Eng. & Tech. Journal, Vol.29, No.16, 2011

A Proposed Secure Protocol for E-Mail System Based on Authentication and Hash Function

Dr. Muna Mohammed Al-Nayar*

Received on: 27/ 3 / 2011
Accepted on: 3 /11 / 2011

Abstract

Internet has opened new channel of communication enabling an e-mail to be sent to a relative thousands of kilometers away. This medium of communication opens doors for virtually free mass e-mailing, reaching out to hundreds of thousands users around the globe within seconds, so e-mail becomes the most popular form of communication today. E-mail systems have suffered from increasing attacking problem that threatens the validity and integrity of communication. Many different approaches for fighting this attack have been proposed, ranging from various sender authentication protocols to encrypt the message itself. This paper demonstrates a promising protocol. The proposed protocol ensures the authentication and integrity of the data and avoids the problem of key distribution or breaking by using multiple random keys generated automatically during communication session.

Keywords: E-Mail System, Security Protocol, Authentication, Hash Function, Randomization, Message Integrity and Confidentiality.

مقترح بروتوكول آمن لنظام البريد الالكتروني مستند على تعريف الهوية ودالة الـ Hash

الخلاصة

فتحت الانترنت قناة جديدة للاتصال تمكن من ارسال بريد الكتروني عبر الاف الكيلومترات. هذه الوسيلة من الاتصال فتحت ابواب امام ارسال كميات من الرسائل الى الاف المستخدمين حول العالم خلال ثواني، لذلك اصبح البريد الالكتروني هو الاتصال الاكثر شيوعا اليوم. يعاني نظام البريد الالكتروني من مشكلة الهجوم المتزايد والذي يهدد صحة وتكامل الاتصال. وقد اقترحت طرق عديدة لمحاربة هذا الهجوم تتراوح ما بين بروتوكولات مختلفة لتعريف الهوية الى تشفيرالرسالة نفسها. يقدم هذا البحث بروتوكول معتمد على تعريف الهوية ودالة الـHash للمحافظة على امنية المعلومات. يأكد البروتوكول المقترح على هوية المستخدم وتكامل البيانات ويتجاوز مشاكل توزيع او كسر المفتاح باستخدامه مفاتيح متعددة وعشوائية وتولد اتوماتيكيا خلال فترة الاتصال.

Introduction

Electronic mail or e-mail is a set of processes designed to allow sending messages between computer users. E-mail is currently the most common, cheapest and convenient method of daily communication between individuals and organization [1]. It is used daily by millions of people to communicatearound the globe and

* Computer Engineering Department, University of Technology / Baghdad

https://doi.org/10.30684/etj.29.16.3
2412-0758/University of Technology-Iraq, Baghdad, Iraq

isamission-critical application for many businesses [1].

E-mail has made communication very fast and very easy. The increasing use of the e-mail increases the attack to it, so sending private information using email without any measurement security or receiving message by e-mail not controlled by security policy is a big problem [2].

This paper develops a secure protocol based on authentication and hash function, which is used to enhance security features of e-mail protocols. The enhanced e-mail protocol can give evidence that the received message is from the right originator and can check the message integrity.

At the most basic level, the e-mail system can be divided into two principle components which are: E-mail server, that hosts, deliver, rout and store email messages and E-mail client that interfaces with users and allows users to read, compose, send and store e-mail messages [3] .

E-mail data is basically a stream of bits that represent the message. Figure (1) shows the flow of an e-mail message via the e-mail system through the following parts:

1- Mail transfer system: which consists of four major components; mail transfer agent (MTA), mail delivery agent (MDA), local delivery agent (LDA), and mail user agent (MUA).
2- Mail transfer protocols: which are the rules that govern E-mail message transferring.
3- Mail box: which is the location where E-mail messages are stored for user.

E-Mail Protocols

In order to send and receive an e-mail message between users, there must be protocols. A protocol is a multi-party algorithm, defined by a message formatted and a sequence of steps precisely specifying the actions required of two or more communication parties in order to achieve a specified objectives [4].

There are many transport standards which established to ensure reliability and interoperability between the sender and the server, between server and server, and between server and receiver.

Actually there are three protocols used, these are[5]:

1- SIMPLE MAIL TRANSFER PROTOCOL (SMTP): used for the actually transport of mail message between two entities.
2- POST OFFICE PROTOCOL (POP): allows single user to collect his mail on his server
3- DOMAIN NAME SYSTEM (DNS): used to identify the e-mail host address for domain or host name.

E-mail protocols are text-oriented, command base protocols. Most of these protocols are designed for the client-server paradigm, where the client is the host that requests a service and the server is the host that responds to the request. In other words the client is the one who “speaks first” and the server is the one trying to fulfill the request. [6 &7].

Types of Attacks on E-mail

E-mail servers are the hosts on organization's network that is most often targeted by attackers. This is because the computing and network technology that underpins e-mail is ubiquitous, it is well- understood [3], and the core of e-mail protocols are designed to provide services and transmit data as a cleartext, also doesn't provide any built-in security features[8]. Also SMTP protocol offers no message integrity or sender authentication mechanisms. [9,10 & 11].

These drawbacks can make user under attack, table (1) shows the general categories of attack [12], by now the need for good authentication should be obvious. Message authentication provides a means to thwart various forms of attack and can enhance other aspects of communication security[13]

It is important to protect the e-mail message from threats to the confidentiality, integrity, authenticity, and availability as it transits through a potentially hostile environment like the internet, and for that it is desirable to use of what is commonly described as secure e-mail.

Ordinary network protocol enables parts of a computer network to communicate with each other, but the security protocol is a communication protocol that has been designed to operate in a potentially hostile environment [14].

Some security and a higher level of trust can be provided to SMTP by applying some cryptographic measures to the message. If message integrity or sender authentication is required then the application of a digital signature is called for [10].

An authentication service called Pretty Good Privacy PGP had been found by Phil Zimmerman 1991[12]. It can be used for e-mail and file storage application and could do many things such that selecting the best available cryptographic algorithms as building blocks and integrate the algorithms with a general purpose application. It is based on securing the message not the communication protocol [12]. This protocol is not built in to e-mail systems and users need keys and software to use PGP.

A secure multipurpose internet mail extension S/MIME was developed by an industry consortium and is now appearing in a number of major products [15]. It is based on (RSA). S/MIME emerged as the industry standard for commercial and organizational use, while PGP remain for personal e-mail security for many users. It offers the ability to sign and/or encrypt messages but it needs an authorized key distribution center to provide session keys. S/MIME can only send and receive encrypted emails for individuals with S/MIME enabled e-mail system requires sender and recipient to have exchanged public keys ahead of time there is a risk of individuals losing their private keys if a hard disk becomes corrupted or a device is lost and keys are specific to e-mail account so that individuals with multiple account must request keys for each account. MIME Object Security Services (MOSS) is another secure e-mail option [16]. MOSS is derived from PEM and is similar to S/MIME in that it is a proposed

Internet standard for providing security to MIME. MOSS depends on the existence of public/private key pairs to support its security services. Users must exchange public keys with those other users with whom they wish to exchange MOSS e-mail. Like most of the other protocols, MOSS relies upon digital signatures and encryption to provide authentication of the sender and message integrity and confidentiality.

These competing standards and products are one of the primary reasons that secure e-mail has not been widely implemented. The standards are not interoperable. If user use PGP to send someone a secure e-mail, but the recipient employs S/MIME then the recipient will not be able to open and read the message, there is no single mechanism that will provide all the basic functions such as preventing, detecting and recovering from security attacks.

In this paper we present secure protocol using authentication and hash functions that ensures message originator and message integrity

A Proposed Protocol Using Authentication And Hash Function:

Security protocols use cryptographic algorithms to enable the communicating parties to communicate in a secure way. On the other hand, the cryptographic protocol is a protocol that enables cryptographic mechanisms such as encryption and one-way hash functions to guarantee the confidentiality, authenticity, integrity and availability of the data.

Two important aspects in e-mail message(data) to verify these are:

1- The contents of the message have not been altered
2- The message is authentic

In this section we will describe the design of the proposed protocol for e-mail system which we called it Ath-Pro. Ath-Pro system is implemented using "Visual Basic6", because of its facilities that include visual interface handling, Winsock component to provide TCP/IP connection, outlook MIME viewer component to compose read and create e-mail message and manipulate database in an easy and efficient way.

The Authentication Protocol

The goal of an Ath-Pro is achieved by exchanging protected messages between the communicating parties which involve information about the identity of the parties, the current session as well as the timeliness.

The proposed authentication process is done between the e-mail client (MUA) and the server . The authentication process based on two security techniques these are pseudo random number generators and authentication algorithm that uses hash function. Figure (2) summarizes the authentication scenario which is as follows:

1- To open a communicating session the client sends its identity (C-ID) to the server. As acknowledge the server will respond to the client with message identity (M-IDI) token that contains a random number, time stamp, Fully Qualified Domain Number (FQDN) of the server and the sequence number of the session .

2- According to the M-IDI received , the client then will compute a message-authentication code (M-CODE) according to the authentication algorithm described below and send it with a new message identity (M-IDII) separated by a space. M-IDII contains a random number, time stamp, FQDN of the client and the session number.
3- When the server receives the later response. It regenerates the M-CODE again using the stored values and compares the two codes to verify if they are identical.
4- If the two M-CODEs are identical, the server will generate new M-CODE using M-IDII, M-CODEII is sent back to the client to be verified again and the two parties are considered to be authenticated

All exchange messages which are text oriented, will be sent signed digitally by M-CODEII to ensure the message integrity. The last message (S-END) should be sent by the client to inform the server that the session ended to end the communication session.

Message Identifier (M-ID) generating

The M-ID is a random unique identifier used between two communicating entities as a challenge in any challenge-response protocol. The M-ID token is the challenges that required in the proposed authentication protocol, and consist of four parts separated by star (*) character, these parts are:

1. Arbitrary sequence of random digits
2. Time stamp of the current time.
3. The issuer FQDN of the connection host or account name for users,
4. Session Sequence Number.

Since any M-ID is consider strong against security attacks as much as it random and unique, the proposed protocol ATH-PRO uses the above sophisticated M-ID format to prevent many type of authentication attacks (such as reply attack, reflection attack… etc) due to the Pseudo Random Number Generator(PRNG) used. An ideal random number generator would provide numbers that are uniformly distributed, uncorrelated satisfy any statistical test of randomness, have a large period of repetitions, can be changed by adjusting an initial "seed" value, are repeatable, portable, and can be generated rapidly using minimal computer memory.

The proposed generator XOR two random values "generated from XORing previously generated value from PRNG with a value generated from other PRNG" and rotate the output to make it more unpredictable, that leads to modified generator based on the idea of XOR-TREE to get better result, long period, longer than those generated using more complicated XOR-TREE generators in short time, figure (3) describes the proposed method.

M-CODE Generator

Most mechanisms that provide message authentication and integrity check are based on secret key. These mechanisms are usually called message authentication codes (M-CODE). Typically M-CODE is used between two parties that share a secret key in order to validate information transmitted between them.

The proposed M-CODE generator in ATH-PRO uses M-ID to drive the secret key to avoid the problems of key loosing or breaking and using different keys in different sessions makes the protocol more strong and more secure. The generator is based on HASH function, and a randomize function with supporting functions such that splitting, merging and truncate functions. Figure (4) shows the structure of the proposed generator.

The combination of the above functions will make the authentication process more complex to the intruder even if he fined the key he will not be able to find the code, so it is more secure. In the other hand using well defined and understood functions without modification make the generation simple and easy to implement.

The randomize function used here to disorder the bits of the key in a way such that have unpredictable value from the original key by swapping the bits two by two from left to right then rotate result right 3 digits. The resulting key is different from the original key that makes the protocol more secure even if the key have been found.

Table (2) shows a comparison between the ATH-PRO and other e-mail protocols.

Conclusions

Although authentication and encryption have their own responsibilities in securing a communication session, maximum protection can be achieved when two are combined. The proposed protocol uses the combination of application of these technologies to ensure the confidentiality and integrity of the message. The designed protocol can achieve more secure communication due to using multiple functions such as hash function, randomize function, splitting and merging which make it more complex unpredictable and easy to implement. Also avoiding the use of secret key and using automatically generated key will avoid the protocol from key losing and breaking problems.

References

[1]Ahmed Khorsi, "An Overview Of Content-Based Spam Filtering RANDOMIZE1
Techniques" Infomatica 31(2007) P 269-277.

[2]Marcus Condaves And Steven A. Brown "Check Point Fire Wall-1", Mcgraw-Hill Companies, 2000.

[3]Miks Tracy, Wayne Jansen and Scott Bisker, "Guidlines On Electronic Mail Security, Recomandation Of The National Institute Of Standards And Technology", Special Publication 800-45 NIST, Internet Paper September 2002.

[4].Menzes, P, Van Oorsehot And S. Vanstone, "Handbook Of Applied

Cryptography" , CRC, Fifth Printing, Augest 2001.
[5]Mathew Naugle, "Illustrated TCP/IP", John Wiely & Sons, Canada.
[6]Kevin Johnson " Internet Email Protocols, Developer's Guide", First Adition, Anddison Wesley Longman, Hallow England 2000
[7] Stamp, "Information Security Principles And Practice", Wiely-Interscience, 2006
[8]Tiffany Taylor "Security Complete", Second Edition Sybex Inc, 2002.
[9]Enrico Blanzieri And Anton Bryl, "A Survey Of Learning-Based Techniques Of E-Mail Spam Filtering", Technical Report #DIT-06-056,UNIVERSITY OF TERNTO-ITALY, Information Engineering And Computer Science Department, 2008.
[10]Yan Luo, "Workload Characterization Of Spam Email Filtering Systems", International Journal Of Network Security & Its Application (IJNSA), Vol.2, No.2, January 2010.
[11]Mikael Svensson, "Countering Voip Spam:Up-Cross-Down Certificate Validation", Master Thesis In Communication Systems, Kth Information And Communication Technology, 2007.
[12]William Stallings, " Network Security Essentials: Applications And Standards", Printice Hall, New Jersey 2000
[13]Harold F. Tipton & Micki Karause, " Information Security Management Handbook", CRC Press LLC 2004.
[14]Helsinki J. "Modeling of Cryptographic Protocols, A Concurrency Perspective", Final Draft, Pekka Nikander, Final Internet Draft 1997.
[15]Andrew S. Tanenbaum, "Computer Network", Third Addition, Prentice-Hall, Asimon & Suchster Company 1996.
[16]Behrouze A. Forouzan, "Data Communications and Networking", Fourth Addition, McGraw-Hill Higher Education 2007.

.

Table (1) the General Properties of E-Mail Attack

	Attack	Description of Attack
1	Interruption	A message is destroyed or becomes unavailable or unusable. This is an attack on availability, and it is a type of active attack
2	Interception	An unauthorized party gains access to read the message this is an attack on confidentiality .The unauthorized party could be a person, a program or a computer, and it is a type of passive attack,
3	Modification	An unauthorized party not only gains access to but tampers with the message. This is an attack on integrity, and it is a type of active attack
4	Fabrication:	An unauthorized party inserts counterfeit message into the system. This is an attack on authenticity, and it is a type of active attack

Table (2) A Comparison Between The Proposed Protocol (ATH-PRO) And Other Protocols

FEATURES	PROTOCOLS			
	SMTP	PGP	S/MIME	ATH-PRO
Message Authenticity	No	No	No	Yes
Message Integrity	No	Yes	Yes	Yes
Key Management	-	Uses Single Private Key (symmetric key)	Uses Single Public Key (asymmetric key)	Uses Different Keys (A Key For Each Communication Session)
Key Distribution/Exchange	-	Yes	Yes	No Need Because Keys are self generated
Digital Signature	No	Yes/Separated From The Message	Also	Yes Within The Message
Encryption/Decryption	No	Uses Block ciphering	Uses RSA ciphering	Uses Hash Function

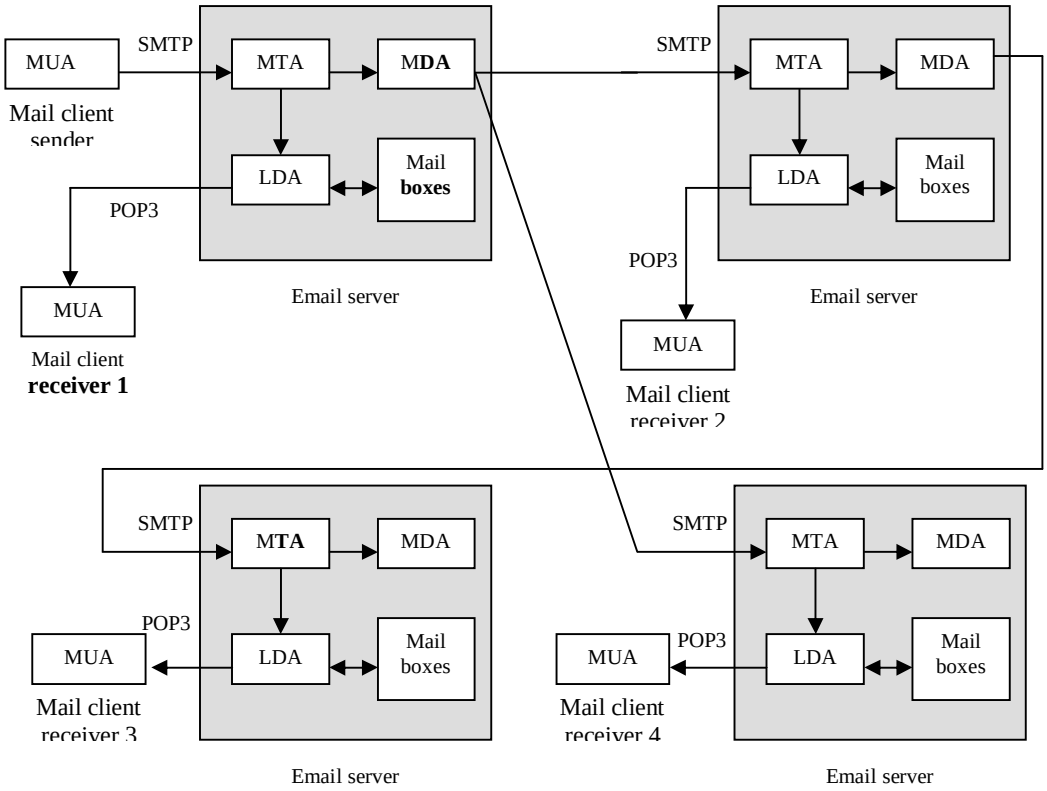

Figure (1) E-mail System: General Process of Message Flow

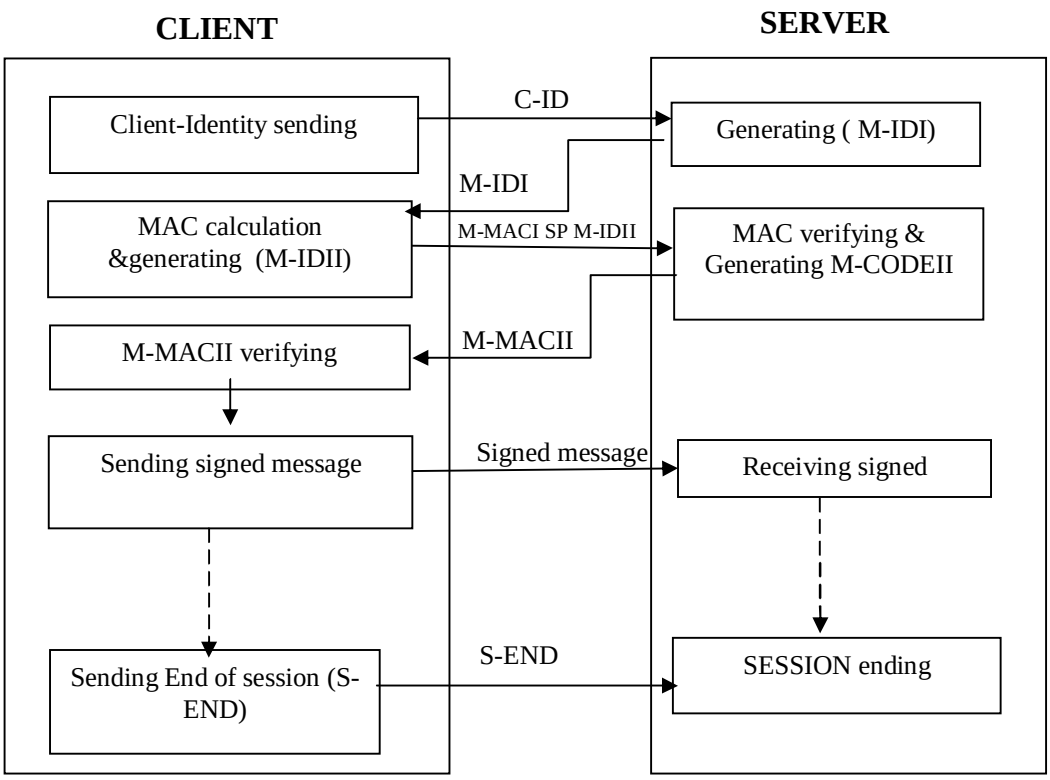

Figure (2) the Authentication Protocol

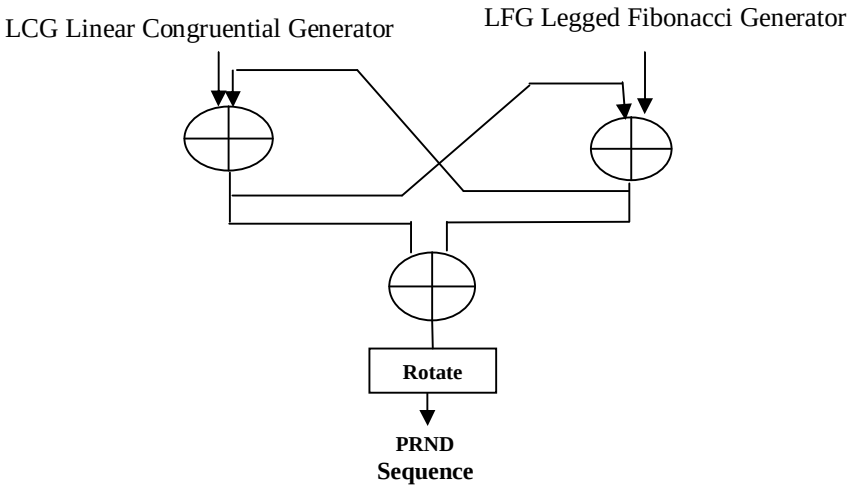

Figure (3) Random Number Generator

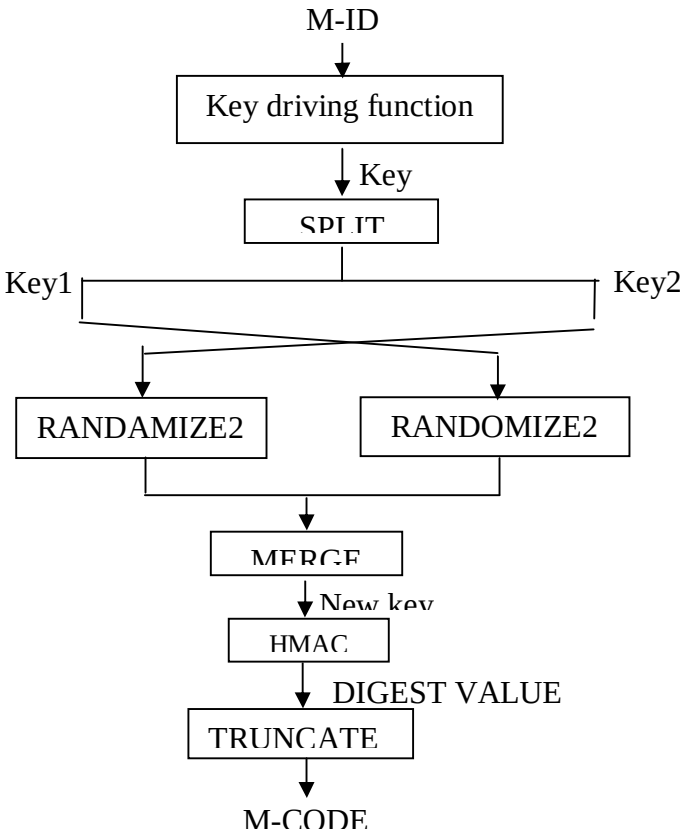

Figure (4) M-CODE Generator