Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 8, August 2015, pg.246 – 258

RESEARCH ARTICLE

Multi-Level Security of Website: A Review of Use Multitier System with Many Password Encryption Method

Lecturer: **Hind Saleem Ibrahim Harba**
University of Mustansiriyah/ College of Science / Atmospheric Science
Email: hindharba76@yahoo.com

Abstract:** Multi-tier web server systems are used in many important contexts and their security is a major cause of concern. Such systems can exploit strategies. In this paper, a model was present based on three-tier architecture (Client tier, Server tier and Database tier) and applying multilevel security on it. The database server tier consists of the database and the database management system (DBMS) which has been built off-line to reduce unauthorized access to sensitive data. The Client tier is generally a web-browser that displays and processes web code. Web browsers are HTTP clients that interact with the Web servers using standard protocols); which is requests code from server and then processes the code. The Middle or application server tier consists most of the application logic. Inputs are receives from the clients tire and it interacts with the database but only the results sent to application server then to client. This achieved by using multilevel of security to protect database, using Authorization, Password Encryption. The process of authorization done by allowing the access to proposed system pages depending on authorized level; Password encrypted using bcrypt with fallbacks on sha-256/512 with key stretching to protect it from cracking by any types of attack. Client-to-Application Server Protocol (CAP) uses the RC4A algorithm to provide data confidentiality to secure transmitted information from application server to client.

***Keywords:** Authentication, Multi-tier model, Multi-Tier Security, Security, Data protection, Internet security.*

1. Introduction

Internet applications such as financial sites, online news, retail, have become ordinary in recent years. Nowadays, Internet applications are complex, which is in general, employ a multi-tier architecture and are distributed or replicated on a cluster of servers. These tiers are connect with each other directly or indirectly with a certain functionality in such way that makes successor to carry out its part of the overall request processing. For instance, a typical e-commerce application consists of three tiers a front-end Web tier that is responsible for HTTP processing, a middle tier, Java enterprise server that implements core application functionality, and a backend database that stores product catalogs and user orders. [1]

The three-tier architecture pattern provides a means of structuring and decomposing applications into three tiers or layers, where each tier provides a different level of responsibility. One tier deals with the presentation part of the system (user and system interfaces), another handles the business logic, being the core of the system, and the last tier is representing the data storage. Enterprise applications are typically implemented as three-tier architectures that consist of clients in the front tier, servers that perform the application business logic processing in the middle tier, and databases that store the application data in the back-end tier. [2]

This paper describes a method for design three-tier system and protecting its streamed data from possible security attacks. The main feature of the suggested design is its ability to provide a secure environment for real-time data or file downloading watching. One of security parts is to secure pages content, this done by used authorizing and authentication. Secondly, is to make password hashing very strong to prevent the password cracking by attacker. Thirdly, secure communication between Web browsers and servers this done by used RC4A with Secure Sockets Layer/Transport Layer Security (SSL/TLS).

2. Related Work

Wells et al. [3] made a Web servers performance analysis by used colored Petri nets. In their work, they made a model consist of three layers. The model includes several parameters, some are known and some are unknown parameters, which are determined by simulations. Doyle et al. [4] made a simplified analytical model to predict the Web services response time. Their model is a combination model of storage I/O and server CPU. The model are just applies for single tier and it's also valid just for requests of static content.

Rykowski, and Wieczerzyck [5] propose a new architecture for web servers. This architecture is of three-tier type, and it is composed of a query language interpreter as the interface to the server, a specialized object-oriented database of resources as an engine, equipped additionally with semi-transaction and user managers, and an XML wrapper as a gateway to data repositories.

He Liduo and Chen Yan [6] provide a technology of three-tier architecture with J2EE-based for Web Content Management System construction; their work aims to improve the effectiveness of maintenance, management and development in web applications.

3. Background

Multi-tier architectures are traditionally used for database applications. The middle tier separates presentation and business functions and its services allow communication between programs based on different technologies and programming languages. Different technologies for realization of the middle tier exist (e.g. transaction processing, message-oriented, object-oriented, and Web-based). They differ in communication protocols and service allocation [7].

Multi-tier architecture provides many benefits over traditional architecture of client/server [8]:

- Deploying and installing the user interface is practically instantaneous. That mean web interface in the middle tier are only needs to be updated.
- It is modify, maintain and easier to deploy applications everywhere clients are located.
- Because the application itself is server-based, users always access the most up-to-date version.

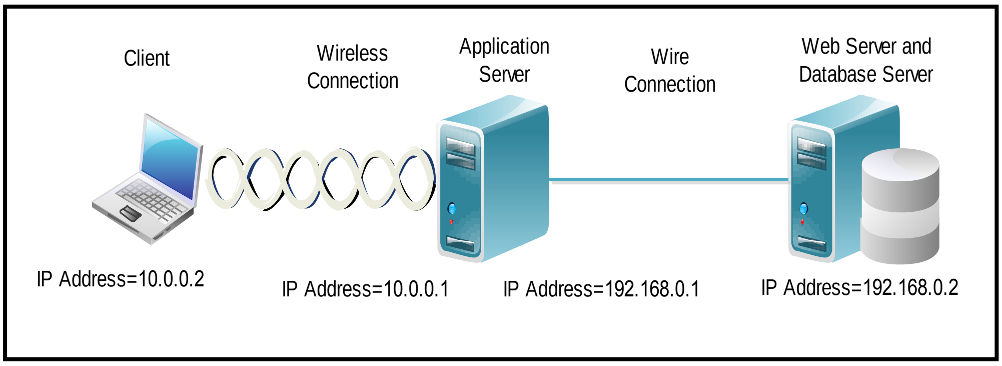
Today, providers of Web services use architecture of multi-tiered to provide required services. Commonly most Web applications use two tiers as Web server and database server, while sites with high volume are typically put a third tier that is the application server that used to support complex business logic and provides both high level of reliability and scalability. So, the 3-tiered architecture are most common deployed infrastructure of Web services, as shown in Figure 1[9].

In 3-tiered architecture, the Web server acts as the presentation layer, it has three functionalities: Firstly the Web server are receives clients requests (service static Web requests); secondly, the web server forwards requests of complex dynamic content to the second tier in the same time; Finally, it receives responses from the second tier and then sends it back to the clients. Typical PHP Web server includes Apache and Microsoft Internet Information Server (IIS). [10]

4. Architecture of the Proposed System

The system is constructed from three-tier (client-server architecture) to specify the application as shown in figure (1).

- Client tier: a web browser runs in any computer which is responsible for handling the information representation for user request.
- Application server tier: it resides in middle tier, where it handle the initialization and the updated information. It is responsible for receiving client request, processing the data contained in request and applying the client response for updating the demand information.
- Database tier: the backend database reside on web server side and stores the data for system, which is required by the middle tier.



Client tier	Middle tier	Database tier

Figure (1): Implemented network for the proposed model

All three tiers (in this model) are connected with special network which consist of wired and wireless networks.

The application server is the important part of the network which contain two interface card for interfacing with client computer in one side and with the database in other side. The client computer (IP= 10.0.0.2) connected with server computer (IP= 10.0.0.1) in wireless network with special group. But the server computer used wired network for connecting with database server as (server comp. IP= 192.168.0.1) and (database server comp. IP= 192. 168.0.2) in other group.

4.1 Client

In the client side the user of a web application can view data across the internet and into the web application. For the sake of simplicity, the assumption of a browser-based web application will be made. Static HTML pages are manipulated by the user and the data is submitted via an HTML request into the web application. Data specific to the user is submitted within this request through the use of HTML page. After the client is connected to web application the user identifies himself to the system by sending secret password. To ensure the authentication of this password hashing algorithm is used. Only authorized user can enter the system and view home page to request specific page (such as view order table) the user request is sent to web application and the client is waited a response which is encrypted by using RC4A algorithm therefore the client must decrypt the encrypted page using the same algorithm to enable user to view data.

4.2 Application Server

Application server can be defined as a program which is handles all application operations between clients (users) and backend business applications of organizations or databases. The typically usage of application server is for complex transaction-based applications. In this work, the middle tier is usually split recursively into three tiers again. The Client applications that run inside the browser submit requests to the web server using HTTP protocol/ The ‘presentation layer’ on the server transforms the request and passes it to the ‘business layer’ which will perform some computation by interacting with the ‘data layer’. The results from the ‘business layer’ are then transformed into HTML by the ‘presentation layer’ and returned as the response to the client. The most popular way of generating HTML responses in the middle tier is by using the server pages (shadow files). The server page is a special HTML page that contains embedded scripts.

4.3 Database

The main idea of a database that driven the web site is to permit the content of the site to remain in a database, also, it allow that content to be pulled dynamically from the database to create web pages or show content for people that have permission to view it.

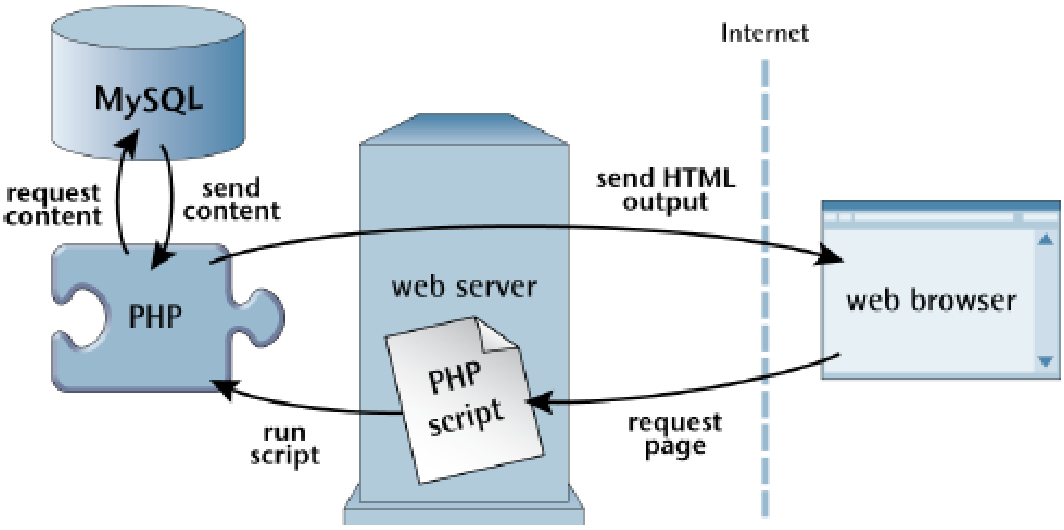


Figure (2) PHP retrieves MySQL data to produce web pages.

As shown in Figure 2, the PHP is the scripting language that processes the request of page and fetches the data from the database (MySQL database), after that it generate dynamically a nicely formatted HTML page that view in browser. When a person visits a page on database, driven web site the flowing steps is happen:

1. The client requests the webpage through web browser by used a standard URL.
2. The web server (which is software typically Apache) recognizes if the file requested is a PHP script, then the server fires up the interpreter of PHP to execute the code included within the file.
3. Commands of PHP connect to the database (MySQL) and requested the content that contained in the web page.
4. The database of MySQL has been respond by sending the content that has been requested to the PHP script, that stores content into one or more variables of PHP; output the content as part of the web page by uses echo statements.

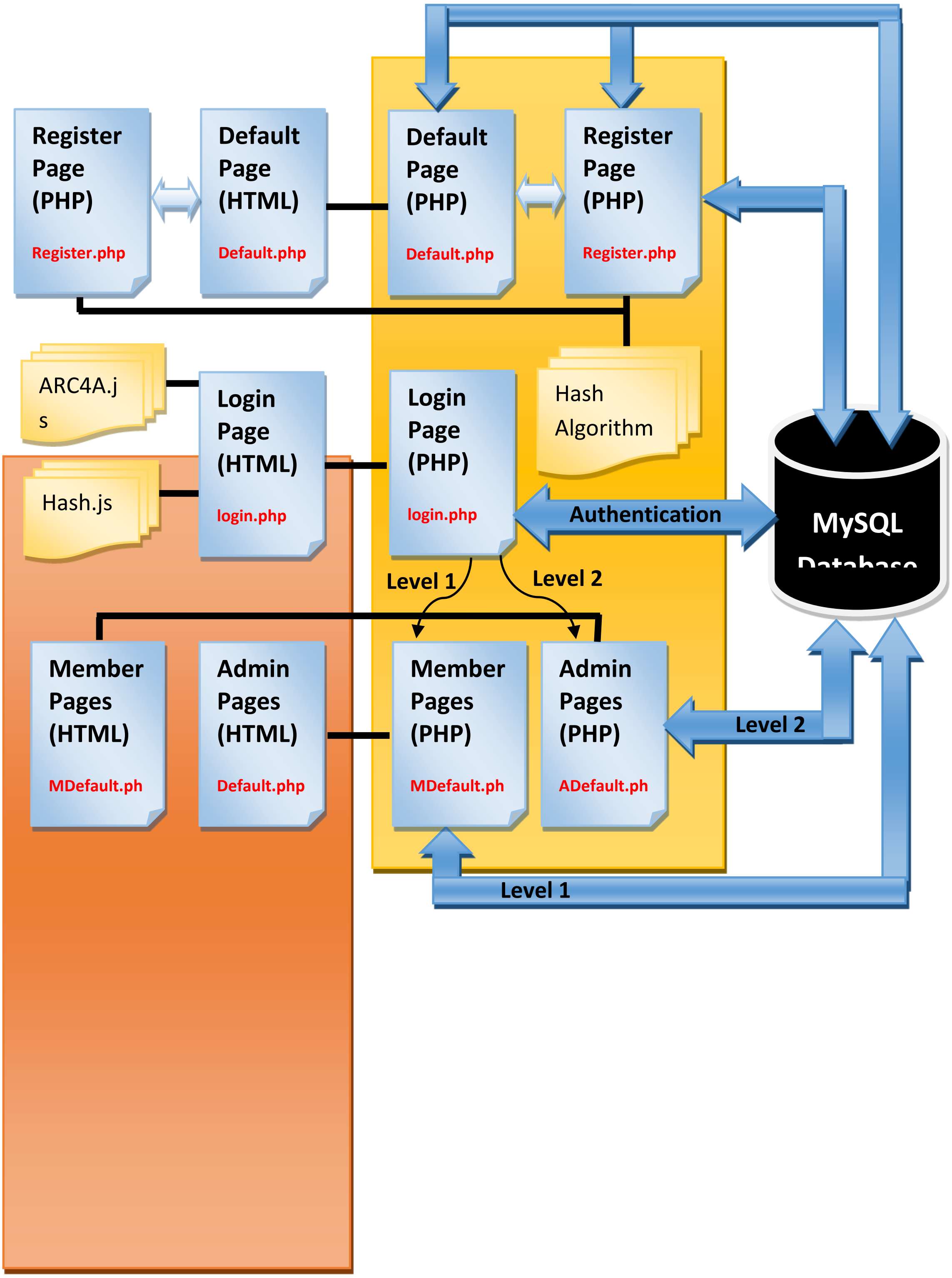


Figure (3): System architecture

5. System security

The security of system can be described as follows:

1- **Data Confidentiality:** The Client-to-Application Server Protocol (CAP) gives a standard method for multi-protocol datagrams transporting over client to application server links. The CAP uses the RC4A algorithm to provide data confidentiality. The process of sending encrypted information is from application server to client to configure secure channel and this information is decrypted in client.

2- User Authentication and Authorization: Site Authorization is used to determine the level of user (visitor, member or administrator). The visitor can view the books content but cannot view or buy books but only the activated members have ability to view allowable books or buying not allowable books. In order to view member library user needs to enter authentication process to redirect to the member library.

3- Password Encryption: This method is used to encrypt user password transfer from client to server and then storied in MySQL database to protect them from being stolen or attacked from different attacks (SQL injection, Dictionary and Brute-Force Attack, Lookup Tables, Reverse Lookup Tables Rainbow Table, etc.), this is done by hashing password using BCrypt and salt.

4- Disabling Browser Caching: The Method used to bypass, clear, and disable browser cache so that each time client visit a page all the files are freshly downloaded.

5- HTTP over Secure Sockets Layer (HTTPS): It gives authentication of the website and associated webserver that client communicating with it. HTTPS provide a protection against Man-in-the-middle attacks. In addition, it also provides bidirectional encryption of communications between server and client that protects against tampering and eavesdropping with and/or forging the contents of the communication. Thus, it provides a sensible guarantee that when client is communicating with the website, the HTTPS ensuring that the communications contents between the visitor and site cannot be read or forged by any third party.

5.1 Data Confidentiality

The Client-to-Application Server Protocol (CAP) provides a standard method for transporting multi-protocol datagrams over Client to application server links.

Cryptography is the method used to provide security services in many applications. Many researches on cryptography has exploded and a many algorithms and techniques of cryptographic have emerged. RC4A is one of them.RC4A, an RC4 family algorithm designed by Ron Rivest for RSA Data Security, Inc. in 1987, developed by S. Paul and B. Preneel they have been tried to increase security without decreasing efficiency. Their work mainly takes two instances of RC4 and made crosses information between them. RC4A stream cipher works in two phases, KSA (Key Scheduling Algorithm) phase and PRGA (Pseudo Random number Generation Algorithm) phase. During PRGA two successive output byte are generated. The aim of usage RC4A was to rise security firstly by increasing the internal algorithm complexity. RC4 used in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards that have been define for communication between Web browsers and servers. [11]

In proposed, the CAP uses the algorithm of RC4A to give confidentiality of data. The session key length that be used for initializing the encryption tables can be negotiated. CAP currently supports 256-bit session keys. RC4A is a symmetric key, stream cipher algorithm. The same algorithm has been use for both encryption and decryption as the stream of data is simply XORed with the sequence of generated key. The stream key is completely independent on the plaintext that used. It initialize a 256-bit state table by uses a variable length key from 1 to 256 bit. The state table has been use for pseudo-random subsequent generation of bits and then uses to generate a pseudo-random keystream, which is give the ciphertext by XORed it with the plaintext.

The sequence of bytes generated is not random since the output is always the same for a given input but it has to approximate random properties to make it harder to crack. The process of sending encrypted information is from application server to client to confm igure secure channel and this information has been decrypt in client.

5.2 User Authentication and Authorization

The proposed system offers three main user levels:

- *Visitor Level*, which allow all user to enter the site and view book content but not have the ability to view or buy books.
- *Member Level*, allow just for member users to show the full allowable books and the ability to buying not allowable books, but cannot access administrator pages.
- *Administrator Level*, which has the ability to access to all site content beside the ability to manage the site (i.e. add or remove members and edit his information) or books content

5.2.1 Passwords Hashing

Passwords are a notoriously weak authentication mechanism. Users frequently choose poor passwords. An adversary who has stolen a file of hashed passwords can often use brute-force search to find a password p whose hash value H (p) is equal to the hash value stored for a given user's password, thus allowing the adversary to impersonate the user. [12]

Hashing passwords with direct MD5 (even it is storing passward) is not recommended [13], this due to the MD5 is an older algorithm which it is hash-pool is smaller (32 characters, but not all combinations are possible). SHA1 is a little better. It is a new algorithm, supposedly has less collision, which has a larger pool (about 40 characters) and it has a higher percent of possible combinations).

In the proposed system, PHP hash (bcrypt) Passwords with random Salt have been used.

5.2.2 Bcrypt Algorithm Scheme

It is an algorithm of hashing, which is amenable with hardware (by a configurable number of rounds). Its multiple rounds and slowness that ensures that an attacker should be deploy massive hardware and funds to be capable of cracking the passwords. Adding bcrypt to that per-password salts it will definitely sure that the attack is practically infeasible without either ludicrous amount of hardware or funds.

The bcrypt has uses the algorithm of Eksblowfish to hash passwords. Whilst the Eksblowfish encryption phase and Blowfish are same, the Eksblowfish key schedule phase are ensures that any subsequent state are depend on both salt and key (user password); thus, without the knowledge of both (password and salt) there is no state can be precomputed. Due to the difference of key, the bcrypt is a one-way hashing algorithm that cannot retrieve the original password (plain text password) without already knowing the key, rounds, and salt (password).

5.2.3 System Password Algorithm Scheme

The proposed system uses a proper implementation of encryption by used bcrypt and fallbacks on sha256-512 with key stretching.

Password Encryption Algorithm

```
Input:    Password Characters ($password)
Output:   Encrypted Password Characters

Step 1:   Start.
Step 2:   Create hash using Blowfish hashing with a salt is as follows:
          $2a$" + a parameter of two digit cost + "$" + 22 digits from the base64
          alphabet "./0-9A-Za-z" + "$"
Step 3:   Create a new salt string which conforms to the requirements of
          CRYPT_BLOWFISH.
Step 4:   Fall-back SHA512 hashing algorithm with stretching.
Step 5:   Generates the password and verifies functions.
Step 6:   End.
```

In other word, after a user enters their ID and password, proposed system needs to take the user’s ID and checking a database to determine if the account are exists or not. If the user account are exists, then it will get the user’s password (hashed password) that storied in database. With the returned hash, it then the user input password will pass through encryption algorithm to get the hashed password and then it compared with the returned encrypted password from the database to find the similarity. If the two are the same, the user will be authorized to enter the pages. If not it will not permit to user and error message will appear.

5.3 Disabling Browser Caching

In browser caching the visited pages and files are stored in hard drive (HDD) and when the users visit same pages it will be load from the HDD rather than downloaded it from the Internet. This method is a beneficial feature because it makes web browser run much faster. However, browser caching sometimes are undesirable which may cause missing updates on a webpage that may changes frequently. If the cache is disabled, the browser is instructed to not save page content and will request it anew from the server. From a security perspective the cache should be disabled, so the browser does not store sensitive data and will always request pages from server if the URL changes. There way used around this. It could be clear, bypass, or even disable web browser cache so that each time user visit a page all the files are freshly downloaded.

- **Meta Expires**
  The following tag is used to expire the content immediately:
  <META HTTP-EQUIV="expires" CONTENT="0">

The above tag is also said to disable caching so that search engines will load a new copy of the site from the server every time an end user visits the site.

5.4 Secure Sockets Layer Authentication

Secure Sockets Layer (SSL) is a developer's tool for securing the transmission of data. A trusted certificate installed on the Web server offers visitors that good feeling of a secure environment. In the proposed system, a client (web browser) was authenticating themselves to server (server application or website), also that server are authenticating itself to the client by verifying the digital-certificate/public-key certificate issued by the trusted CAs (Certificate Authorities). The general process of establishing an encrypted channel and authenticating by using SSL involves the following steps: (as show in figure 3.8)

Step 1: Satrt
Step 2: A client requests access to server that includes a protected resource.
Step 3: The server attends its certificate to the client.
Step 4: The client verifies the certificate of server.
Step 5: If the verification successful, the client sends its certificate to the server.
Step 6: The server verifies the credentials of client.
Step 7: If successful, server will give access to client to the protected resource requested.
Step 8: End.

This SSL authentication has to great advantage that even hackers try to attack server he/she cannot access to the certified pages (like login page and member ship pages) without having the digital certification. In addition, the big advantage of using SSL is that all that data are protected (like passwords, information, videos, etc…).

6. Possible Attacks on Passwords and Their Solution

The common practice to store user passwords in a hashed form instead of the clear text has been from long time. For many years, hash-algorithms like (MD5 and SHA-1), have been used to encrypt password which is the preferred methods in that time, but now days it is not favored, this because they have well-known vulnerabilities(apart from lazy and inept people who are using passwords that are too short and simple to stand against educated guess). Instead, there are many recommend algorithms used to encrypt password (such as SHA-2), because it has no known exploitable vulnerabilities.

A function of SHA-2 is a one-way cryptographic algorithm which get input with variable length and calculates a value that is unique for the specific set of data (e.g. file or string). The hash value are not possible reverse to reveal what the original value was. Thus, when user need to pass to pages, the input passwords will hashed with the same algorithm that used for user password in database and then verify with the stored hashed password in the database, So if the two hash values are identical it means that the right password was given and use may login. For example, if the password is 'secret' the hash value (SHA-256) is '2bc80w537bqda3ee81d30261ak853696bdp0eaxd7132fes6q25fe9 7bf527a25b'. User databases get hacked all too often.

6.1 Cause of Problem

While hashing is a perfect method to protect a password from the eyes of unauthorized persons, they can be vulnerable against brute force attacks. Nowadays the components of computer are simply efficient and so fast that makes brute force attacks (where every each possible combination will continue tried until reach the right characters combination is found) have become quite reasonable option for attackers.

Brute force attack in these days are used utilizes GPU rather than traditional CPU, this do to instead of use password recovery tool that used CPU in processing (which takes about a year to crack an eight-character password), a similar password recovery tool that use GPU in processing could do the same trick in less than a day. In another words, an old gamer's desktop computer with simple software tool could crack a list of typical hashed passwords within days or hours, if not in minutes. For example ATI Radeon 5770 can crack a password with five-character under one second and seven-character password in about 17 minute while a typical CPU might be do the same in about 24 seconds with five-character password and around 90 minutes and four days for seven-character password. The respective times for a typical CPU would be, or so. A cheap ATI Radeon HD5450 can handle about 126 million MD or 552 million SHA1 hash computations per second. Rise up to ATI Radeon HD5970 it would doing about 5631 million MD5 or 2320 million SHA1 calculations per second, which they are single GPU. Most desktops can have two linked GPUs and high level can reach to 6 GPUs.

6.2 System Solution to prevent password attacks

Apparently there are no guarantees to prevent attacks, but there are ways to thwart almost attackers by make them reach to a point when the reward isn't worth the trouble. Generally, the best protection for user is not just use hard hard to remember passwords (i.e. password with numbers, special characters, caps like #fK1~2), but simply the efficient way is to use longer passwords. To explain that, if the system is using ASCII, which has 95 printable characters, the each character of the password multiplies the number of possible combinations by 95. So, to make strong password the developers should use hashing algorithms like SHA-2, SHA-3 and hard it by use Bcrypt.

The Bcrypt is a variant of Blowfish which has an important advantage from other hash algorithms that it can be made attack very expensive to use, this due to that most hash algorithms have been optimized to increase calculation of hash value for data with large sets of data (i.e. >10 character passwords) as fast as possible, this property are great when needs to find out if two large data sets are identical, but its be a disadvantage when dealing with passwords less than 10 character. For that reason, Bcrypt has been designed to be slower rather than be faster when calculating the hash which makes attacking (like brute force attack) be slower and needs to increase the expense of as a single hash calculation that makes it takes milliseconds or maybe rise to seconds instead of takes microseconds. This not effect on user doing login or register because it is not perceptible, but for cracking password will be very long process. Thus, if combined bcrypt with long unobvious passwords it will be seriously frustrate brute force attacks based on GPU.

The other important property using bcrypt is that it can be accommodate to Law of match Moore's: the bcrypt has a work factor that it can be increased freely as computers be faster. The bcrypt is supported by many programming languages. Additionally, the proposed system can be increase the strength of encryption by using bcrypt with fallbacks on sha-256/512 with key stretching.

7. Conclusion

This work has reached to the following conclusions

1- The three tier architecture of the proposed system plays the basic role of database security because the client does not have a direct access to the database server connect to it across the middle application server (active server) especially when using LAN network (off-line connection) between the two servers.

2- Using disable caching is more important because the stored files are loaded from the hard drive instead of being downloaded from the Internet. This is a useful feature because it makes the Web surfing much faster.

3- The Client-to-Application Server Protocol (CAP) provides data confidentiality by using the RC4A algorithm.

4- Using bcrypt to that per-password salts make attacked much more difficult, because it have been sure that an attack is virtually unfeasible without either ludicrous amount of funds or hardware.

5- Password encrypted using bcrypt with fallbacks on sha-256/512 with key stretching to protect it from cracking by any types of attack.

References

[1] Bhuvan U., Giovanni P., Prashant S., Mike S., and Asser T., “An Analytical Model for Multitier Internet Services and Its Applications”, SIGMETRICS’05, Banff, Alberta, Canada, June 2005.

[2] Mumtaz A. and Sarmad H., “Developing a Three-Tier Web Data Management Application for Higher Education Admission Environment”, International Arab Journal of e-Technology, Vol. 2, No. 4, June 2012.

[3] Wells L., Christensen S., L. Kristensen M., and Mortensen K. H., “Simulation Based Performance Analysis of Web Servers”, 9th International Workshop on Petri Nets and Performance Models, 2001.

[4] Doyle R., Chase J., Asad O., Jin W., and Vahdat A., “Model-Based Resource Provisioning in a Web Service Utility”, presented at USITS, 2003.

[5] Te-Kai L., Santhosh K., and Jen-Yao C.,” Performance Engineering of a Java-based e-Commerce System” Proceedings of the 2004 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE’04), Taipei, Taiwan, pp.33-37, 2004.

[6] He L. and Chen Y., “Design and Implementation of Web Content Management System by J2EE- based Three-tier Architecture”, 2nd IEEE International Conference on Information Management and Engineering (ICIME), Zhengzhou, China, pp.513-517, 2010.

[7] Diane C. and Sajal D., “Smart Environments: Technology, Protocols and Applications”, Wiley Inc., ISBN: 0471544485, pp. 101-127, 2004.

[8] Oracle Technology Network, http://java.sun.com/products/jsp/ JavaServer Pages.

[9] Ramesh N., Robert S., Rima P. S., “Developing Java Web Services: Architecting and Developing Secure Web Services Using Java”, Wiley, ISBN: 0471236403, 2005.

[10] Douglas K. B., “Web Services, Service-Oriented Architectures, and Cloud Computing: The Savvy Manager's Guide”, Elsevier Science Inc, ISBN: 9780123983572.

[11] Abdullah A., Roslina S. and Abdul Rahman R., “Hardware Implementation of RC4A Stream Cipher”, International Journal of Cryptology Research 225-233, 2009.

[12] Kevin J., “What is hashing”, Thycotic Software Ltd., (2007).

[13] Chi-Chaochang and Tzonelih H., “Modular Design for Round-Oriented PasswordAuthentication Protocols”, Journal of Information Science and Engineering 22, 1295-1308, (2006).