the internet itself. Printed version of the journals is also available upon request of readers and authors.

IISTE Knowledge Sharing Partners

EBSCO, Index Copernicus, Ulrich's Periodicals Directory, JournalTOCS, PKP Open Archives Harvester, Bielefeld Academic Search Engine, Elektronische Zeitschriftenbibliothek EZB, Open J-Gate, OCLC WorldCat, Universe Digtial Library , NewJour, Google Scholar