IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 10, Issue 2 (Mar. - Apr. 2013), PP 46-49
www.iosrjournals.org

SQl Injection Protector for Authentication in Distributed Applications

Mrs.R.Velvizhi,
PG Scholar M.E Computer Science IFET Engineering College, Villupuram.

Abstract: *In today's information age, information sharing and transfer has increased exponentially. The treat of an intruder accessing secret information has been an ever existing concern for the data communication experts. Cryptography and steganography are the most widely used techniques to overcome this threat .Web application has been developed with very rapid progress. Security vulnerabilities due to amendment of intruders and hackers become predominant in the current trends. The work of this paper proposes a technique using hash value of user name and password,to improve the authentication process. We have built an prototype,SQL injection protector for authentication (SQLIPA).In addition to the proposed hash technique we are trying to conceal the logged in information using chaffing and winnowing technique in a stenographical image. These images will be stored as file stream by an encrypted layer in the backend to hide the tuples used for storage in a distributed environment. Validating the XML content with typed dataset will scrutinize the input data further associated with XSD filtration.*

Key Words: *Security, Cryptography, Stenography, SQL Injection Protector for Authentication, Hash Technique.*

I. Introduction

The objective of this project is to propose a new system model which will guarantee a system where the user couldn't hack the data. Our systems provide solution for most of the possible SQL attacks. The scope of this project is to detect the SQL injection attacks at presentation, business and database levels. The SQL attacks can be prevented by anti spoofing technique. The XSD validation also done to avoid the hackers to access the data.

This paper proposes a SQL Injection detection method by comparing the static SQL queries with the dynamically generated queries after removing the attribute values. The paper compares our method with other detection methods and confirmed the efficiency of our proposed method. The proposed method simply removes the attribute value in the SQL queries for analysis which makes it independent from the DBMS.

The remaining part of this paper is formulated as, chapter II deals with Literature survey, chapter III describes the system proposed with testing, chapter IV concludes with future scope.

II. Literatire Survey

An authentication methodology that combines multimodal biometrics and cryptographic mechanisms for border control applications is discussed in [1]. The method described accommodate faces and fingerprints without a mandatory requirement of (tamper resistant) smart-card-level devices on e-passports for easier deployment. It is even allowable to imprint (publicly readable) bar codes on the passports.

Survey about the past decades and advancement in the area of database management systems shifts towards multimedia is discussed in [2]. Multimedia information is very expressive, self explanatory, narrative, etc. The growing of digital medias (digital camera, digital video, digital TV, e-book, cell phones, etc.) gave rise to the revolution of very large multimedia databases, in which the need of efficient storage, organization and retrieval of multimedia contents came into question. Among the multimedia data, this survey paper focuses on the different methods (approaches) and their evaluation techniques
used by many of recent research works on image retrieval system.

The paper [3] presents a detailed review on various types of SQL injection attacks, vulnerabilities, and prevention techniques. Alongside presenting the findings from the survey, it also denotes the future expectations and possible development of countermeasures against SQL injection attacks. This paper explains an extensive dealing of various types of SQL injection attacks, vulnerabilities, and prevention techniques were discussed in this paper.SQLCounter measures were covered in multi angles. And the drawback of this paper is that it covers all the items related to this topic and it's not implemented at any case. There is no clear strategy explained to overcome the issue.

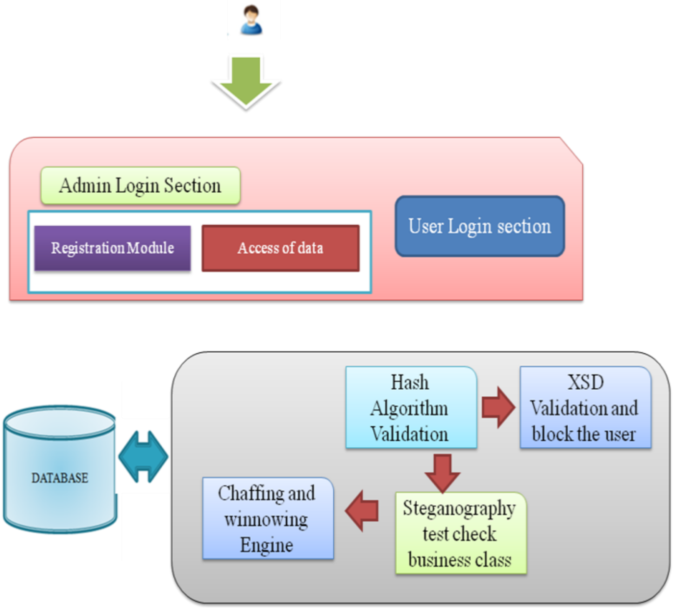
The paper [4] proposes security architecture to detect and prevent zero day attacks and techniques to deal with the polymorphic and metamorphic behaviour of the attacks. The entity validation component is used for capturing information of the operating system and applications running in the virtual machines, secure logging and detection of attacks that are generated with spoofed source address. The intrusion detection engine component is used for detection of known attacks and suspicious behaviour of the entities by monitoring the incoming and outgoing traffic of virtual machines. The dynamic analyzer is used for detection and validation of hidden processes, detection of zero day attacks and fine granular isolation of malicious process that is generating the attack traffic. After a zero day attack is detected, interactive VM technique is used to determine if the zero day attack exhibits polymorphic or metamorphic behaviour and develop attack signatures to deal with the attacks efficiently. This paper clearly emphasizes the secure logging and detection of attacks that are generated with spoofed source address.The paper [5] proposes a Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm which is a modified version of Data hiding in halftone images using conjugate error diffusion technique (DHCED). We use this DHOCD algorithm for proposing a new three phase visual cryptography scheme. DHCOD technique is used to hide an binary visual pattern in two or more ordered dither halftone images, which can be from the same or different multi-tone images. In proposed scheme we shall generate the shares using basic visual cryptography model and then embed them into a cover image using a DHCOD technique, so that the shares will be more secure and meaningful. This paper proposes a flexibility of using different multi tone images that can be used to do the encryption process. Decryption can be done by human without any decryption algorithm. The major demerit is that in the half tone image they didn't share the exact percentage of the first share and second share. No points specify the impact of using highest share by the individual partners and the encrypted images are still accessible to the user and this project doesn't give a strongest form of encryptions.

III. Proposed System

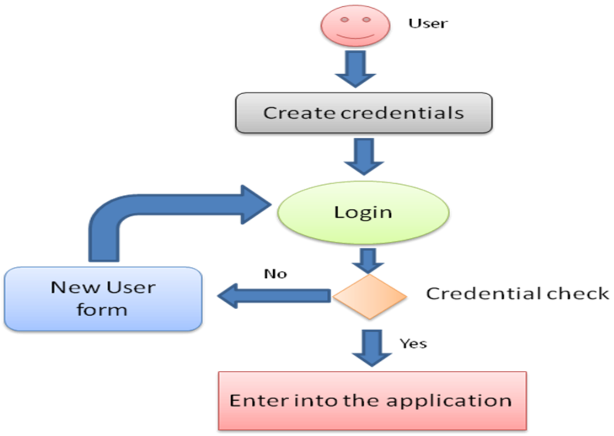
The Paper proposes a new system model which will guarantee a system where the user couldn't hack the data. Our system provides solution for most of the possible attacks. The techniques implemented in this system are too simple and strong. The proposed system tries to address some of the huge issues like, Spam bot attack which can be fixed up with Anti spoofing approach. The proposed system can overcome hacking at all the levels of the system based upon the classifications. If the hacker enters into the first level of authentication means hacking can blocked by using XSD validation and Hash key generation methods. The anti spoofing method and the winnowing and chaffing method to give the prevention from the hacking.

System Architecture

Login Module describes the interface implemented by authentication technology providers. Login Modules are plugged in under applications to provide a particular type of authentication. The user is allowed to create his credentials to login into the system. An admin module to approve the users created and login approval the user will be allowed to log into the system. Tautological way – In this type, the intruders will be injecting the data in the conditional statements. So that, the condition is always be true.Union way The intrusion data/query will be appended with the existing query by union operators. So that, the intrusion of your data will be achieved. , the algorithm to store the Image contents for an user is defined by the admin user. The images will be tagged based on the profile. The XML data transformed will be validated with the defined XSD model.


Admin Login Section
Registration Module
Access of data
User Login section
DATABASE
Hash Algorithm Validation
XSD Validation and block the user
Steganography test check business class
Chaffing and winnowing Engine

Authentication Module



Hash Module

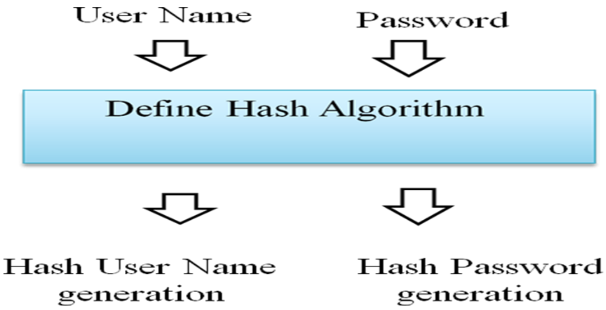
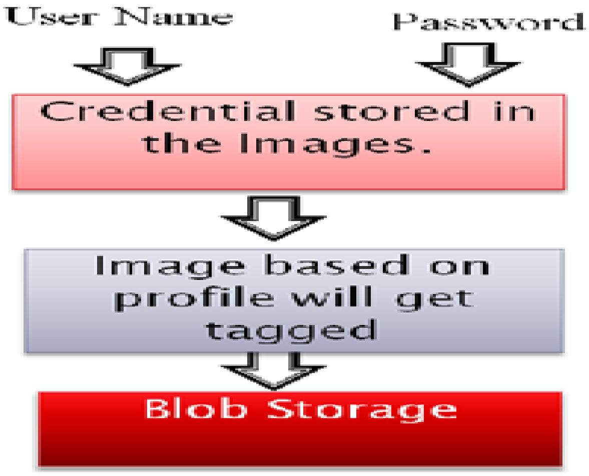
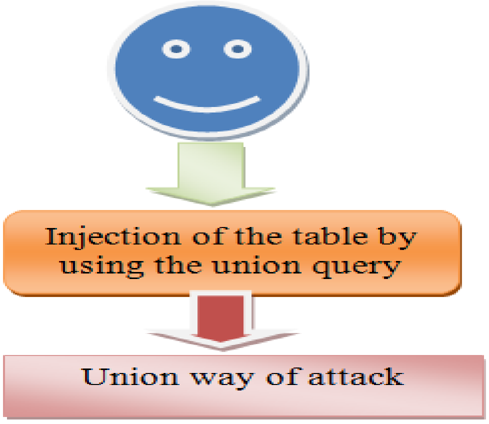


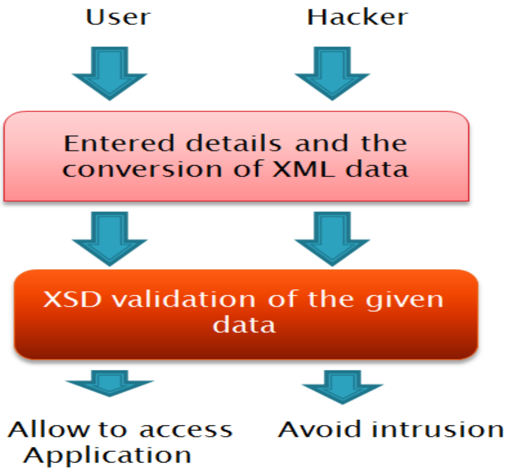
Image Authentication Module


User Name
Password
Credential stored in the Images.
Image based on profile will get tagged
Blob Storage

Union Hacking Module



XSD validation module


User
Hacker
Entered details and the conversion of XML data
XSD validation of the given data
Allow to access Application
Avoid intrusion

IMPLEMENTATION

Module describes the interface implemented by authentication technology providers; here the user is allowed to create his credentials to login into the system. An admin will approve the users created and login approval the user will be allowed to log into the system. Users can able to sign on because this associates content they create with their account and allows various permissions to be set for their roles.

Admin user will decide the type of security or hash value algorithm to be incorporated for the system. The hash value is being generated for both username and password of the user. Customizing the algorithm frequently will provide a secure system. Now in the second phase of authentication, we will evaluate the user's credentials with the steganographical password validation. The algorithm to store the Image contents for an user is defined by the admin user. The images will be tagged based on the profile. We are using the latest SQL Server technique to store the images in BLOB format using File Stream data type.

In Union Hacking module, the hacker will append the intrusion data or query with the existing by using union operators. So that the intrusion of your data will be achieved. XML data transformed will be validated with the defined XSD model. XSD format needs to be defined so that the data needs to be validated for their types and its value range.

IV. Conclusion

In this paper we have reviewed the most popular existing SQL Injections related issues. The proposed approach presents a new series of techniques to secure the authentication process of the database. Multi angle checks in securing the system with step by step process and data validation enable this system a more secure one. Concept of "Anti Spoofing" will avoid spams through automated machines. Data filtration using XSD schema provides an additional filtration at the data level. All the test cases were passed successfully. No defects encountered.

FUTURE ENHANCEMENT

We can implement the system to protect our database from session oriented hacking. The cookies level injection can be detected and avoid those type of hackings.

Reference

[1] Piyush Marwaha,Paresh Marwaha," Visual Cryptographic Steganography In Images" 2010 Second International conference on Computing, Communication and Networking Technologies.Infosys Technologies Limited,

[2] Taekyoung Kwon, Member, IEEE, and Hyeonjoon Moon, Member, IEEE," Biometric Authentication for Border Control Applications", IEEE transactions on knowledge and data engineering, vol.20,no. 8,august 2008.

[3] Yihun Alemu, Jong-bin Koh, Muhammed Ikram,Dong-Kyoo Kim, "Image Retrieval in Multimedia Databases: A Survey",Department of Computer Engineering, Ajou University South Korea, Suwon.

[4] Diallo Abdoulaye Kindy and Al-Sakib Khan Pathan ," A Survey On SQL Injection: Vulnerabilities, Attacks, and Prevention Techniques", Department of Computer Science, International Islamic University Malaysia, Malaysia 2011 IEEE 15th International Symposium on Consumer Electronics

[5] Vijay Varadharajan, Udaya Tupakula,"Security Techniques for Zero Day Attacks" Information & Networked Systems Security Research Faculty of Science, Macquarie University, Sydney, Australia

[6] IndiaDebashish Jena, "A Novel Visual Cryptography Scheme", IEEE International Conference on Advanced Computer Control, 2009.

[7] K. Kemalis, and T. Tzouramanis (2008). SQL-IDS: A Specification- based Approach for SQLinjection Detection. SAC'08. Fortaleza, Ceará, Brazil, ACM: pp. 2153 2158.