International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-3, Issue-1, March 2014

Pehchanmail: IBE Based E-Token Authenticated Secure Email

Rakesh Shukla, Hari Om Prakash, R. Phanibhusan, S. Venkataraman, Geeta Varadan

Abstract: ***Ubiquity and speed of email have made it increasingly effective to look in to the security aspect. Providing reliance over this medium has become an inevitable requirement and security has been a growing concern over the past few years. The average individual, who uses e-mail, naively believes that their e-mail is private and secure. The electronic world is filled with snoopers who can access all types of data over the network. In secure email and other secure communication, there is a major problem of key management. As the world goes digital, with more and more raw information about individuals available electronically, the need for security with hassle free key management increases. The emails of today are secured by encrypting the content on an external medium and sending this as an attachment over the mail. The paper discusses the implementation of providing security using any public identity information of the recipient and authenticating using cryptoki standard E-Token. Identity Based Encryption is a public-key cryptography which uses unique or exclusive data about the identity of an email client or a recipient to encrypt the data and later generates a public key corresponding to that unique/exclusive information. The unique information about the recipient can be his/her's email address in congregation with his mobile number or Social Security number. All these become parameters to create the public key. Time Stamp can also be incorporated to above parameters to create the public key. IBE is subset of larger set ABE (Attribute based Encryption) were one can enable automatic encryption of messages based on the attributes one chooses. The message gets decrypted on the recipient system regardless of the operating system. There are other systems that provide specific security but are strongly tied to the mail servers and browsers. A browser-based method allows the recipient to decrypt and read the secure message.***

Index Terms: Encryption, Decryption, IMAP4, SMTP, Symmetric key, block cipher, key, variable key, EToken, Cryptoki, Identity Based Encryption

I. INTRODUCTION

For the last so many years, one has become increasingly reliant on e-mail. It is ubiquitous, and unlike real mail it can chase from continent to continent in seconds. It is assumed that no-one else is going to be able to read an email, and that it can't ever get into the wrong hands. E-mail security has been a growing concern over the past few years. The biggest challenge in Email-Security or as a matter any kind of network security, is key management.

The major problems that ordinary e-mails suffer are data origin authentication and connectionless integrity apart from privacy. Also it is quite difficult with the ordinary e-mail to prove that the sender actually wrote the message, or that it has not been tampered with.

These days the requirement of secure mail also comes with the delivery to meet various decisions related to policies and should provide respite from the process of certificate and key management They want an encryption solution that is easy to deploy and use and meets policy requirements for secure communications. Pehchan mail is an easy to use secure email system which doesn't stress over the need for key management/certificate. Pehchan mail was developed as a strategic user requirement. Pehchan mail application provides following advantages:-

- Email clients can send email to recipients/recipients who have not yet setup a public key infrastructure
- There is no need to set up a PKI infrastructure before sending email as there is no requirement to obtain the recipient's public key certificate.
- It is taken care internally to keep changing the recipient's private key every short time period
- Pehchan mail reduces the overhead of the PKG server by contacting only once, to get the private key corresponding to a given identity information.

Usage of E-token not only takes care of the authentication but also helps in storing the private key received once from PKG corresponding to a given identity information in a safe and secure way.

II. GOAL

To provide Email Security using Identity Based Encryption [3] in a web based environment with a hassle free key management. The basic features like Confidentiality, Integrity, Authentication, Non-Repudiation and Availability have to be taken under the security head.

III. APPLICATION

This email security solution [7] is designed to work in a pluggable mode and can be made to work in any current/existing email setup (with any email server). This means that the old emails will open in a normal way without any security mechanism. The application uses IMAP4 and SMTP for retrieving the emails and sending the emails respectively. Security in the application has been designed to provide confidentiality, authentication and integrity. This solution provides security at the client end which is independent of intermediate securities like mail server security, communication channel security, etc. It uses the concept of plug-ins which one can plug into a mail client.

Revised Manuscript Received on 30 March 2014.
* Correspondence Author
Rakesh Shukla*, Department of Space, ADRIN, Secunderabad, India.
Hari Om Prakash, Department of Space, ADRIN, Secunderabad, India.
R. Phani Bhushan, Department of Space, ADRIN, Secunderabad, India.
S. Venkataraman, Department of Space, ADRIN, Secunderabad, India.
Geeta Varadan, Department of Space, ADRIN, Secunderabad, India.

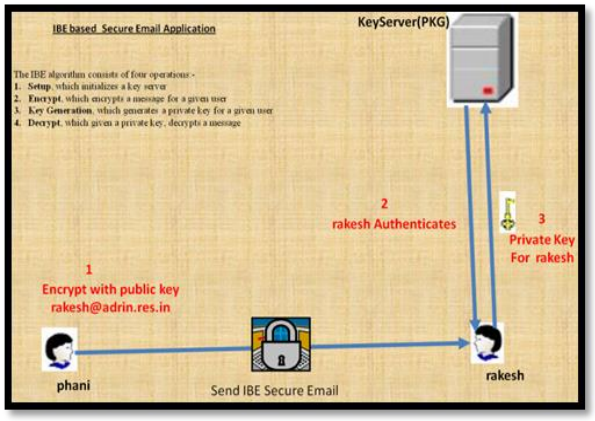


Fig 1: IBE Flow diagram

An IBE algorithm mainly works in four phases:
Setup: This phase initializes a key server
Encryption: This phase encrypts a message for a given email client.
Key Generation: This phase is involved in generating a private key for a given user
Decryption: This phase is involved in decryption of message which given a private key.

i. Unsecure mail: These emails are sent without any security and are ordinary emails.
ii. Secure Email: These emails are provided a wrapper of security covering the various aspects of security like authentication, confidentiality, privacy.
iii. Speaking Email: This option has been added in the application to prevent shoulder browsing. The emails are invisible in this option and emails can only be heard as a voice. Speech part of the email uses SAPI-5.0.
iv. Single Hop Email: These mails cannot be forwarded. These mails can be only read. The contents of the email cannot be copied and print screen facility also gets disabled as these mails are opened.

The application has been designed to cater to multiple users as 'cc' and 'bcc' with individual session keys encrypted with individual public keys of recipient. The Fig 1 shows the message frame format [4]. The architecture diagram of the application is also shown in the Fig 2 below.

IV. SECURITY

IBE uses the concept of "bilinear map" for providing security. Bilinear mapping is a type of pairing that has the property defined below [8]:
Pair (a o X, b o Y) = Pair (b o X, a o Y)
The operator "o" is multiplication of a point on an elliptic curve by integers. In IBE the multiplication is easy but finding the inverse operation is practically impossible. Two bilinear mappings which are extensively used across the globe are Weil Pairing and the Tate Pairing [1]. The above example can be explained in this way that we can calculate aoX without much operations but calculating, the inverse assuming that X and aoX are given is practically impossible [2]. This is where the security of IBE is into action.

A. Confidentiality

The confidentiality or privacy issue of the application has been addressed by using a 448 bit symmetric key algorithm. It is a formidable block cipher which is speedy, compact, simple, and very secure. The cipher encrypts 64 bit blocks of plain text into 64 bits blocks of cipher text. It uses variable size key ranging from 32 bits to 448 bits. F function in the algorithm is very difficult to unscramble the substitution performed by F function. The block cipher encrypts data at a rate of 18 cycles per byte. It can run in less than 5 K of memory. Sub-key calculation requires all sub keys to be calculated advance of any data encryption. The random session key of 448 bit length is generated and used for encryption of the payload that is message as well as attachment. This randomly generated 448 bit session key is encrypted with public key generated from the identity of the recipient(s) which is email id in this case.

B. Message Integrity and Non-Repudiation

Issue of message integrity is addressed by using SHA-1 and RSA. The message to be send is hashed and the value which comes out is sent as an input for digital signature. The public key which is the public identity of the recipient(s) is used for encrypting the hash function. In our case the public key will generated from the identity of the email id of recipient(s). The hash function is encrypted private key of the sender and public key of recipient to form a bi-directional digital signature. Identity based encryption doesn't address the issue of non-repudiation, but using the above strategy the issue of non-repudiation is addressed.

C. Authentication

Authentication in the application is achieved by using the following technique:
Password (what you know): Password which authenticates the email account is asked at the start of the system.
E-Token (what you have): The E-tokens [6] are USB based devices and use Cryptoki standard as defined in pkcs11. An E-token device is to be inserted before any email is being sent or email is being viewed. E-Token device asks for a user id and password which when entered, authenticates the user. The eToken Initialization option restores an eToken to its initial state. It removes all objects stored on the eToken since manufacture, frees up available memory, and resets the eToken password, allowing administrators to initialize the eToken according to specific organizational requirements or security modes. E-Token enables setting token policies, performing basic token management functions. In addition, E-Token provides users and administrators with a quick and easy way to transfer digital certificates and keys. E-Token Properties include an initialization feature allowing administrators to initialize tokens according to specific organizational requirements or security modes, and a password quality feature which sets parameters to calculate an eToken password quality rating. Initializing an eToken is useful, for example, after an employee has left a company. It completely removes the employee's individual certificates and other personal data from the eToken, leaving it ready to be set up and used by another employee.
The following data is initialized:-

- E-Token Name
- User Password
- Administrator password (optional)
- Maximum number of Logon Failures (for user and administrator passwords
- Requirement to change the password on the first log on
- Initialization key

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

An E-Token is not to be removed from the USB port during an operation. Many operations, such as private key request, require multiple actions. If the token is removed during one of these actions, the data structure on the token need to be reinitialized.

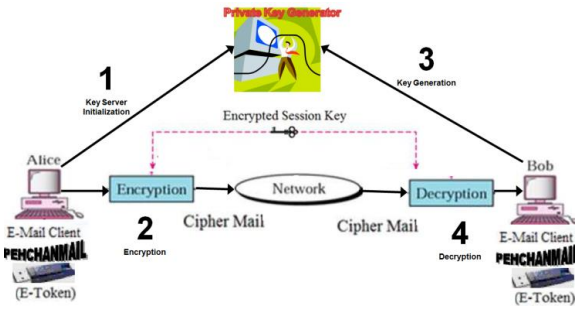


Fig 2:Pehchan mail flow diagram

V. PKG (PRIVATE KEY GENERATOR)

A private key generator (not public key) is a very important entity for is responsible for generating the private key for the mail client [3]. The email recipient sends a request for the private key to the PKG.As the system assumes a trusted environment, registration of the email client is not required. In case of public environments we can invoke registration of the email clients and it can be made mandatory. If the registration of specific email client is not there, private key will not be generated for such clients. The private key which is transmitted is symmetrically encrypted using CBC version of modified 448 bits blowfish algorithm with the hashed password (using SHA 256) to work as the key.

VI. WORKING

When the user client logins into the system he has to invoke the system. The https enabled SSL connection is invoked to login to the web server. Once the login page comes, the user enters the email id and password. After this process the user is asked to insert the E-Token into the system. User checks for the E-token and invokes password to be entered. The correct password completes the authentication phase correctly. After this the email client which is sending the email connects to the PKG and register's itself. This is a onetime process. If the email client has already logged in before, he or she need not register with the PKG. The registration process is purely automatic. For composing the email the user clicks on the compose message option. Once the user presses the send button a session key is generated, which is of 448 bit key length [5] and encrypts the complete payload i.e. the message and any attachment(s).After this based on the email id of recipient (s) in To:, CC, BCC, public key is generated and this public key encrypts the 448 bit session key and is attached with the payload. In case of multiple recipients this session key is encrypted separately for all public keys of the recipients and added to the payload. This eases the process during decryption as the specific recipient can choose his encrypted session key and decrypt using his private key. During the delivery of the email, the recipient contacts the PKG or private key generator. PKG generates each email client or the recipients (in our case) private key. As long as an entity has registered to RS, he/she can send a private key request to PKG, in order to receive the private key. For security reasons the transmitted key is encrypted using modified blowfish 448 bits with the password of the email taken as key. This is done by taking 448 bits from concatenating hash of password three times and choosing the 448 bits. Once this process gets completed and private key is received, the E-Token also stores the key in a safe way and can be invoked again for the same identity. The final payload which is creating during the sending of email includes encrypted payload, containing both message and attachments, session keys encrypted using the public key of different recipients. This makes easy for specific recipient to pick up his her encrypted key. Along with this the payload consists of bidirectional digital signature of the content that is message digest , encrypted with the private key of sender (received from PKG) and also encrypted with public key of various recipients. This complete content is zipped and base64 is applied over and above it. A brief description of the complete message frame format is shown in Fig 3 below. Concept of bi-directional digital signature is used for non-repudiation by encrypting the output of hash function with the private key of the sender and then the public key of the recipient. When Single Logon mode is enabled, users can access multiple applications with only one request for the eToken password during each computer session. This alleviates the need to log on to each application separately.

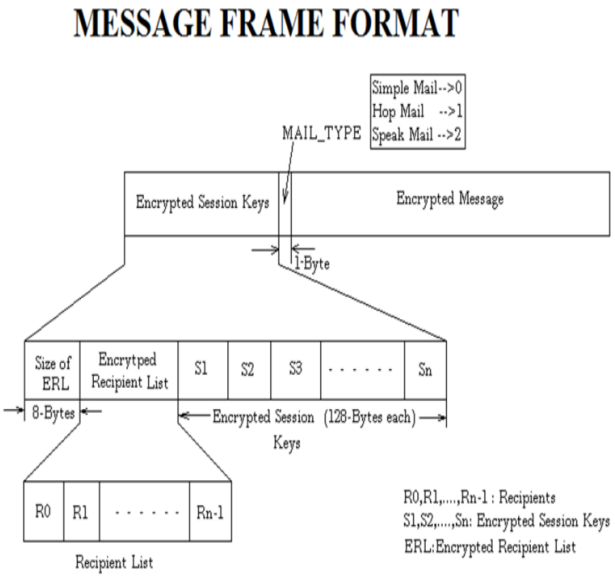


Fig 3:Message frame format

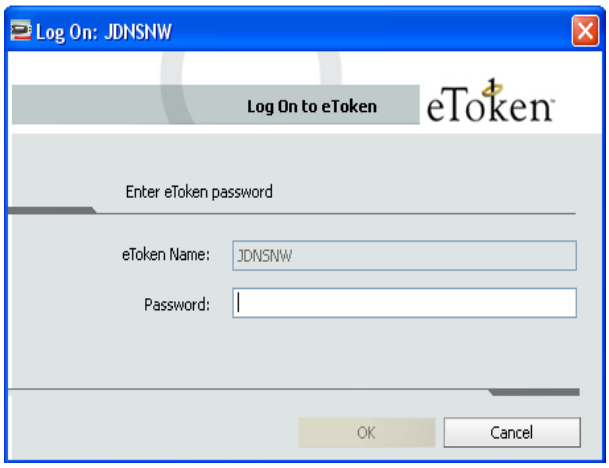


Fig 4:E-Token authentication screen

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

VII. SCREENSHOTS

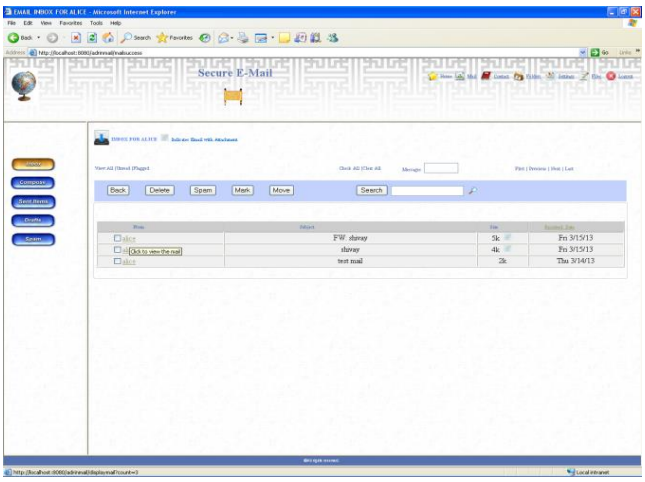


Fig 5:Inbox display

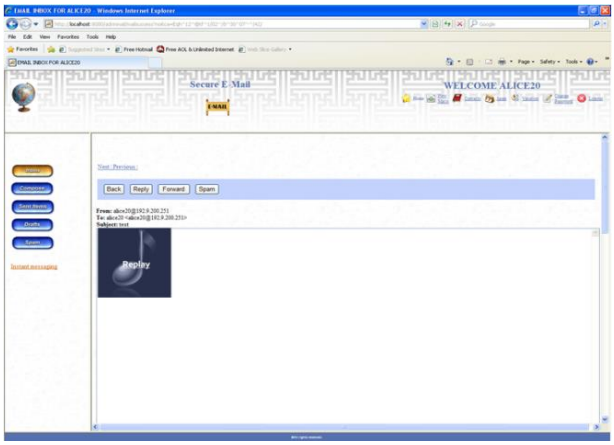


Fig 6:A speaking email window

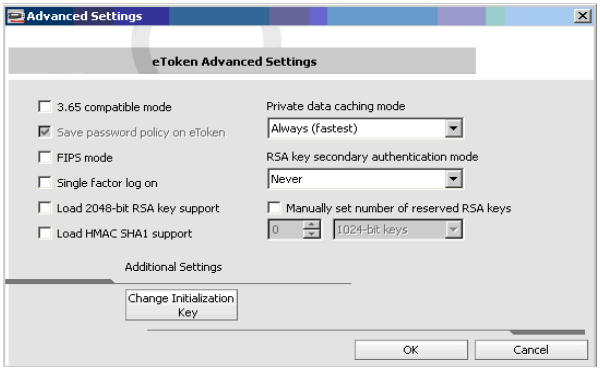
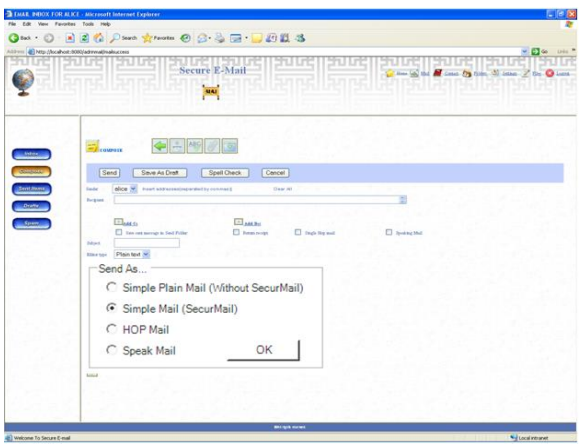


Fig 7:E-Token advanced settings



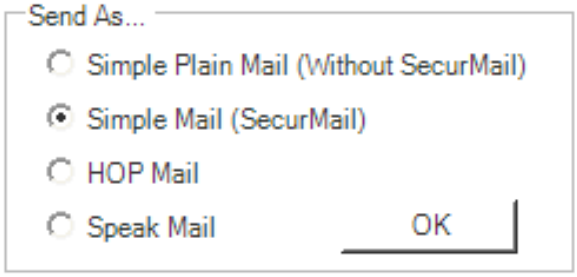


Fig 7:Options while sending email

VIII. CONCLUSION

The application was developed with objective of providing security in a web kind of environment using IBE. This was done to remove the hurdle of key management and public key certificate. This concept can be implemented for MANET security as well. The application uses POP3 and SMTP but can be made to work for IMAP4, POP3, SMTP (and also IMAP4S, POP3S, and SMTPS). Further developments have been proposed in the direction of giving option of self destruction email. Such emails get destroyed automatically, after single display and no traces are left in the email server. This facility will be helpful for strategic users. Future developments also include implementation of Virtual E-Tokens. This saves the user to carry the hardware physically for authentication and also avoids the cost for purchase involved behind the E-Token hardware.

REFERENCES

1. D. Boneh and M. Franklin, “Identity based encryption from the Weil pairing”, in Proc of Advances in Cryptology - Crypto 2001, LNCS
2. Rakesh Shukla, Hariom Prakash, R. Phani Bhushan, "Sahastradhara Biometric and Etoken Integrated Secure Email System", IEEE ICACT-2013. pp. 000-000 Published in Advanced Computing Technologies (ICACT), 2013 15th International Conference , 21-22 September, 2013 Pages 1-4 Print ISBN 978-1-4673-2816-6 , INSPEC Accession Number: 14066359 , DOI 10.1109/ICACT.2013.6710516
3. Identity-Based Encryption from the Weil Pairing, pp.213–229, Springer-Verlag ,London UK, 2001 , CRYPTO 01 Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology.Pages 213-229, ISBN:3-540-42456-3
4. FortiMail Identity Based Encryption.:
5. http://www.fortinet.com/sites/default/files/whitepapers/FML_WP_IBE.pdf
6. Information Encryption for Email, Files, Documents & Databases http://www.voltage.com/technology/identity-based-encryption
7. Bruce Schneier, Applied Cryptography--Second Edition, pp. 8. ISBN 0-471-11709-9
8. E-Token help information PKI version 4.55.22.
9. http://www.safenet-inc.com/data-protection/data-encryption-control/
10. Practical Implementation of Identity Based Encryption for Secure E-mail Communication
11. http://ieeeplore.ieee.org/xpl/freeabs_all.jsp?arnumber=5600456&abstractAccess=no&userType=inst Informatics (PCI), 2010 14th Panhellic Conference Date: 10-12 Sep,2010 ISBN : 978-1-4244-7838-5 INSPEC Accession Number: 11598030 DOI 10.1109/PCI.2010.48

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)