Global Journal of Computer Science and Technology
Volume 11 Issue 19 Version 1.0 November 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Efficient HMAC Based Message Authentication System for Mobile Environment

By Kavitha Boppudi
Aurora's Technological and Research Institute

Abstract - Computationally constrained environments like Rfid, sensors and hand held devices require noncontact automatic identification technology. The wireless communication channel of these systems is vulnerable to various malicious attacks and has limited calculation resources and small storage capacity, aimed at these problems, a HMAC-based lightweight authentication protocol has been proposed. The main aim of the proposed protocol is that the calculation capacity and storage space of reader should be utilized efficiently, and the demand for the capacity of calculation and storage of device should be reduced. The analysis of security and performance show that the new protocol can resist some malicious attacks, such as spoofing attack, replay attack, tracking, etc., and is suitable for low-cost and computationally constrained system.

Keywords : *Secured Communication, MAC, HMAC, Stream ciphers, Signcryption Challenge response, Digital –Signatures.*

GJCST Classification : *D.4.6, K.6.5*

Strictly as per the compliance and regulations of:

Efficient HMAC Based Message Authentication System for Mobile Environment

Kavitha Boppudi

Abstract - Computationally constrained environments like Rfid, sensors and hand held devices require noncontact automatic identification technology. The wireless communication channel of these systems is vulnerable to various malicious attacks and has limited calculation resources and small storage capacity, aimed at these problems, a HMAC-based lightweight authentication protocol has been proposed. The main aim of the proposed protocol is that the calculation capacity and storage space of reader should be utilized efficiently, and the demand for the capacity of calculation and storage of device should be reduced. The analysis of security and performance show that the new protocol can resist some malicious attacks, such as spoofing attack, replay attack, tracking, etc., and is suitable for low-cost and computationally constrained system.

Index Terms : *Secured Communication, MAC, HMAC, Stream ciphers, Signcryption Challenge response, Digital–Signatures.*

I. Introduction

Security and authentication features were rudimentary in the original analog cellular phones. Authentication and security in cellular phones are important, and there is existing and ongoing work both in the United States and Europe. Secured communication means when the two parties are participating in the communication the messages should be authorized and visible to only two parties. When message are transferring between two parties the security place very important role. The authentication, snooping attacks and replay prevention are essential in secured communications. When we are checking for the message integrity the receiver able to identify the message is getting from valid resource and is that message is not modified. For the above concerns we have symmetric and asymmetric cryptographic schemes. Here when we dealing with constrained environment like hand held devices have limited resource and capacity is small, but these application wants support Authentication and Integrity.

MAC (M, K) is the technique to transfer the message M and a secret key K with the verifier .The verifier gets the cipher along with the message and key. The receiver again encrypts the message and compare with received cipher text HMAC is the one which is the implementation of MAC .The hash function is used to generate the digit .Hash function H ( ) is a one-way function which take variable length message, M as input and produce a fixed length output value, h=H (M).The digit is alphanumeric and it should be fixed length. It is varies from one message to one message. The HMAC is the best technique in cryptographic.

We have so many encryption/decryption methods. Like block cipher, CBC, Stream cipher. When we referring the previous papers the researchers saying that stream cipher is more essential that the block cipher. The block cipher not suitable when we are dealing with long message. The long message takes much time to generate cipher text. A stream cipher is a symmetric encryption technique i.e. shares the same secret key between sender and receiver. The RC4 cipher and one time pad are also stream ciphers. In stream cipher the Initial vector (IV) is encrypted to get output block which is the key, this output block encrypted to get another output block .The sequence of these output blocks are called key streams .These key streams are XOR with plaintext to get cipher text.

Challenge response approach gives the lesser performance in wireless communication when we compare to wired communication because it requires the overhead of handshake before any message shared between sender and receiver. But we want to achieve the better authentication .i.e. identifying the attacker we must use the technique challenge response.

The signcryption is a public-key primitive that performs functions of both digital signatures and encryption. The encryption and digital signatures are basic fundamental tools can guarantee the confidentiality, integrity and non-repudiation .In previous researcher papers many signcryption schemas to achieve the all security issues .The signatures schemes prevents the repudiation because any one can verify a signature using only the senders public key. When we want to authenticate the parties we can achieve by using the best technique signcryption.

The organization of this paper is given as fallows. In section II, provide an overview of cryptograph mechanisms and how the HMAC is extensively using to full fill the security applications. In section III, discussed some security issues rectified using by the appropriate security mechanism. In section IV, shows the work flow of HMAC algorithm, while in section V, discussed how signcryption works between two users to provide authentication. In section VI, how much security is

Author : *M.Tech (CSE) Aurora's Technological and Research Institute, Hyderabad, India. E-mail : boppudikavitha@gmail.com*

improved by using HMAC based protocol. Conclusion in section VII.

II. Related Work

Now days the security place very important role in all the communication systems. The wireless communication system has to support the security mechanisms because the ubiquitous nature of the wireless communication system susceptible to security attacks. The encryption and decryption are done in two ways i.e. Symmetric and asymmetric schemas As the previous research papers gave the some of the efficient algorithms for encryption are DES, AES [8] .Some suggested papers AES is the best algorithm when we compare with DES because the size key in DES support on 56-bit key, but AES can support any length of key and it can be implemented in Hardware and software. Most of AES calculations done at finite state. The AES giving the better performance than DES [6] in the constrained environment.

In paper [6] the three security techniques show the different behavior. The constrained environment uses the steam cipher for the encryption for this the data should be in binary form. This paper attempts to declare which mechanism is suitable for the constrained environment. They concluded AES giving the better performance because it can implement in software not only in hardware.

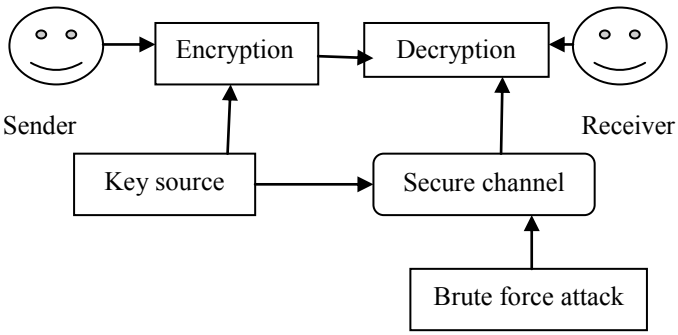

Figure 1 : MAC and Brute force attack.

According to my survey I analyzed that attempts was made in cryptographic system to provide the security applications. Before introduced the concept HMAC the people extensively using the MAC for communications between two parties. The message and key shared between sender and receiver. The sender encrypts the message with his key and send the cipher along with the message, the key also shared by using suppurate channel. In some previous stated that MAC does not guarantee the accompanying message is authentic because of the attacker can identify the key he can access the message. The brute force attacks can modify the message. However various security papers have suggested this mechanism vulnerability to malicious attacks.

The above figure represents the MAC schema work flow and why MAC does not guarantee the security, the attacker can get the key form secure channel.

All the previous research papers attempts was made pointing to HMAC algorithm is mainly for provide the message authentication and preventing the snooping attacks. The design of HMAC specification was motivated by the existence of attacks on more trivial mechanisms for combing a key and a hash function [2][3][4]. No attempts to be found for authorizing the sender and as well as receiver .The previous papers done attempts about the HMAC and signcryption techniques separately. The HMAC can be an implementation of any function like MD5, SHA-1.

The message digest is based on one way function it takes the long plain text as input and produces the fixed length bit of output.

Suppose X is message and MD(X) gives the fixed length of output, if any attacker changes even one bit also it is going to give a different output.

Keyed Hash Message Authentication Code (HMAC) is approved by Federal Information Processing Standards as best mechanism using cryptographic hash functions [7] .It can be used with any iterative hash function in combination with key. The HMAC's was designed with two functionality distinct parameters .a message input and a secret key known only to the message originator and intended receivers.

III. Security Consideration

Security play very important role in current constrained environments, the constrained environment cannot support some complex computations and has limited resources and these systems must support the security applications message authentication, integrity and replay attacks [1].The previous research papers aimed to declare the one-way block information based in stream cipher is fulfill the all security applications.

A stream cipher exhibits the fallowing behavior:

a. The stream cipher initial using the one vector value to generate the pseudorandom stream which is strongly dependent on a secret key.
b. The security of cipher is measured in term of rotation of the message key stream to generate pseudorandom.

The above mechanism is suitable when the short string of message should be transformed, when we want share the short length of string random key generation is not required .In cryptographic system so many type of attacks, one of those attacks are based on establishing the validity of partial guess of secret key the attacker can guess with the given output string .The attacker can get the value only when the output string is considerably higher than the guessed value. To prevent

these attacks by compressing the string into too short that is not longer than secret key. The HMAC can resist the key related attacks. These types of attacks are plays critical role, here the key is which are the one important to generate the MAC value. In HMAC schema the key is divided and each key again XOR with some text. This is the way of showing how the HMAC can resist the related–key attacks.

$$HMAC\ (text) = H\ [Kout \parallel H\ (Kin \parallel text)]$$

Security has become an important issued in the constrained environments .In wireless communication security can achieve by using the some specific procedures and methods. The security applications can achieve by using DES is a big deal. It is a big headache to the parties. To overcome this headache the previous research papers attempted to achieve the security application by using the AES, because of AES can implement in hardware and as well in software [6] [9].

IV. HMAC Based Protocol and Signcryption

I analyzed previous attempts made on HMAC and signcryption [2][3][4][5].The attempts made individually and not constrained environment. One paper [1] made attempts on only HMAC i.e. they aimed to provide the security for the message .No one made attempts to authenticate the parties those are participating the communication.

The constrained environment like hand held device, Sensor networks and Rfid these wireless environments require non- contact automation. Such components should support the security application like message authentication, integrity, time stamping and snooping attacks. These components cannot support the complex computations, high communication overhead and has limited resource. The paper [1] attempts made to get the authentication in Rfid environment. I proposed the mobile environment is the one of constrained environment because of the resource very limited in mobile environment and also high over headache for complex computations. The HMAC can be used to provide the security for message which is part of transmission. As part of HMAC we can deal with any algorithm MD5 or SHA-1.The difference between these two algorithms is the only length of generated output stream and can be used based on the requirement.

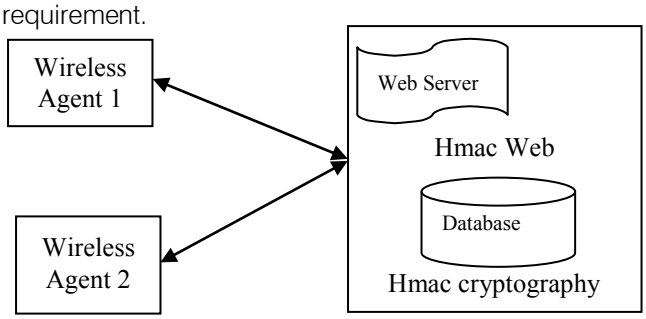

Figure 2 : Architecture of proposed protocol

In the above architecture the communication established between two wireless agents. The protocol is developed based on the HMAC this protocol should be mutual authentication protocol between the sender and receiver. HMAC algorithm is developed by referring the paper [4].I used the algorithm which proposed in paper [4]. I have taken the approach described in that paper I used the MD5 algorithm to get the hash value for the string. The hash-function methods require constant monitoring, maintenance, and updates to maintain integrity.

a) Work flow of HMAC algorithm

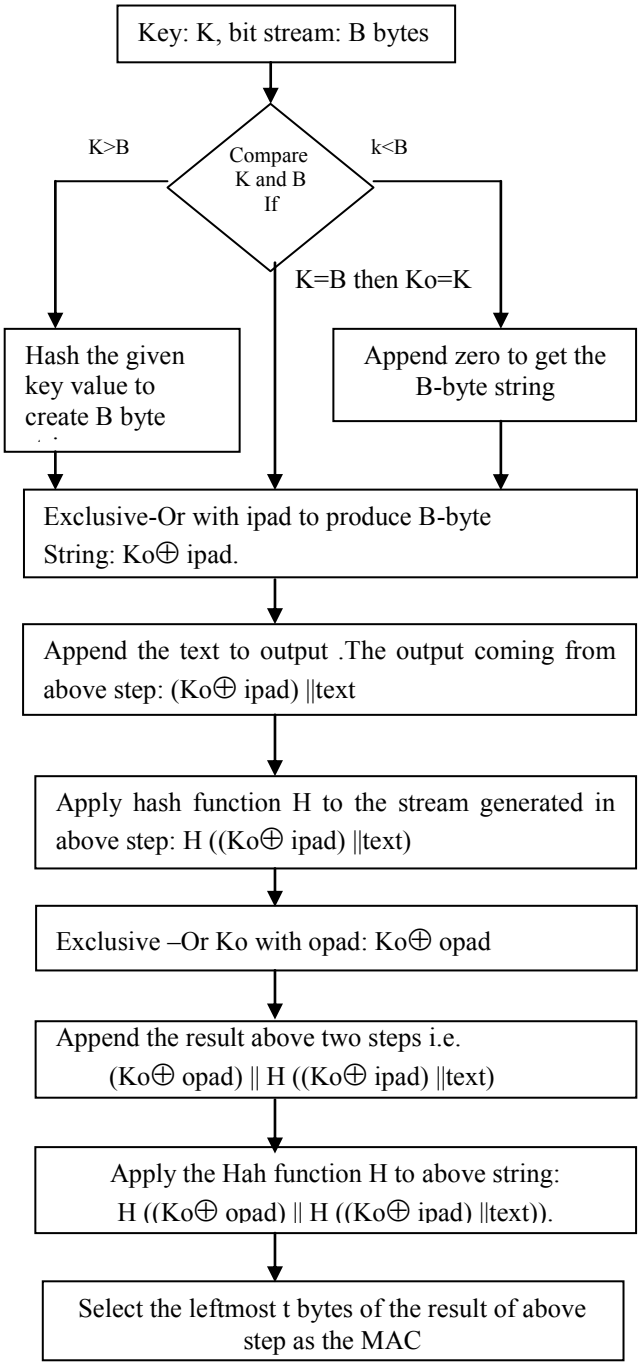

Figure 3 : Internal flow HMAC Algorithm

Addition to above proposed algorithm I enhanced the protocol for Authorization of parties i.e. sender should be authenticated and as well as receiver also should be authorized this enhancement I did by using the RSA algorithm. In wireless communication before sharing the message the handshake process is done by using RSA.I suggest the RSA algorithm is best when want verify the sender and receiver is valid source or not .In RSA algorithm the sender should generate the challenge value before sending the message .This challenge is sent to receiver, the receiver again generate one response and send back to sender by this flow the sender and receiver both authorized.

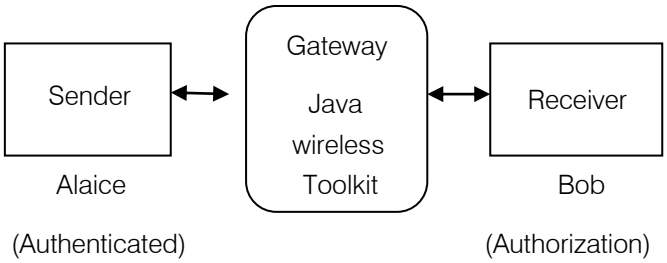

Figure 4 : The architecture of protocol with Enhanced work

V. Implementation Setup

This section describes implementation of HMAC based protocol .This protocol developed in mobile environment by using JME.As part of JME API one of the most useful class us MIDlet. This web application can be developed by using the javax. microedition interface. The class in java.io package is used to develop the cryptographic functions. In HMAC based protocol developed as web application the complete security as developed as part of web server. This is part of providing the security for the message.

Table 1 : Procedure to develop the signcryption

Steps	Step-by-step Description (Aliace-Bob)
Step1:	The users Aliace has to create or generate the keys
Step2:	Bob has to generate the keys.
Step3:	Aliace should be registered with gateway
Step4:	Bob also registered with the gateway by giving his identification i.e. he must entre his Unique ID
Step5:	Aliace make the contract signing with the Bob
Step6:	Finally bob prepare the Initial challenge value.

In enhancement of HMAC based protocol, the sender and racier both should be authorized .I suggest the asymmetric algorithm RSA for this enhancement. In a above table 1: Aliace and Bob are two parties whose generate the challenge response. The users must register with gateway for sharing the message, and receiver has to give his identification to sender. The implementation of this handshake process between Aliace and Bob as shown above Figure c and d.Aliace and Bob generating the keys and sharing the challenge values to verify whether the originator is valid resource or not.

VI. Performance Analysis

The performance analysis done by considering the some scenarios.

1. Only MAC
2. HMAC with DES
3. HMAC with AES
4. HMAC with AES and Signcryption

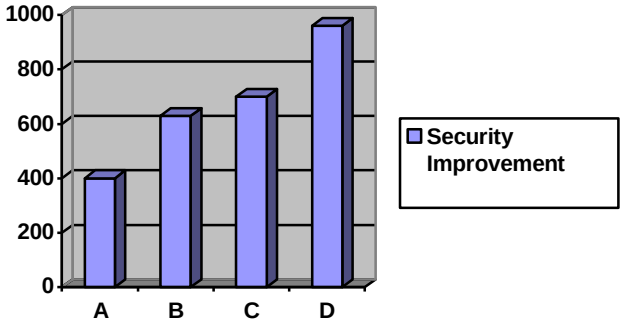

Figure 5 : Security Improvement

A -MAC, B -HMAC with DES, C -HMAC with AES, D-HMAC with AES and Signcryption

The above graph represents cryptographic mechanisms support the security application i.e. message authentication, integrity, and time stamping and snooping attacks. In existing system the block cipher along with DES also gives the less performance than AES. Security improves more when we use the HMAC along with the signcryption. In my proposal system along with the security of message by using HMAC, we are authenticating the parties who are involved in the communication.

VII. Conclusion

Hand held devices and Wireless Sensor Networks pose a need for efficient implementation of MAC. To achieve efficiency, while not sacrificing security, there is a need to evaluate new approaches, while also utilizing any characteristic of the specific implementation of MAC that can enhance efficiency. A complete highly compact MAC implementation, based on stream ciphering, was presented. The principle was

to implement a hash transformation based on the stream cipher, where the strength of the hash is associated with the underlying security of the cipher. The hash is then utilized to implement HMAC based on standard 5 procedures. The HMAC based protocol with signcryption can prevent the attacks and gives the guarantee for authentication and integrity. A specific implementation, based on DECIM (v2) [1], a highly scrutinized stream cipher, was presented and analyzed in detail.

Acknowledgment

I would like to thank Sr.Asst.Prof V.Sathish, Sr. Asst.Prof A. Poongodai and Prof D. Sujatha (Aurora's Technological and Research Institute, Hyderabad, India) for proposing the concept of HMAC with signcryption in constrained environment as well as providing their careful reading and valuable suggestions. I would also like to thank the anonymous referees for their helpful comments, correction and suggestions to improve this work.

References References Referencias

1. Benjamin Arazi, Senior member,IEEE,"Message Authenticaiton in Computationally Constrained Environments",IEEE Trans. Mobile Computing ,Vol.8 ,No.7 July 2009.
2. Smith- Mstr Thesis," Digittal signcryption " ,thesis presented on Combinatorics and Optimization Waterloo,Ontario ,Canada,2005.
3. Bellare, R. Canetti, and H. Krawczyk, "Keying Hash Functionsfor Message Authentication," Proc. Ann. Int'l Cryptology Conf.(CRYPTO '96), pp. 1-15, 1996.
4. H. Krawczyk, M. Bellare, and R. Canetti, "HMAC: Keyed-Hashingfor Message Authentication," IETF RFC 2104, 1997.
5. ANS Institution, "Keyed Hash Message Authentication Code," ANSI X9.71, 2000.
6. Majithia Sachin, Dinesh kumar,"Implementation and analysis of AES, DES ,and Triple DES on GSM Network",IJCSNS ,Vol.10,No.1,January 2010.
7. National Institute of Standards and Technology, "The Keyed-Hash Message Authentication Code (HMAC)," FIPS PUB 198, Information Technology Laboratory, 2002.
8. National Institute of Standards and Technology, "Secure Hash Standard," FIPS PUB 180-1, Information Technology Laboratory, 1995.
9. "Wireless Security Handbook," Acerbic Publications 2005.
10. L. Talavera and J. Bejar, "Generality-Based Conceptual Clustering with Probabilistic Concepts," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 23, no. 2, pp. 196-206, Feb. 2001.
11. H. Jin, M.-L. Wong, and K.S. Leung, "Scalable Model-Based Clustering for Large Databases Based on Data Summarization,"IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 27, no. 11,pp. 1710-1719, Nov. 2005.
12. T. Honkela, S. Kaski, K. Lagus, and T. Kohonen, "WEBSOM—Self-Organizing Maps of Document Collections," Proc. Workshop Self-Organizing Maps (WSOM '97), 1997.
13. M. Junker, M. Sintek, and M. Rinck, "Learning for Text Categorization and Information Extraction with ILP," Proc. First Workshop Learning Language in Logic, 1999.