Cryptographic Mutual Authentication System with HMAC for Networking Application

Ansu Merin Varughese, M.Lakshmi
Dept.of Computer Science, Sathyabama University, India.
Faculty Of Computing, Sathyabama University, India

ABSTRACT
Mutual Authentication is a process which involves two way authentications where both the user and system must convince each other that they know the shared secret password. It is a part of security which is ascertained at the time of initiation of the communication between the two communicating entities like client and server. It is defined as a security module which is defined at the time of starting of communication between the two communicating entities such as client and server due to the unlimited amount of insecure and malicious intruders it becomes significant to protect the network communication. The mutual authentication is performed using challenge-response handshake with HMAC. It will be performed in a bidirectional way, the server ensures that the client knows the secret and client ensures that the server knows the secret, which protects against a unreliable server impersonating the real server. Here the working of this mutual authentication system is verified using a client and server communication which accesses a file, the HMAC is applied on it for providing better data authentication and data integrity.

Keywords
authentication, challenge-response, client challenge, server challenge, hash message authentication code.

1. Introduction

These days there are many different kinds of computer networks by which multiple number of users share and communicate their specific information types. There is always a continuous need of protection for such transactions. In the organizations like Department of Atomic Energy (DAE), there is always a need to have a secure authenticated transfer of data. These organizations will have many research and highly important files and papers. So there is a requirement to provide security for the transfer of such files. A researcher from BARC, Mumbai may want a data from another scientist who is at Indira Gandhi Center for Atomic Research, Kalpakkam, so in this case if there is no secured transfer of data then the confidential files may be attacked by an intruder easily. The one way authentication is a part of privacy protocol under which a wireless access point may authenticate a user but not the other way around. The disadvantage is that this leaves an unauthorized access point open as a potential launch pad for denial of service attacks. There is no proper authentication and data integrity. In order to overcome the disadvantages of the one way authentication we propose a new scheme by using mutual authentication with HMAC- Hash Message Authentication Code. It uses a Hash Function for providing a fixed length string. Here it uses a SHA-1 as hash function and produces a 160 bits data. In mutual authentication, both the user and system must convince each other that they know the shared secret. The mutual authentication is performed using challenge-response handshake, it will be performed in both the directions, the client ensures that the server knows the secret and the server ensures that the client knows the secret. Challenge-Response mechanism is a scheme that provides security against passive eavesdropping. The password is exchanged using challenge-response. This is used in order to identify a legal user. It ensures that the client and server communication is an authenticated one. It will calculate the client response and the server response using client challenge and server challenge through a client-server communication and verifies whether both the o/p are matching, if so then it is said that authentication is successful. This paper is structured as follows: Section II presents the related work. Section III contains the existing and the proposed system analysis. Further in section IV discussed about main features and the implementation of the proposed system. Finally section V presents our result and conclusion and future work.

2. Related Work

A large number of cryptographic protocols depend in the password[5] that is selected by the people for better authentication and security. Multiple malicious intruders are present to disrupt the communication networks. Password authentication protocol, or PAP, is a method used to authenticate a user to a network. Basically, the PAP works when a network requests a user name and password combination from a user. The user supplies this combination and sends it to the network's authentication server. If the combination is found to be legitimate, the server returns the user's computer an "authentication-ack" that allows the user to access resources allowed by his privileges. If the combination is not successful, an

Manuscript received February 5, 2015
Manuscript revised February 20, 2015

"authentication-nak" is returned and no access is allowed. The disadvantage of PAP[6] was is related to password strength. Reports have shown that people still commonly use passwords like 1234 and abcd. Passwords like this are easily cracked using special software that can be downloaded for free. Another problem of using PAP is that there is a lack of identity check. Supplying a correct password does not prove an individual is who she/he says she/he is. Anyone can falsify their identity to gain access to a network. Because PAP does not have any other identity checks, it is at a disadvantage compared to other authentication methods. Other methods that were developed enhanced authentication scheme using password integrated challenge response protocol. It includes unique password generation and Challenge Response protocol. The above mentioned scheme reduces the risk of third party attacks but more better and efficient user interaction can be implemented and the password exchange must be made more confidential.

3. System Analysis

3.1 Existing System:

The existing system is the one way authentication system that uses normal user name and password for fetching data and communicating with others. Such systems are very much prone to hacking and intruders can easily disturb the network. In the institutions like Department of Atomic Energy (DAE) it is very essential to provide security for the data that is being handled and transmitted. A researcher sitting at BARC, Bombay may want to fetch a resource or a file that is very much confidential from another researcher at IGCAR, Kalpakkam, so in this scenario the data or the file must be transmitted through a dedicated link and it can be prone to various hackers. For this reason we are moving on to the proposed system that uses mutual authentication with hmac. It uses a challenge response mechanism.

3.2 Proposed System

This paper proposes a two way mutual authentication scheme with HMAC for networking application and network communication. The authentication scheme introduces a method where both the user and system must convince each other that they know the shared secret. The mutual authentication is performed using challenge-response handshake, it will be performed in both the directions, the client ensures that the server knows the secret and the server ensures that the client knows the secret. The implementation of challenge-response protocol makes it less vulnerable to security threats. The HMAC uses a hash function for providing a fixed length string. The hash function which is used here is SHA-1. A hash function is defined as a public function that maps a message of any length to fixed length. Grid computing platform is considered as way to connect all computational & data resources present at Department of Atomic Energy (DAE) institutions. DAE Grid project is currently implemented at four DAE institutions namely VECC Kolkata, RRCAT Indore, IGCAR Kalpakkam, and BARC Mumbai. We move on to the proposed scheme to provide mutual authentication with HMAC for connecting to DAE grid user interface machine. It will also allow the DAE grid users from their own desktop to connect to the grid portal. This will allow to provide a secured authentication without transferring password over network.

4. Implementation

The implementation of this project involves four different modules namely HMAC module, communication module which is used by both client and server, client authentication and server authentication module. The whole project is based on the below given project design

4.1 Design:

Client challenge and the Server challenge is created by the client and server respectively. Client computes client response (cr): CR=HMAC(cc+sc,secret), and client sends cr and cc to the server. Server calculates the expected value of cr and ensures that the client responded correctly, server computes sr: SR=HMAC(sc+cc,secret) and server sends the sr to the client. Client calculates the expected value of sr and ensures that server responded correctly. Here we combine both the challenges and apply HMAC with the use of secret key and verify whether they are matching. The implementation is based on this design. It mainly involves mutual authentication with HMAC and challenge response method. The HMAC is used for providing better authentication and security for the data that is being transmitted.

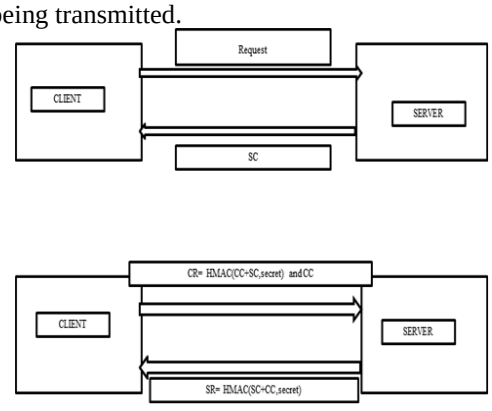

Fig.1: Mutual authentication with HMAC

4.2 HMAC module:

Input:[text, pwd]
Where, text=cc+sc
cc: client challenge
sc: server challenge
pwd: secret key(64 bytes)
Hash function: SHA-1
Output: 160 bits data (20 bytes)
Algorithm:
Step 1: If the length of K=B; set K0=K. Go to step 3.
Step 2: If the K <B: append zeroes to the end of K to create a B- byte string K0.
Step 3: Exclusive-Or K0 with ipad to produce a B-byte string: K0 $\oplus$ ipad.
Step 4: Append the stream of data 'text' to the string resulting from step 4:(K0 $\oplus$ ipad)$\|$text
Step 5: Apply H to the stream generated in step 4: H((K0 $\oplus$ ipad) $\|$text).
Step 6: Exclusive-Or K0 with opad: K0 $\oplus$ opad.
Step 7: Append the result from step 5 to step 6: (K0 $\oplus$ opad) $\|$ H((K0 $\oplus$ ipad) $\|$ text).
Step 8: Apply H to the result from step 7: H((K0 $\oplus$ opad)$\|$ H((K0 $\oplus$ ipad) $\|$ text)).
Where,
B: Block size (in bytes)of the approved hash function
H: Hash function
Ipad: Inner pad; the byte x'36' repeated B times.
K: Secret key shared between the originator and the intended receiver.
K0: The key after necessary pre-processing to form a B-byte key.
Opad: Outer pad; the byte x'5c' repeated B times.
Text: Data on which the HMAC is calculated; text does not include the padded key

4.3 Hash Function:

The Hash function which is used is SHA-1. The SHA-1 is known as a one-way hash function, meaning there is no known mathematical method of computing the input given only the output. The specification of the SHA-1, as defined by Federal Information Processing Standards (FIPS) Publication 180-2, states that the input consists of 512 bit blocks with a total input length less than 264 bits. Inputs which do not conform to integer multiples of 512 bit blocks are padded before any block is input to the hash function. The SHA-1 algorithm outputs 160 bits, referred to as the digest. SHA-1is used for computing a condensed representation of a message or a data file. When a message of any length<2^64 bits is input, the SHA-1 produces a 160 bit output. The SHA-1 is called secure because it is computationally infeasible to find a message which corresponds to a given message digest, or to find two different messages which produce the same message digest. Any change to a message in transit will, with very high probability, result in a different message digest, and the signature will fail to verify. The SHA-1 engine is used to calculate a modified HMAC value. Using a public message and a secret key, the HMAC output is considered to be a secure fingerprint that authenticates the device used to generate the HMAC.

5. Result:

The result when there is a perfect authentication between client and server and the time taken for the authentication success is shown below:

Fig 5.1.a: Final output in client side

Fig 5.2.b: Final output in server side

The client response and the server response are matching, therefore authentication is successful

6. Conclusion And Future Work

The paper describes the integrated mechanism of mutual authentication using challenge response scheme with HMAC. The proposed scheme reduces the risk of third party attacks and provides data integrity and security for the confidential files which must be transmitted. It provides better authentication during communication between client and server in the organizations like Department of Atomic Energy. The future work of this paper is performing the password exchange more confidential. It can be further improved as per the core demands thus it can be observed that the method is readily acceptable for future work.

References

[1] S. Santhosh Baboo, and K. Gokulraj, "Multifactor Hash Digest Challenge-Response Authentication Scheme for Session Initiation Protocol", Network Protocols and Algorithm Vol. 2, No. 4, ISSN 1943-3581 2010.
[2] Nitesh Rastogi, Avinav Pathak and Shweta Rastogi, "Enhanced Authentication Scheme using Password Integrated Challenge Response Protocol", International Journal of Computer Applications Vol. 62, No.9, January 2013, pp.(0975-8887).
[3] "The Keyed-Hash Message Authentication Code(HMAC)" Federal Information Processing Standards Publication, july 2008
[4] http://www.ogf.org/OGF23/materials/1304/0GF23+EU-IndiaGrid+Presentation+DAE-Grid.pdf.
[5] Arkko J, et al. "Security mechanism agreement for SIP sessions", IETF Internet draft, June 2002.
[6] Zhu Zhao, Zhongqi Dong and Yongge Wang, "Security analysis of a password-based authentication protocol proposed to IEEE 1363" ,Theoretical Computer Science, Year 2006, pp 280-278.
[7] http://www.igcar.gov.in
[8] SHA-1 in Wikipedia, http:// en.wikipedia.org/wiki/SHA-1

Ansu Merin.V received the Bachelor of Engineering from Sthayabama University and is currently working for a project in Indira Gandhi Atomic Research Centre.