ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

Security Enhancement Using Two-Server Model

Anshu Malhotra[1], Animesh Sit[2], Neeraj Dubey[2], Abhinav Tyagi[2], Pranav Bhatia[2]

Assistant Professor, BVCOE, India[1]

Student, Department of CSE, BVCOE, India[2]

ABSTRACT: These days, most of the Internet Services use a single server model, where a single server is used to store the encrypted password. But, in case this server gets compromised, whole of the user's data is lost. So, to address this problem we may use multiple servers to store a single user password.

In this paper we present the technique of using two servers for storing the encrypted password. Here, firstly we are dividing the user's password into two parts, then encrypting it and storing it into two separate servers. Further, the original password is retrieved by decrypting and combing the two parts of the password. Our system has a number of other features. Like in our system, only a front-end service server interacts directly with the users while a control server which does not interact with the user remains behind the scene; therefore, it can be directly implemented to strengthen the existing single-server password system that uses only a single server to store the password. In addition, the system is secure against various kinds of attack like the Brute Force Attack which may be either Dictionary attack or exhaustive search.

KEYWORDS: Password Authentication, Two Server Concept, AES, Brute Force Attack

I. INTRODUCTION

Password based user authentication systems are cheaper and simple to use. A user just needs to remember a short password and by using that he/she can be authenticated anyplace, anytime, regardless of the types of access devices he/she uses. Authentication systems based on password are still popular even in the presence of newer authentication approaches, like, two factor authentication and biometrics. The reason for this is that it does not require any additional devices or symbols/tokens like in the case of biometrics and two factor authentication systems respectively. In two-factor authentication system the loss or theft of the token/symbol not only risks revealing the secrets inside but also confines the authentication functionality. The best example implementing this two factor authentication system is our ATM system, in which the two factors considered are the ATM card and the PIN number associated with the card. So if the ATM card is lost then it implies that the authentication functionality will be disabled. While in the case of biometrics, the security level attained is very effective and efficient but the only concerns are the cost of hardware and software complexity associated with the system.

Customary protocols for password-based authentication use a single server to stores all the information (e.g., the password) required to authenticate a user. Authentication based on password is the most frequently used authentication technique, since the user is only required to memorize his/her password and on the basis of this can be authenticated anytime at anyplace. Most of the existing password based authentication systems utilize the single-server model where only a single server exists in a system that is used for password. The major disadvantage of this single server model is that the single server used may result in a single point of failure, such that compromise of the server discloses all passwords of users held by the server. The server can be compromised by means of various attacks like the Brute Force Attack which may be either Dictionary attack or exhaustive search. To resolve this problem, a new kind of structure for authentication called the multiple- server authentication was proposed. In such schemes, the process of verifying a password is split between two or more servers, and more than a certain threshold number of servers are required to recover the password. In our system we are using two servers.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

II. LITERATURE REVIEW

In today's world security over the web has become a great matter of concern. The alarmingly high rate of cyber-attacks in the recent year has motivated the need of new and more secure authentication system. First we discuss various types of password authentication system.

Following three types of architectures are normally used for password systems.

- Single-server Model.
- Plain multi-server Model.
- Gateway augmented multi-server model.

Single Server model

This is the simplest type of server which is still being implemented in many places .Such type of system stores the password of the user in a single server, which is vulnerable to many attacks especially the offline dictionary ones

Plain multi server model

In order to remove the vulnerability of single server model this model was introduced which uses many servers in parallel. But there is a problem with this model because the servers need to be synchronized and there is a need of larger bandwidth. This may lead to many problems with resource constrained devices.

Gateway augmented multi-server model

In this model a gateway is used between the user and the servers. The user needs to connect with the gateway. Although this implementation removes the anomaly of simultaneous connection of user with multiple server but the gateway introduced between additionally provides a layer in the architecture which seems redundant. This gateway acts only as a relaying point as a result it may give concerns to security problems as no security measures are taken. Protocols based on the gateway augmented multi-server model include [1] and [2].

TWO-SERVER MODEL

In recent years, attention is being given on designing password based authenticated protocols that can resist any offline dictionary attack by an intruder. To resolve this problem, a new authentication structure named as the multiple-server authentication was proposed. In such systems, the capability of authenticating a password is divided between two or more servers, thus securing the system from invaders. Among these multiple server authentication systems, the two-server authentication procedure is the simplest and the most acceptable to users.

Two-server model [3] consists of two servers at the server side. Only one of these server is open to p ublic while the other server which is back-end is not exposed to public. A user can contact only with the public server but the two servers work together to authenticate users. Here each server is used to store the two separate parts of password. In this paper we will explain the implementation of two-server using AES algorithm for encryption and decryption.

So far, few multiple server schemes have been proposed. Out of these multiple server authentication schemes, the two-server authentication protocol [4] [5] [7] is the simplest and the most acceptable to users. Six two server protocols have been proposed [6].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

III. AES (ADVANCED ENCRYPTION STANDARD)

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001 [8]. It was designed by Rijmen-Daemen in Belgium. It has 128/192/256 bit keys, 128 bit data. Also, it is an iterative rather than Feistel

cipher. Further, it processes data as block of 4 columns of 4 bytes and operates on entire data block in every round. It was designed to have:

- resistance against known attacks
- speed and code compactness on many CPUs

AES Structure:

AES has a data block of 4 columns of 4 bytes is a state. Here, key is expanded to array of words and has 9/11/13 rounds in which state undergoes:

- byte substitution (1 S-box used on every byte)
- shift rows (permute bytes between groups/columns)
- mix columns (subs using matrix multiply of groups)
- add round key (XOR state with key material)

Few comments about AES:

- It is a symmetric algorithm which means both the encryption and decryption uses the same key.
- Here each stage is easily reversible.
- Being a symmetric algorithm decryption uses keys in reverse order.
- In the end decryption does recover plaintext.
- In this algorithm final round has only 3 stages.
- It can be efficiently implemented on 8-bit, 32-bit CPU and 64-bit CPU.

IV. PROPOSED SYSTEM BASED ON TWO SERVER AUTHENTICATION

There is a lot of ongoing research in the two server authentication system. We are using a two server based password authentication system which is effective as well as easier to implement.

Here we are using the two servers namely front end server and back end server. There is no special preference associated with any of the server.

It consists of following servers:

- Server 1
- Server 2

Server 1

In this server the user has to enter the password whose length is 16 characters. For example the user can register his/her password as," 1234567890abcdef". Now this server will divide the password into two parts and both the parts are encrypted using the AES algorithm. It stores in itself the first half and second half gets transferred to the second server. At the time of decryption this server will obtain encrypted password from the second server for the second

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 12, December 2014

half. Then, both the halves are decrypted and combined.

Server 2

This server is storing password obtained from the first server. The first server can request for the second half of the password at any time and second server completes this request.

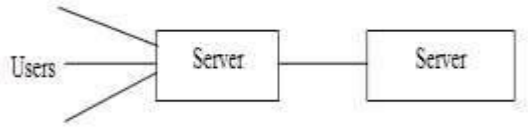

Fig.1 Abstract Representation of Two-server model

Security Analysis

In case of any Brute force attacks, it may be either Dictionary attack or exhaustive search, this method works. Even if the front end server which is open to public is compromised the back- end server will always be safe since it is not exposed to public, thus preventing our system from any kind of attacks.

V. CONCLUSION

In this paper we described the procedure of password authentication using two -server architecture. The procedure starts with the user entering a 16 characters long password thereon we divide the user's password into two equal parts, then encrypting it and storing it into two separate servers. Finally, the original password is retrieved by decrypting and combing the two parts of the password. Here we used AES algorithm which is a symmetric key algorithm used for encryption and decryption purpose.

REFERENCES

1. Bruce sheienier,"cryptography algorithms and source codes, The Blowfish Encryption Algorithm" –Tata mcgraw hill Inc
2. Bruce Schneier, "Schneier on Security: Cryptanalysis of SHA-1" , htttp://www.schneier.com/blog/archives/20005/02/cryptanalysis_o_html, Februry 18, 2005.
3. "A pracical password –based two server authentication and key exchange system", Yanjiang Yang, Robert H.Deng and Feng Bao, IEEE transactions on dependable and secure computing, vol3, no.2, 2006.
4. Xun Yi, "Security Analysis of Yang et al.'s Practical Password-Based Two-Server Authentication and
5. Key Exchange System", 2011 4th International Conference.Network and System Security (NSS).
6. Jiang Huiping. "Strong password authentication protocols", 2010 4th International Conference Distance Learning and Education (ICDLE)
7. B. Kaliski and M. Szydlo J. Brainard, A. Juels. Nightingale: "A new two -server approach for authentication with short secrets", in Proceedings of the 12th USENIX Workshop on Security, pages 1 -2. IEEE Computer Society, 2003.
8. Shuo Zhai, "Design and implementation of password-based identity authentication system", 2010 International Conference Computer Application and System Modeling (ICCASM).
9. Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001. Retrieved October 2, 2012.