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. 3, Issue 6, June 2015

DKIM Enabled Two Factor Authenticated Secure Mail Client

Saritha P, Nitty Sarah Alex

M.Tech Student[Software Engineering], New Horizon College of Engineering, Bangalore, India

Sr. Asst Prof , Department of Information Science, New Horizon College of Engineering, Bangalore, India

ABSTRACT*:* Email has been emerged as the commonly used network application which made it necessary to be secured. An email client is a computer program by which user’s access their mail. The proposed mail client provides two factor authentication login rather than the normal username and password login by generating a security code. It also includes a feature called Domain Keys Identified Mail (DKIM) which appends digital signature to each of the mail being sent by the particular organization.

KEYWORDS: DKIM, Pretty Good Policy, Privacy Enhanced Mail, Secure Multipurpose Mail Extension, Two factor Authentication

I. INTRODUCTION

The most prevalent form of login has used an ID and password which is classified as one factor authentication. There have been various methods through which the attackers could hack the password. This could be very problematic especially in large organizations. In this way any of the important mail send from an organization can be hacked and could be modified. Another major issue which is found in the current email systems is the email spoofing wherein the emails appear to be from a legitimate sender but in real would have been send by a attacker. It could be a link or message viewing of which could result in system attacked by viruses or hacking the entire personal account of the users. This paper mainly concentrates on making an email secure for a user or for an organization. It uses a two factor authentication mechanism rather than the normal single username and password in order to overcome the problems of using single username and password like the hacking of passwords. It also tries to avoid the common problems of spamming by digitally signing the mail using any of the values in its header fields and it particularly focuses on the security of organizations by using their domain names.

II. RELATED WORKS

The first email client program ever developed was named MSG. At the beginning, email was sent through a FTP(File Transport Protocol)-like structure. MSG was also one of the basis in creating the SMTP (Simple Mail Transfer Protocol)-type server, which is now the standard gate through all of the messages pass in order to reach their email clients. One of the first email clients that offered the user with a text interface was Elm[1]. There are different types of mail clients existing. All of these have the traditional login method of a single username and a password. If the username and password is found to be valid then the user would be directed to their mails folder wherein they could view their mails. In this approach a hacker who hacks the username and password of a user using any of the attacking methods as discussed above could view the mails of the particular user. There are various opportunities for the hackers to send unauthorized messages or to modify messages during delivery. Messages sent in clear text could be easily read by the intruder if the installed server is “Rogue Mail server”. When messages are sent to these compromised servers during the delivery process, the messages could be send to alternate destinations along with the correct destination. Many of the problems that E-Mail users encounter are related to the material contained in messages that they receive. These sometimes include HTML formatted messages, harmful attachments or other forms of executable code. The most common and most known harmful E-Mails commonly contain viruses or malware. If these attachments are opened on a computer they can install viruses or spyware that can do anything from format the computer to sending an

DOI: 10.15680/ijircce.2015.0306057

entire address books worth of viruses and personal information. Another disadvantage is the email spoofing [2]wherein the emails send from hacker appears to be from a legitimate sender and other is the phishing attack[3] where the messages are altered in between by the man in middle. It could be a link or message viewing of which could result in system attacked by viruses or hacking the entire personal account of the users. Also there are many advertisements like mail which arrives at the inbox of the current mails systems viewing of which could again result in getting attacked by a Trojan. There has been various email secure methods like Privacy Enhanced Mail(PEM)[4] which had two main protection features which were the signed messages and the encrypted messages, Pretty Good Policy(PGP) [5] where users could independently certify keys as belonging to other users and Secure Multipurpose Mail Extension(S/MIME) [6] which is a standard for public key encryption and signing of MIME data.

III. PROPOSED ARCHITECTURE

The Fig.1 shows the overall architecture of the proposed system. It clearly shows how the login to the mail folders is done and how the digital signatures are appended to the mail composed by the user.

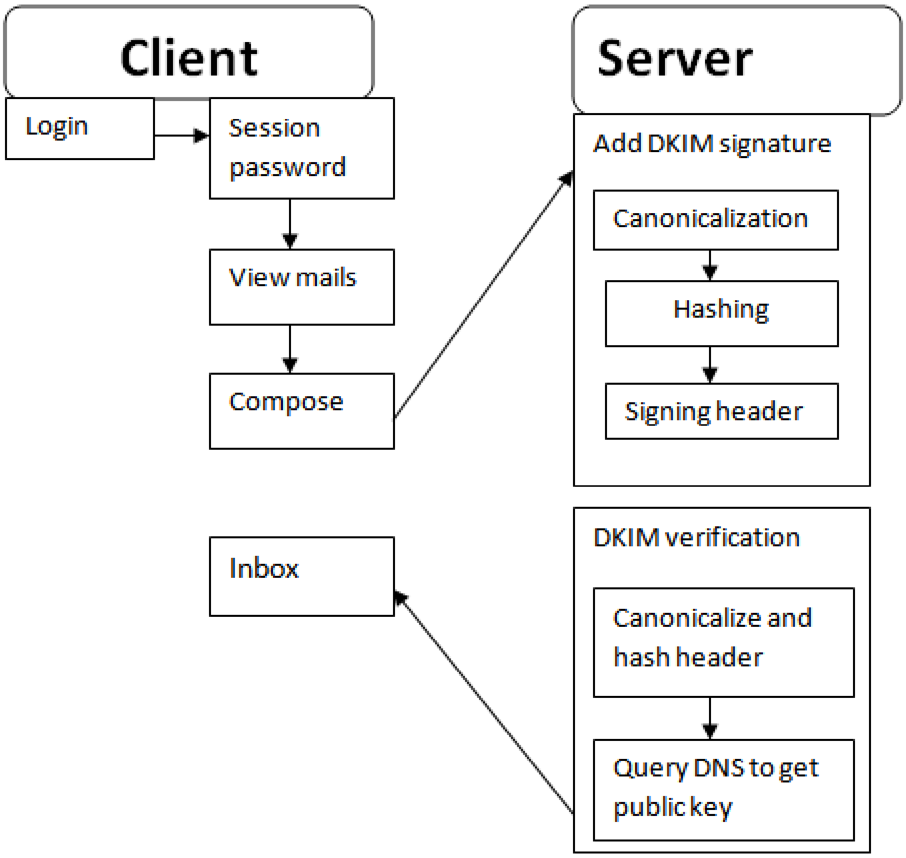


Fig 1 Proposed system architecture

User logs in to the mail client using SSL handshake. SSL is implemented using openSSL which is an open source tool for implementing SSL and TLS protocols. Whenever the user logs in to mail client it first establishes connection to the web server which is responsible for finding the respective mail transfer agent (MTA) of the particular mail client. This MTA is also responsible for sending the mails to the MTA of the destination mail client. The user initially logs in using his username and password which was created during the registration. The server first checks if the user is logging in from within the organization or is from a reliable IP, if found reliable then he will be directed to his mail's inbox folder wherein he could view his mails. If the user is found to log in from outside then he will be directed to page where he has to enter the session password which is created by the server and send to the particular user's mobile.

User composes a mail and transfers it into the sender's Mail Transfer Agent which appends the signature by canonicalising and hashing the message body. Whenever a mail arrives the receiving Mail Transfer Agent would initially check if it is a DKIM signed mail or not. If it is found to be digitally signed then it checks the signature by creating a text DNS query to the senders domain. If found to be valid then it checks for the reputation of the sent domain and if this is invalid then the mail received from the particular domain would be either sent to spam or would be discarded depending on the organization policy.

IV. IMPLEMENTATION

Implementation of this project deals with issues of quality, performance and delivering the end product. The entire project is coded in java. The different modules included are:

- Login

Initially the registered users are provided with a usual login screen containing the username and password. Users then enters their valid username and password after which they would be directed to a page wherein they have to enter the session password. This session password is created by using hashing algorithms by combining parameters as the username, pin timestamp and IMSI number. All these parameters are concatenated, xored and converted to eight digit hexadecimal number which is send to var/spool/sms/outgoing directory. If their entered password is same as the password generated by the server only then the user would be directed to their email inbox wherein they could view their mails.

- DKIM signing

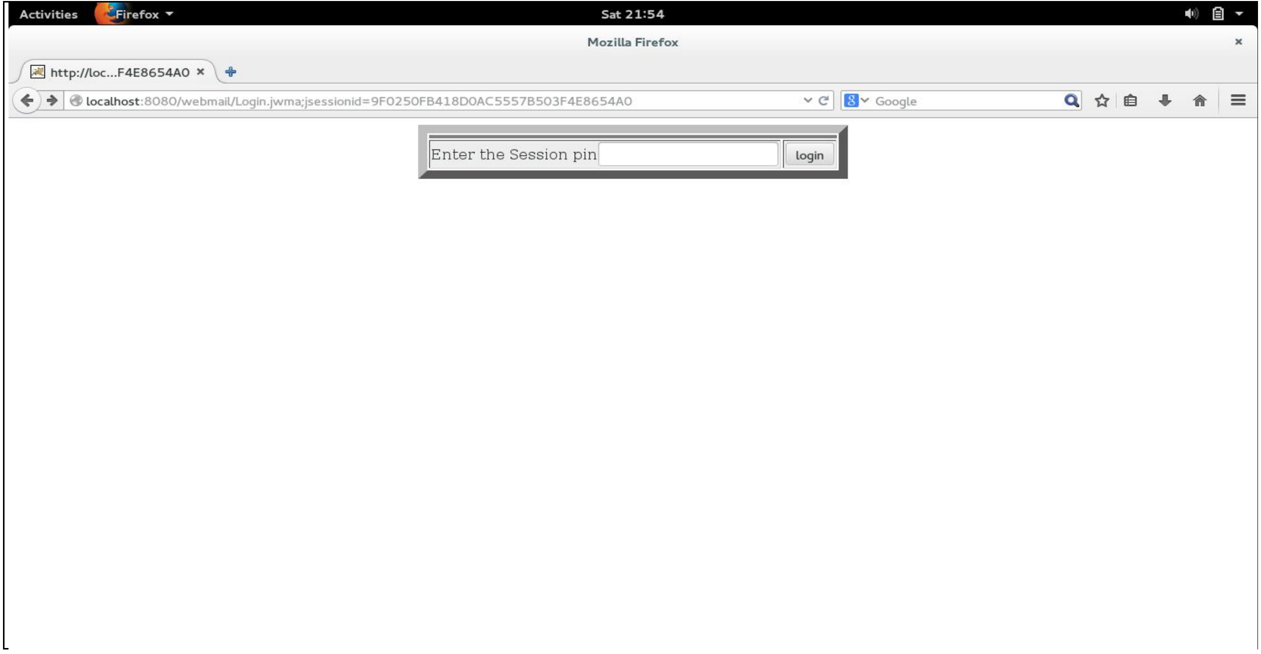
This module is concerned with appending the digital signatures to the emails being send by the mail client of an organisation. The process of Domain keys identified mail signing is mainly useful in large organisations. If an organisation uses DKIM then all of the mails sent out by their mail client is said to be digitally signed. DKIM performs email sender identification by associating a domain name and owner to the content of the email message, allowing the organization to confirm the content of the message. This is then passed to the sending Mail transfer agent which creates a digital signature by selecting the header fields to be hashed and create a digital signature using RSA algorithm using a private key. The public key which is used to verify the digital signature will be made available in the form of a text record in sending domain name server. It also hashes the body of the message using SHA 256 algorithm in order to maintain the integrity of the message.

- DKIM verification

This module is designed in order to perform the verification of mails received by the client. The receiving mail transfer agent performs the verification of all the mails received from outside the organisation. It does the verification by checking the digital signature which is the DKIM signature by using the public key from the sending domain name server. Different organisations have different policies regarding the verification i.e if a mail is found to fail the signature verification then the receiving organisations mail transfer agent can either send it to a spam folder or can be discarded or can be sent to the mail client with a warning message that the particular mail has failed the DKIM verification. Thus this signature verification helps in avoiding problems of email spoofing wherein the mail is send from an illegitimate sender appearing to be legitimate and also avoids altering of the message contents as the messages would be hashed when the mails are digitally signed.

V. RESULTS

The following snapshots shows the output obtained after the execution of different modules

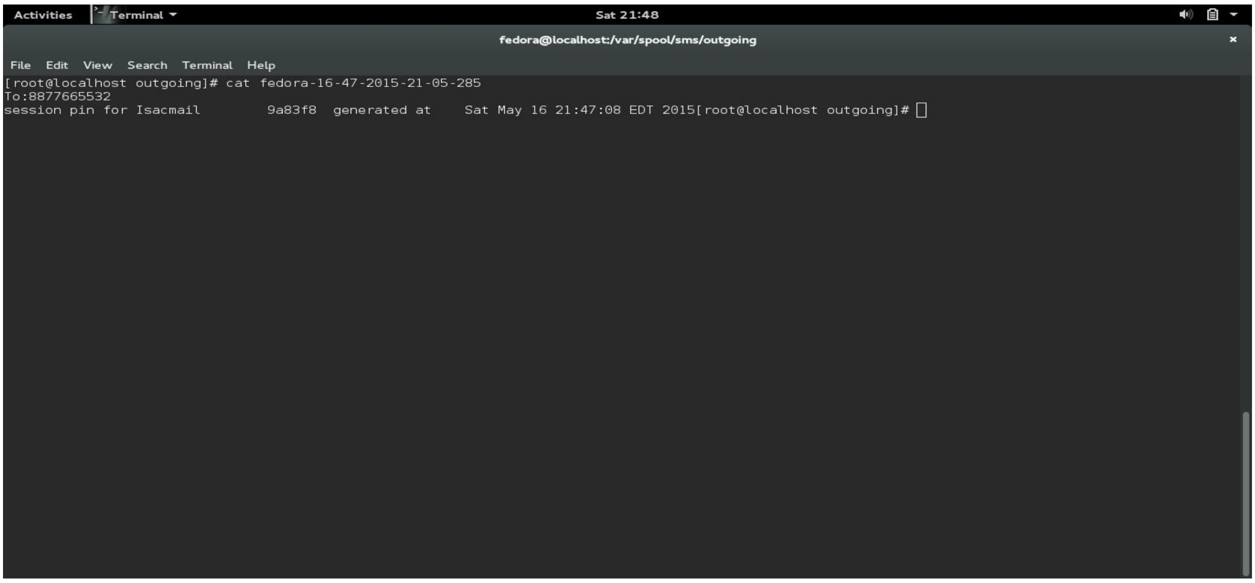


localhost:8080/webmail/Login.jwma;jsessionid=9F0250FB418D0AC5557B503F4E8654A0

Enter the Session pin

Fig 2 Figure showing page to enter session pin

The above figure shows the screen which would be displayed to the users who login after entering the correct username and password. If the username and password is found to be valid then the user would get this screen otherwise they will stay on the initial screen itself. The user has to provide the correct session pin each time he logs in to get access to his mail folder.

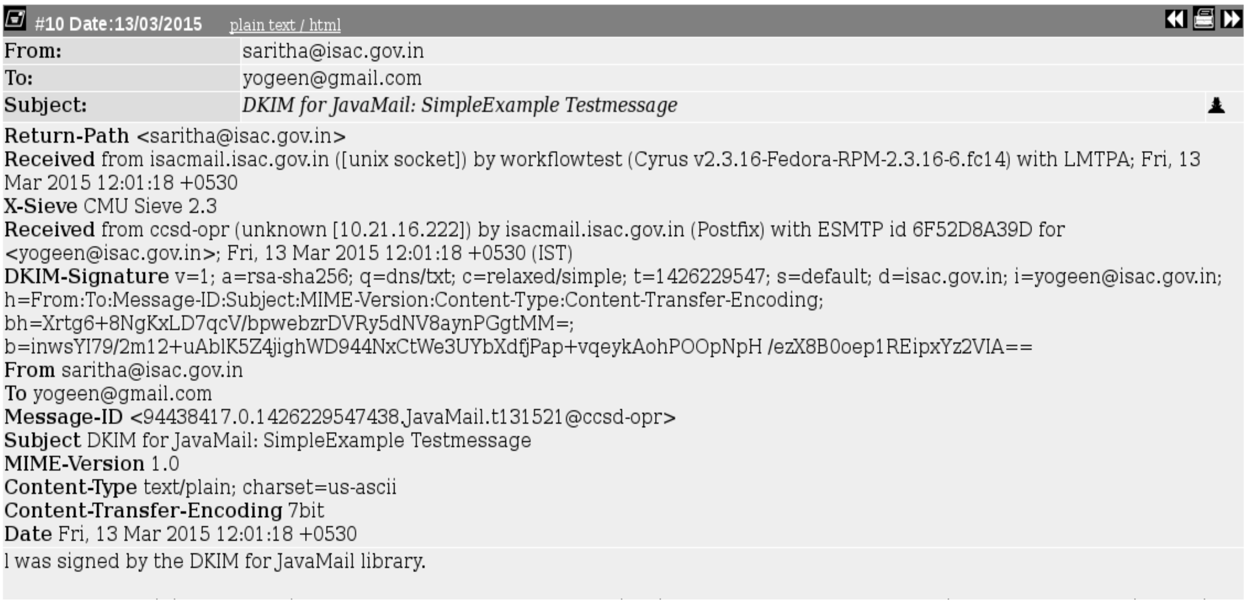


```
[root@localhost outgoing]# cat fedora-16-47-2015-21-05-285
To:8877665532
session pin for Isacmail        9a83f8   generated at    Sat May 16 21:47:08 EDT 2015[root@localhost outgoing]# 
```

Fig 3 File displaying password

DOI: 10.15680/ijircce.2015.0306057

The above screen shows the file in which the session password would be stored . Whenever the user provides the correct login details he would be directed to a page where he has to enter the session password. The user would get this password each time he logs in which would be send to the shown file and then would be sent as an sms to the user.



From:	saritha@isac.gov.in
To:	yogeen@gmail.com
Subject:	*DKIM for JavaMail: SimpleExample Testmessage*

Return-Path <saritha@isac.gov.in>
Received from isacmail.isac.gov.in ([unix socket]) by workflowtest (Cyrus v2.3.16-Fedora-RPM-2.3.16-6.fc14) with LMTPA; Fri, 13 Mar 2015 12:01:18 +0530
X-Sieve CMU Sieve 2.3
Received from ccsd-opr (unknown [10.21.16.222]) by isacmail.isac.gov.in (Postfix) with ESMTP id 6F52D8A39D for <yogeen@isac.gov.in>; Fri, 13 Mar 2015 12:01:18 +0530 (IST)
DKIM-Signature v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple; t=1426229547; s=default; d=isac.gov.in; i=yogeen@isac.gov.in; h=From:To:Message-ID:Subject:MIME-Version:Content-Type:Content-Transfer-Encoding; bh=Xrtg6+8NgKxLD7qcV/bpwebzrDVRy5dNV8aynPGgtMM=; b=inwsYI79/2m12+uAblK5Z4jighWD944NxCtWe3UYbXdfjPap+vqeykAohPOOpNpH /ezX8B0oep1REipxYz2VIA==
From saritha@isac.gov.in
To yogeen@gmail.com
Message-ID <94438417.0.1426229547438.JavaMail.t131521@ccsd-opr>
Subject DKIM for JavaMail: SimpleExample Testmessage
MIME-Version 1.0
Content-Type text/plain; charset=us-ascii
Content-Transfer-Encoding 7bit
Date Fri, 13 Mar 2015 12:01:18 +0530

I was signed by the DKIM for JavaMail library.

Fig 4 Digitally signed mails

The figure shows the outgoing mails from the organisation. As we adopt the technology of DKIM all the mails send from the domain would be digitally signed by using SHA 256 and RSA encrypting. Thus there would be a verification done based on the key provided in domain of all the received mails only afte which the mails would be directed to the user's mailbox.

VI. CONCLUSION

This paper discusses about the development of a secure mail client which provides a two factor authentication based on session pin generation and also reduces phishing and email spoofing by the use of Domain Keys Identified Mail. This is provided by using hash algorithms. Thus it is more secure than the existing mail clients which has only a single username and password authentication. As a future enhancement extra security feature other than using PGP or S/mime can be provided by creating a proxy server which could be placed in between the email client and the email server. In this the email client either generates self signed certificates or requests it from the Certifying Authority. Server also generates a self signed certificates or requests from Certifying Authority. A connection will be initiated only if the certificates could match each other thereby ensuring security.

REFERENCES

1. Xing Hu, "Development Of Textual Email Clients in java",University of Bath,2005
2. http://cds.unibe.ch/teaching/cn%20applets/IP_Spoofing/IP%20Spoofing.pdf
3. http://web.mit.edu/~bdaya/www/Network%20Security.pdf
4. S.Kent,RFC 1422,"Privacy enhancement for electronic mail: Part II :Certificate based key management",Obsoletes RFC1114, February 1993
5. Simson L. Garfinkel Erik Nordlander, David Margrave, effrey I. Schiller, "How to Make Secure Email Easier To Use"
6. B.Ramsdell RFC3851: "Secure or multipurpose internet mail extensions(s/mime) version 3.1 message specification", july 2004.