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. 4, April 2015, pg.114 – 129

RESEARCH ARTICLE

STREAMING MEDIA: RISKS AND SOLUTION DESIGN A SECURE STREAMING SYSTEM

Assistant Lecturer: Samera Shams Hussein

University of Baghdad / College of Education Ibn AL Hiathum / Department of Computer Science

E-mail: sameraalshalal@yahoo.com

Abstract

Media streaming over internet is compelling for popular data shared in the Web, and the protection of it via security techniques is of vast interest. The video data creates security risks as data is moved over internet. This paper will cover generation architectures of security on the Video (Motion Picture + Sound) streams applied in order to achieve high security level of video transfer through the web. We present a secure video streaming website to securely transfer the valuable multimedia video streams on the internet using the Authorization, Password Encryption, Path Encryption, and Video Encryption. The process of authorization has been done by allowing the access to web pages or videos depending on authorized level; Password encrypted used hashed with salted algorithm to protect it from cracking by any types of attack. AES (Advance Encryption Standard) algorithm is used for both video & path encryption, and then encrypted data is embedded into the website. After undergoing all these processes, the data is finally traveling over the internet media in secure ways . The site was tested experimentally through multiple tests including site security tests, password cracking tests and finally site performance and video streaming tests. As a result, we hopefully tend to apply the best possible security on video streams traveling among the internet.

Keywords: Media streaming, video streaming, media streaming risks, password encryption, video encryption, Internet video security

1. Introduction

Streaming media is a sequence of "moving images" that are sent in compressed form via the Internet and received by the viewer to display it as they arrive. It is simply, a technique for transferring data such that it can process as a steady and continuous stream and it called streaming. Streaming media is streaming video with sound. With streaming media or streaming video, a Web user not need to wait download a large file before hearing the sound or seeing the video. Rather than that, the media (video or audio files) is sent in a continuous stream and can be view directly as it arrives. For viewing streaming media the user needs a player, which is a program that receiving compressed media that transfer by streaming process and uncompressed it then sends video data to the display. A player program can be either downloaded from the software maker's website or it an integral part of a browser. In streaming mechanism, the file sent to the end user in a (more or less) constant stream. [1]

Streaming visual data to different users is becoming increasingly popular in recent times, and protecting the transmitted data from every possible security threat has become one of the main concerns both for the end users and data providers [2]. Functionally, there isn't a big network security risk with streaming video or audio itself, but there are inherent risks in some site interaction like authentication scam to stolen password (Users are often scammed into clicking on a link in an email to view fake site like the origin to put his password to stolen it), man in middle attack to stolen information that transfer from client to server, SQL injection to stolen data base data etc.

A Cryptographic hash function [4] is used for the encryption of password where it can't be decrypted. Hashing algorithm used is a combination of (MD5, SHA384, and SHA512) depending on site manager entry that can change the way in each time and it merge hash with salt [5] to give strong protection for password.

A computer security standard Advance Encryption Standard (AES) [6] is used for the encryption and decryption of data where the cryptography scheme is a symmetric block cipher that encrypts and decrypts data using 128 bit key. As an efficient encryption standard, it is currently being deployed on a large scale.

This paper describes a method for protecting streamed data from possible security attacks and suggests a design of secured system architecture for multimedia video streaming to multiple receivers (one receiver at a time) considering the state of the art for the video streaming existing today. The main feature of the suggested design is its ability to provide a secure communication environment for real-time data or file downloading watching

2. The Proposed Architecture

Basic network architecture of secure media streaming is client-server based. There are two major implemented modules of this network architecture (as shown in figure 1):

- Video Streaming Server
- Client Computer

In server side there is a site designed in ASP. .NET used visual C# .NET with three levels of accessing video content. These levels are:

- *visitor level*, which allow all user to enter the site and show allowable video content,

- *member level*, allow just for member users to show the full content except the
- *special contain*, which it need from member to either put a key to view video file in real time streaming or to download encrypted video file and then use **the Proposed Decryptor** program to decrypt video file after put the password of that encrypted video.

In addition the *member level* and *special level* run with secure connection with SSL authentication.

The responsibilities of Video Server are to register or authorize users, to verify their identity, to allow them to make request for data they require, only member users that has the permission to access to special level can view or download the special video files. Here, we opt for the instantaneous view of video file application by using bit –by- bit transfer of data in real time streaming or using HTTP streaming to download encrypted video file and view it in client side after decrypt it. To view this application, the pre-existing players witch is Adobe Flash Player was used. This application allows the user to upload and, download video files. Once the client get registered to Video Server, it can avail all the features of application, it can ask for any available video file from server and can get it with full confidentiality and without any fear of data theft on the network. SSL authentication used so that client (web browser or client application) authenticating themselves to a server (website or server application) and that server also authenticating itself to the client through verifying the public key certificate/digital certificate issued by the trusted Certificate Authorities (CAs).

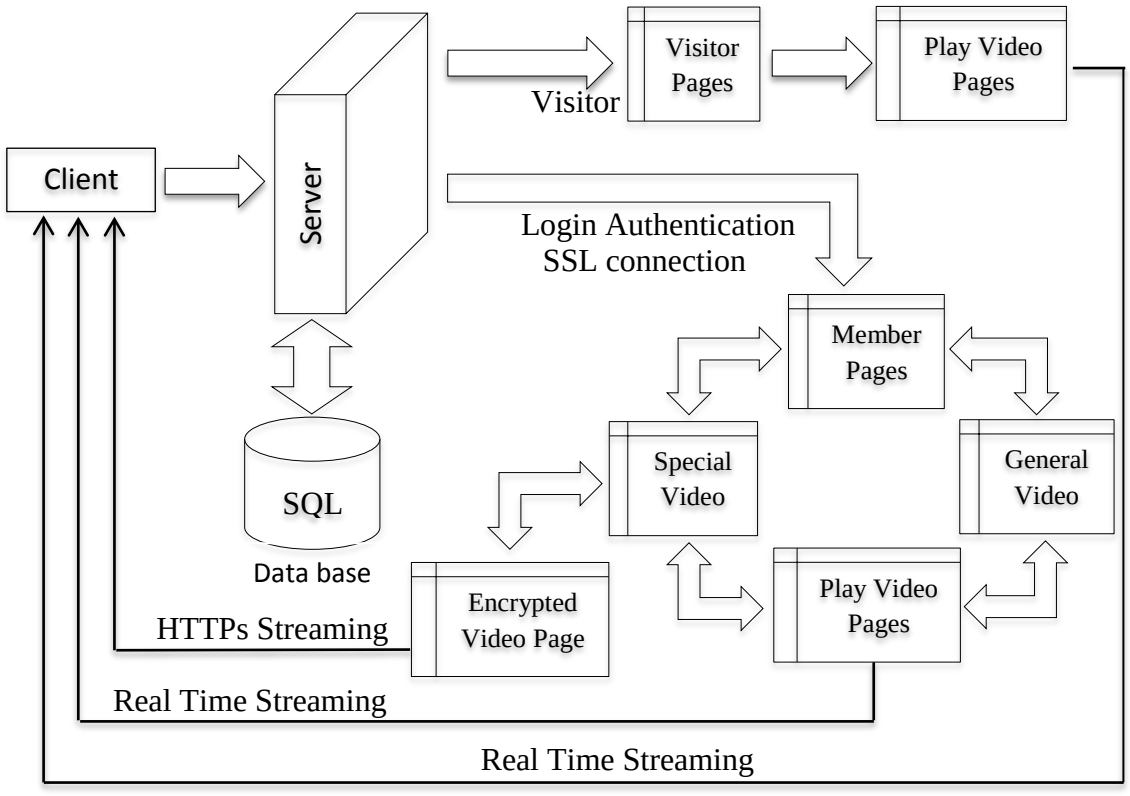

Figure (1): The Proposed Secure Media Streaming Architecture

The security has been described as follows:

1- **User Authentication and Authorization:** Site Authorization used to determine the level of user (visitor or member) the visitor can access to obtainable video library but cannot access to member video or special video just activated member have an access to member video and special video, to view member library user need to enter authentication process to redirect to member library.

2- **Client-Side ID-Password Encryption:** This method used to encrypt user ID and password that travel from client to server to protect them from (Man-in-the-middle attack), this done by hashing password using SHA1 and salt.

3- **Server-Side Password Encryption:** This method used to encrypt user password that store in SQL database to protect them from stolen or attacking from different attacks (SQL injection, Dictionary and Brute-Force Attack, Lookup Tables, Reverse Lookup Tables Rainbow Table, etc.), this done by hashing password using SHA512 and salt.

4- **URL Video Encryption:** This method used to encrypt path of special video that stored in SQL database, the bath of video encrypt using AES algorithm in process of video uploaded, the video path will be unknown till decrepit it. The member user request special video will redirect to switcher page, switcher page included URL condition if the user input the video password then it will be appear the video link, either it will appear error message. Video password will be send to member by e-mail after sending request to administrator to allow or not allow that member from view video.

5- **Video File Encryption:** This method used to encrypt video file that stored in site, the video file encrypt using AES algorithm in process of video uploaded, video extension will be (.encrypt). The member user request special video will used http streaming to download this video, and after that he/she used decryptor program that provide from site to decrypt video file after entering video password that request from administrator.

3. User Authentication and Authorization

In the proposed user authentication-authorization, has given main attention. There are three levels of video accessing: obtainable video, membership video, and protected video (special video). Visitor allowable to access to obtainable video, authorized client (member) can access to both obtainable video and membership video, member can also access to protected video library but cannot view this video until having video key that sending to him by e-mail after request this password from administrator.

When being as member of the server, member will needs to provide some of its confidential information to server like Name and Identity card number etc.. Server will stores all the information, maintains a complete log of all registered users that waited from site manger to activate there accounts after checking their information, and each time they try to login, they are verified by their existing information like user name and password.

4. Client-Side Password Algorithm Scheme

For encryption in client side, a Java Script to do encryption used, but it has big disadvantage that JavaScript source code can view in a web browser so it's not secure because it can be then used by hacker to decrypt encrypted password. For the proposed method, three values P, S, H used. P is the user password, S is the salt value request from server and H is hash value generated. User input the password P, browser request S from server and then generated H, in server the same operation run to store hashed value for same S value to decrypt the hashed value sending from client. For this method even hacker captured the encrypted values, they would be worthless because the salt value changed in each request and its value must be the same in server and client side so it will be used to executed the user password again.

SHA1 hash algorithm used to encrypt password. Client input his password (Let's say A), server generate random number (salt) and compute SHA1 algorithm of the salt and then send the same salt value to client, browser compute SHA1 algorithm of the password and salt and generate a value (Let's say B). Browser sends this value again to server, then these two hashes (A & B) subtracted to extract the user password value then use this password in Server-Side Password Algorithm.

5. Server-Side Password Algorithm Scheme

In the proposed secure media streaming system used a salt hashed password with salted algorithm to encrypt password. This password algorithm scheme employs the following steps to secure the use data:

Password Encryption Algorithm

Input:	Password Characters
Output:	Encrypted Password Characters

Step 1: Start.
Step 2: Used the encryption algorithm (SHA-1). This function takes an input string and generates a one-way hash using the "SHA512CryptoServiceProvider" algorithm.
Step 3: Generates a truly random number between 8 and 24 using RNGCryptoServiceProvider Class. This will used to determine the length of the random salt.
Step 4: Using this variable length, it then generates a random salt.
Step 5: Next the user input is encrypted using this variable length random salt bytes using SHA512 crypto algorithm. In addition, the algorithm performs 1000 (or more) passes over the hashed output to provide a higher level of security.
Step 6: Generate the password and verify functions.
Step 7: End.

In other word, the encrypt functions do a few steps. It first converts the user input string to bytes. It then inserts the un-encrypted salt bytes at the beginning of the user bytes. Next, using the SHA512 crypto algorithm, it runs a 100 passes over the (salt+input) byte array to generate a strong hash.

Next, it appends this variable length random un-encrypted salt to the hashed encrypted (salt+input) byte array and also sets the first byte to hold the length of the salt. Finally, it converts this to a Base64 encoded string and returns it to the user.

6. Reverse Turing Test Algorithm Scheme

A reverse turing test is a Turing test in which the objective or roles between computers and humans have reversed. Conventionally, the Turing test conceived as having a human judge and a computer subject, which attempts to appear human. [7]

The idea of Reverse Turing is to prevent using web bots by spammers which is used to automatically post form data in order to login (for sending spam). The text in the image usually distorted to prevent the use of optical character recognition software (OCR) to defeat the process. In the proposed system, the code presented produces only an image and had no code to generate an audio file.

This Reverse Turing test employs the following steps to build image test:

Step 1: Text-Image Class: creates an image for given parameters for the text to be display. This steps can be classified in follows:

a. Creating a new 32-bit bitmap image.
b. Creating a graphics object for drawing.
c. Setting up the text font and adjusting the size of font until the text fits within the image and Setting up the text format.
d. Creating a path by using text and randomly warp it.
e. Drawing the text with adding some random noise.

Step 2: Linking Reverse Turing test with page post back

a. Creating a code randomly and save it in the Session object.
b. Checking the user input on a postback,.
c. Verifying user input to pass or pop up error message.

Possible Attacks on Passwords and Their Solution

The most attack for encrypted password is the Dictionary and Brute Force Attacks. In web sites that used MD5 or SHA-1 as algorithm to encrypted passwords the hash value of password that stored in database has a fixed value i.e. if the another users entered same password the hash value it's the same, so it can be crack by compare that value with stored value in attacker database. The previous researches have been proved that these algorithms are unsafe and it should not be used.

The solution for the above problem in this proposed system is by used salt bytes with SHA512 crypto algorithm. In addition, the algorithm performs 1000 (or more) passes over the hashed output to provide a higher level of security. The password that entered from user through registration encrypted using The Proposed cryptographic hashing functions that give strong security of user information because the password that stored in database is encrypted and no one can know the password even reach to data base also it's so difficult to brock that encryption even the password is weak.

Table 1 explains the two methods of encryption: (a) by using MD5 algorithm to encrypt password, it show that for two users that enter same password value, the hashed value that generate is the same, so it can cracked. (b) by using proposed method that used a hashed password with salted algorithm to encrypt password, it show that for two users has the same password value, the hashed value that generate is

random and variable length, and the value is different each time so it's too difficult to cracked this password.

Table (1) Hash values for MD5 Password Encryption and encryption method

(a) MD5 Password Encryption

Username	Password Value	Password Hash Value
Samera	Samera1212	kDsBarLuiDBUathFPYSbuw==
Mohammed	Samera1212	kDsBarLuiDBUathFPYSbuw==

(b) Password Encryption

Username	Password Value	Password Hash Value
Samera	Samera1212	25wIzWNW2L8VIu9MxuOv0lRNxJXoyAbTBiopMsT6V2g/wNtUYn41OM8uNLc8HKTQwj0LpHD/B/DLlnhCjcnNHyW8uCSm
Mohammed	Samera1212	fnG7QRkqjo2BIG4nGu0yOYz7LtWRct1GwvThod0RSiEf/+JCFlabRPEgswFK+cLqf3Psrj3g4hGcNdVN37JSgZM3gJ09Ww==

In follows, we apply most attacks that used to crack password to proven the password encryption method is too strong and much more difficult to crack.

SQL Injection

It is a technique commonly used to attack a website. This is done by inserting portions of SQL statements into the entry field of the web form in order to make the website pass a newly formed rogue SQL command to the database (e.g., dump the contents of database to the attacker).

SQL injection is a technique of code injection that use security vulnerability in a software of the websites. The vulnerability happens either when user input is wrongly filter for literal string escape characters embedded in SQL statements or input of user is not mightily typed and suddenly executed. Thus, SQL commands are injected from the web form into the application database (like queries) to change the content of the database or dump information of database like passwords or credit card to the attacker. [8]

SQL Injection has four main categories of attacks against databases: [9]

1) **SQL Manipulation:** it is the modification process of SQL statements by using different operations like UNION .the second way using SQL Manipulation method for implementing SQL Injection is by changing the where clause of the SQL statement to get different results.
2) **Code Injection:** It is the process of inserting new database commands or SQL statements into the vulnerable SQL statement. This type of attack just possible when it support multi SQL statements per database request.
3) **Function Call Injection:** It is process of inserting different function calls of database to the vulnerable SQL statement. These function calls could be making manipulate data or operating system calls in the database.
4) **Buffer Overflows:** It is happen by using function call injection. For most of the open source and commercial databases, patches are available. This type of attack happens when the server is un-patched.

For the proposed secure streaming site, there are multiple security policies can prevent SQL injection. One of these used a mixed mode authentication for SQL database, which need from attacker to Brocken OS authentication and SQL authentication, which is too difficult this side by side with host security, firewall, and SSL defense, even the hacker bracken these defense they hang on the encryption of video path and passwords, which is very strong encryption.

Dictionary and Brute-Force Attack

The easy way for crack a hash is to use guess way to find the password, it done by first put guess password then hashing each guess, and finally compere if the estimating hash are same to the hash being crack. If the two are same, the estimating hash is the password. The common two ways of guessing passwords are brute-force and dictionary attacks. [10]

A dictionary attack is an attack based on method decrypt an encrypted password value through comparing this value with computed encrypted values for different encryption algorithm with the most likely keys. A dictionary attack method uses a file containing common passwords, most words, phrases, and other strings, which are commonly to use as a password. Firstly, this file is encrypt with most hash algorithms, then these values are save, then its hash is compare to the password hash. If the two are match, then the word is the password. The files of dictionary attack are create by use most common words even from real databases of passwords. Moreover, some processing is apply to dictionary files, like replacing words with their "leet_speak" equivalents ("Ali" becomes "Ali2013"), to make the guess process much effective. [11]

A brute-force attack method based on tries all possible characters combination up to a given length. These attacks are high computationally requirement, and are least effective in cracked of hashes per processor time, but it has advantage that it will find the password eventually. The disadvantage it takes too long time to find passwords especially when the password are long. [12]

There is no way to prevent brute force or dictionary attacks or prevent them altogether, but it can made it less efficient. If the system of password hashing is secure, the just way to crack the password hashes by run a brute-force or dictionary attack on each hash. In this paper, an encryption method used to make the brute-force attack and dictionary attack much more difficult to guess password because it used the random bytes or salt at the end or beginning of the password before the key derivation. For security test for the proposed site, we try many sites that given the ability to cracking password and also used some programs that cracked hash value that used a dictionary and brute-force and all failed to cracked password. Table 2 lists the sites and programs its results.

Table (2) sites and programs test secure streaming site and its results.

Test Site/Program Name		Attacking Type	Test Result
1	CrackStation	Lookup Tables	Hash not found and cannot cracked
2	Hash Cracker	Lookup Tables	Hash password Invalid
3	Onlinehashcrack.com	Lookup Tables	Password Invalid characters or not the right length
4	Rainbowcrack	Rainbow Tables	Hash password is Invalid
5	John the Ripper password cracker	All Attacking types	Program cannot detect the hash algorithm

Lookup Tables

Lookup tables are very efficient method used to cracked wide range of hashes with the same type in very fast time. The idea of Lookup tables are based on pre-compute the passwords hashes in a password dictionary and store them in its database with its corresponding password. When lookup table has a good implementation, it can be process hundreds of lookups hash per second. [10]

Reverse Lookup Tables

This attack give an attacker ability to run a brute-force or dictionary attack to many hashes at the same time, with no needs to pre-compute a lookup table. In this attack, the attacker generate a lookup table which maps each one of password hash from the user account database to a list of users who had that hash. This attack is more effective than previous attacks due to fact that many users commonly have the same password. [13]

Rainbow Tables

This attack are a time_memory trade_off technique. It is same as lookup tables attack, except it sacrifice speed of hash cracking to decrease the size of lookup tables. Because lookup tables become smaller, it can be stored more hashes in the same amount of space, which makes them more effective. [14]

Password Test

We test proposed hashed password with different types of hash cracking sites and programs. A week password that its value “1111” was selected and tested, the results appear no one of password cracking sites and programs can be cracked that password as shown below:

Username	**Password Value**	**Password Hash Value**
Samera	1111	upzCzAYKaIwUDvGDWg++IBH88lcTkgwlUxjsUGqfNyLAE8/Bn5LHbA7yBuv8WgOtp9hrz8wzqEka86UdI/+Ya04nQ8XQVg==

5. Password Cracking Test

The site used to decrypt passwords using different techniques (lookup tables, rainbow tables, etc.).

1- CrackStation

CrackStation uses massive pre-computed lookup tables to crack password hashes. URL site Link: http://crackstation.net/

Test Result:

The test appear hash not found and cannot cracked

2- Hash Cracker

Hash Cracker allows cracking strings hashed with MD5, SHA1 and NTLM algorithms. URL site Link: http://www.hash-cracker.com/

Test Result:

The test appear hash password Invalid

3- Onlinehashcrack.com

This site used different ways to cracked hashed password
URL site link: http://www.onlinehashcrack.com/

Test Result:

The test appear hash password Invalid characters or not the right length

4- John the Ripper password cracker

It is a free software tool used to cracking password and most popular breaking programs and password testing. It is auto detects password hash types, includes a number of customizable password crackers. It can be crack various encrypted password formats including many types of crypt password hash that commonly found on various Unix flavors (based on MD5, DES, or Blowfish), Kerberos AFS.
URL site link: http://www.openwall.com/john/

Test Result:

The test appeared the program cannot detect the hash algorithm from first. We tried it with different encryption algorithms like (MD5, Salted MD5, SHA1, SHA2-256, SHA2-512) with the same password, it used to hash in proposed (1111), the program appear to start finding password and the time depending on strong in encryption algorithm, (it find password of MD5, salted MD5, SHA1 and SHA2-512 in about 0 second and talked long time with SHA2-256, salted SHA1, salted SHA2-512) but with proposed hash the program cannot defined it and stop from the beginning. Figure (2) shows the results.

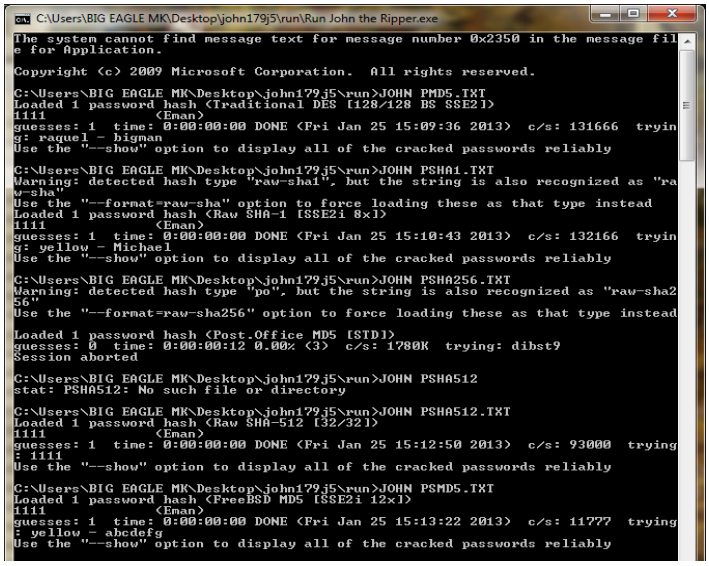

Figure (2) Testing password hash with john179

5- Rainbowcrack

RainbowCrack is a software that used Philippe Oechslin's technique that uses time-memory tradeoff algorithm to crack hashes (as shown in figure 3). RainbowCrack are differs from the hash crackers that it use algorithm of brute force. A brute force algorithm generate most possible plain texts and calculate its hashes on the fly, then make comparison between that hashes with the hash need to be cracked. Once a match of hashes found, the plaintext (password value) found. If the program tested all possible plaintexts without found any match, then it appeared plaintext not found.

URL site link: http://project-rainbowcrack.com/

Test Result:

The test appears the hash password is Invalid.

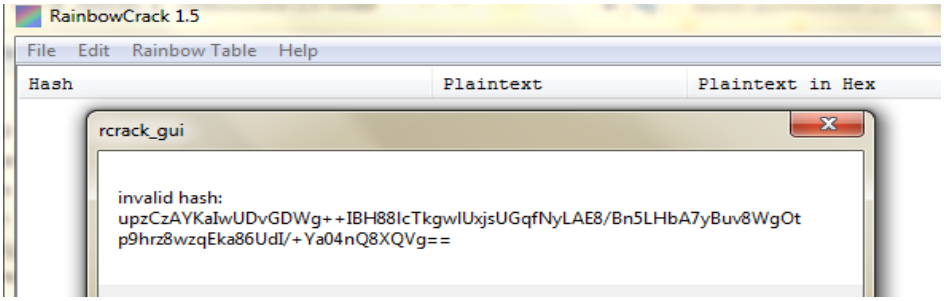

Figure (3) Testing Password Hash in Hash with Rainbowcrack-1.5-Win64

7. Video Path & Video File Encryption/Decryption

Advanced Encryption Standard (AES), also known as Rijndael, used for the encryption and decryption purpose. AES is a symmetric block cipher protocol (operates on a group of bits (a "block") of a certain length all in one go). The standard key lengths are of 128, 192, and 256 bits. It is efficient, and endured extensive cryptanalytic attacks. AES is therefore a desirable choice and is currently being deployed on a large scale. [2]

This password algorithm scheme employs the following steps to secure the use data:

Password Encryption Algorithm

Input:	Password Characters
Output:	Encrypted Password Characters

Step 1: Start.

Step 2: Used the encryption algorithm. It first takes an input string (password) and then generates a one-way hash by used the "SHA512 Crypto Service Provider" algorithm.

Step 3: Generates a truly random number between 8 and 24. This will used to determine the length of the random salt.

Step 4: Using this variable length, it then generates a random salt.

Step 5: Next the user input is encrypted using this variable length random salt bytes using SHA512 crypto algorithm. In addition, the algorithm performs 1000 (or more) passes over the hashed output to provide a higher level of security.

Step 6: Generate the password and verify functions.
Step 7: End.

For the AES algorithm, the length of the input block and the output block is same. It is a point to be noted here that no weak or semi-weak keys have been identified for the AES algorithm and there is no restriction on key selection, only the key expansion routine for 256-bit cipher keys is slightly different from for 128- and 192-bit cipher keys. The strength and design of all AES algorithm key lengths (like, 128, 192 and 256) are adequate to protect information up to the secret level. A high secret information will needing to use key lengths of either 192 or 256. [15]

In the proposed secure streaming media scheme, two method for video encryption one encrypt URL video path which is plaintext (refers to the video data to be encrypted) to AES were provided. It converts URL video path into cipher text, then that cipher text travels upon the network. At receiver side it is deciphered again to brought into its actual form and is stored in the file to be played by user. In addition, in the proposed system, we designed video encrypted and decrypted based on same algorithm that used to encrypt URL. The design of AES is highly conservative that enables us to demonstrate its security against all known types of active and passive attacks.

8. Video Encryption and Decryption Tests

For this tested we compute time request to encryptor and decrepit various sizes of video file using decryptor encryptor program. The tested results that shown in table (3) have been appeared that the time request to encryption and decryption of video file was same and the process runes in relatively very fast time about (35MB/Sec).

Table 3: Video encryption and decryption results

Video Size		Encryption time/second	Decryption time/second
1	10.4 MB	~ 1 Sec	~ 1 Sec
2	30.6 MB	~ 1 Sec	~ 1 Sec
3	80.6 MB	~ 2 Sec	~ 2 Sec
4	672 MB	~ 18 Sec	~ 18 Sec

9. Whole Site Security Test

This test had been used to verifying the security of site in true satiation (on line) and find the possibility of attacking and site breaching used different web-attacking methods. These tests are from commercial companies and it mostly effective and it is an accredited testing.

1- Websecurify

Websecurify is open source and very easy-to-use test tool, which automatically identifies web application vulnerabilities by using advanced discovery and fuzzing technologies. URL site link: http://www.websecurify.com/

Test Result:

After entering proposed URL address http://SMS.somee.com, the plugin started site test; and after run many tests on page the result is the site give appear there is no any gap for the pages but there are two attention described as follows:

1- **File Upload:** this attention that file upload facilities are usually considered dangerous because they can be abused to leverage various types of attacks. This fixed in proposed site because the upload just for video files in three video formats (.flv .avi .wmv) and it must run through converting program and there is a filter to check condition prevent any unsupported file from passing to site.

2- **Path Disclosure (PD):** is the revelation of the full operating path of a vulnerable script. The PD bug is achieved by injecting unexpected characters into certain parameters of a web-page. The script doesn't expect the injected character and returns an error message that includes information of the error, as well as the operating path of the targeted script. PD vulnerabilities are generally observed as low risk threats, too often overlooked by web-masters as nothing to worry about, or features of the scripting language.

2- Exploit-Me

Exploit-Me is a suite of Firefox web application security testing tools designed to be lightweight and easy to use. Rather than using a proxy like most of the security testing tools, Exploit-Me directly integrates into Firefox. It is a very strong test and it consists of three add-ons:

- **XSS-Me:** for testing reflected XSS vulnerabilities
- **SQL Inject Me:** for testing SQL injection vulnerabilities
- **Access-Me:** for testing access vulnerabilities (not supported now with new version of fire fox)

Test Result:

After instilled the three plugins in fire fox and visit proposed site and then run each plugin, the result have been as follows:

1- XSS-Me Test:

The XSS Heuristic Test Results appeared No XSS vulnerabilities found

2- SQL Inject Me Test:

The test appeared that site is very good and there is no warning for any weakness in site from attacking by SQL injection.

3- Netsparker®

The application can detect cross-site scripting issues and the SQL Injection. Once a scan is done, it displays a list of solutions besides the issues and enables to seen the browser view and HTTP request/response

URL site link: http://www.mavitunasecurity.com/

Test Result:

After instilled the program, run the test on proposed site, the test rustle show that no web gap on site and there is three-security information from program, and not classified as threats to increase security (blue Field).

10. Security Techniques Strengths and Weaknesses

From previous tested that applied on site we can describe the points of strength and points of weakness and the proposed solutions.

1- Authentication and Authorizing:

Because of used web streaming protocol there is no way to attacked video streaming through internet but the way of breaking security which mean passing

authentication and authorizing or find the site gaps to be able to view video content. The site designed in way that prevent any not authorizing one can be passed to unauthorized level side by side the page player itself cannot be viewed directly it need to passing through library pages. For special video content their much more security level that need. Site security tested results that done by global sites and programs used to test sites security that used many attack methods appears that site had no site gaps and it been very strong site.

2- Server Side Password Encryption:

encryption technique a simple and effective way to encrypt password and get very strong encryption; this done by used a framework to generated hashed bytes of an input password string, then a random set of bytes, is used to make unauthorized decrypting of a message more difficult, a salt with variable length makes additional protection against password attacks. Totally the algorithm performs 1000 (or more) passes over the hashed output which provides a higher level of security. For all test used the hackers program no one can defriend the encryption algorithm or the hashed value, so this is the one biggest security level of site.

3- Client-Server Password Encryption:

To secure the password travel from client to server we applied encryption method on password to protect it from man in middle attack, because of the encryption done in client side the attacker can know the encryption method and then tried to cracked it, but for site we used third part key which is salt key travel from server to use for encryption which make password strong hashed value and be hard to decrypt. This can be the second advantage of password security.

4- Secure Sockets Layer Authentication SSL

Secure streaming media site used SSL (Secure Sockets Layer) to protected connection between members and site. Because a unique connection has been creating between the client and the server, it cannot be tamper with data passed through an SSL connection. Another advantage of SSL protection is it makes data passed over the Internet be private. The SSL encryption turns useful data (such as addresses, credit card numbers, and other payment information) into useless bits of information and it appeared as random characters. Just the right recipient (the person that have the encryption key) can decode the messages. This means that reception have a channel with private communication, if anyone else tries to get the information, it will appear to be useless.

5- Video URL Encryption Technique:

The big and innovative way to secure video streaming in site is that to encrypt video path itself. Instead of encrypt video file itself the has a novel way that encrypt video file path this means the video file that stored in site cannot be viewed until using its key to generate its path, this technique side by side with architectural authorization prevent any one to view special video unless he have his key. The difficulties that we have encountered that how to address link after decrypt it but we innovate a method that addressed video link.

6- Video Encryption Technique:

The second method for protection videos is to encrypt video file and used AES encryption algorithm. Because the web streaming method need streaming provider and protocols that control the streaming video, the site used http streaming method that encrypt video file then uploading it to site and when client request video file then the encrypted file will streaming to him and then used decryptor to decrypt video file after getting video key that sent to him by administrator. This method has advantage and disadvantage, the advantage is that video file cannot be viewed even attacker hacked client computer or stolen member information and used it to enter special content because he cannot viewed video file and he could not gotten this key because it sent to member e-mail. The only way is to hack his e-mails too. The disadvantage is that the member needs to transfer whole file through http streaming and then decrypt it.

11. Conclusions

The emphasis of this paper is to develop an environment with security infrastructure that performs secure multimedia streaming to users for the prevention of security threats. Different techniques, algorithms and protocols are put together in such a way that they are providing a best security solution to the data traveling upon the network. The attacking rustles appear even with using in http protocol the security of secured pages still strong. The encryption password has been very strong and all cracked site failed to decrypt it. Any pages cannot be access even getting video path without passing authentication process. There is no access to special video without having its key with needs to use strong video key to encrypt special video file or URL path to give video high security level.

References

[1] Jennifer Lagier, "Internet File Types", Ph.D, Hartnell College California State University, 2008.

[2] Mamoona Asghar, Saima Sadaf, Kamran Eidi, Asia Naseem, Shahid Naweed: A Secure Scheme for Video Streaming Using SRTP AES and DH, Request for Comments: 3268, June 2002.

[3] P. Rogaway, T. Shrimpton: Cryptographic Hash-Function Basics Definitions, Implications, and Separations for Preimage Resistance, Second-Preimage Resistance and Collision Resistance, Request for Comments: February 12, 2004

[4] Er ic Gavaldo: SALT Encryption, Request for Comments: August 2002

[5] P. Chown, Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS), Request for Comments: 3268, June 2002

[6] Allison L. Coates,Henry S. Baird andRichard J. Fateman"Pessimal Print: A Reverse Turing Test", International Journal on Document Springer, (2003)

[7] Sagar Joshi, "SQL Injection Attack and Defense", PacketSource SecurityPapers, (July 2011)

[8] Allison L. Coates, Henry S. Baird and Richard J. Fateman"A Classification of SQL Injection Attacksand Countermeasures", IEEE, (2003)

[9] Pascal Junod,Yi Lu,Jean Monnerat and Serge Vaudenay, "A Classical Introductionto CryptographyExercise Book", Springer, (2006)

[10] St´ ephanieDelaune and FlorentJacquemard, "A Theory of Dictionary Attacks and its Complexity",RNTL project PROUVE03V360 and the ACI-SI Rossignol

[11] Prof. Lars R. Knudsen, Dr. Matthew J. B. Robshaw, "Brute Force Attacks", Book, SpringerISBN 978-3-642-17342-4, (2011)

[12] Wenyu Hu and Fang Chen, Liping Zhang, "Using Lookup Tables to Match Data", Merck Research Labs, Merck & Co., Inc., Upper Gwynedd, PA, Paper CC-024

[13] Russell Edward Graves, "High performance password cracking by implementing rainbow tables on nVidiagraphics cards (IseCrack)", M.Sc. thesis, (2008)

[14] J. Postel, User Datagram Protocol: Request for Comments: 768, 28 (August 1980)

