USB BASED SECURE E-MAIL

Rakesh Shukla[1], Garima Kuchhal[2], R.Phani Bhushan[3],
S. Venkataraman[4], Geeta Varadan[5]

ADRIN, Department of Space, Govt of India, Secunderabad, Andhra Pradesh
[1]rakesh@adrin.res.in [2]garima.kuchhal@adrin.res.in
[3]phani@adrin.res.in [4]kalka@adrin.res.in [5]geeta@adrin.res.in

ABSTRACT

E-mail Security[1] 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. As the world goes digital, with more and rawer information about individuals available electronically, the need for security increases. Ubiquity and speed of email have made it increasingly effective. So providing reliance over this medium has become an inevitable requirement. There are other systems that provide specific security and are strongly tied to the mail servers and browsers [4]. To overcome this problem we propose HID Device based Secure E-mail which is immune to root kits, botnets, man in the middle attack, phishing.

KEYWORDS

Encryption, Decryption, POP3, SMTP, Symmetric key, block cipher, key, variable key, USB, XML Encryption

1. INTRODUCTION

USB Based E-mail Security Software deals in providing email security using SSL along with security plug-in with symmetric key encryption and PKI Based Asymmetric key encryption (public key and private key stored in the USB) between client and web server, and secure variable key block cipher with base-64 encoding, between web server and email server. SSL certificates are self signed generated using OpenSSL with SSL protocol (port 8443).

The USB based Secure E-mail Access System consists of an USB device which is ergonomically designed hardware based on the USB interface [13]. The device has a finger print scanner (biometric) for user authentication. The device has flash memory to store the reference fingerprint database. It prevents the misuse of the user fingerprint database and also any mechanical opening of the device. It turns its self destruction mode ON after three wrong authentication attempts (here finger print scan). It destroys the fingerprint information; device memory etc. on the device by writing unwanted information or garbage over the memory area. Every device has its own 16 digit Unique ID (UID). After customization the device is set to read-only mode so that nothing can be written on it. The crucial part of complete

System is that after booting the system through USB, it disintegrates the hard disk of the host system. This makes the web browsing totally secure without leaving the traces of the work done on the host system.

David C. Wyld (Eds) : ICCSEA, SPPR, CSIA, WimoA - 2013
pp. 183–192, 2013. © CS & IT-CSCP 2013 DOI : 10.5121/csit.2013.3519

Without the USB device [14], the Secure Speaking E-mail Software cannot be accessed. The mandatory biometric authentication is made available through USB only. Cryptography key pairs also reside in the USB device without which the software will not function.

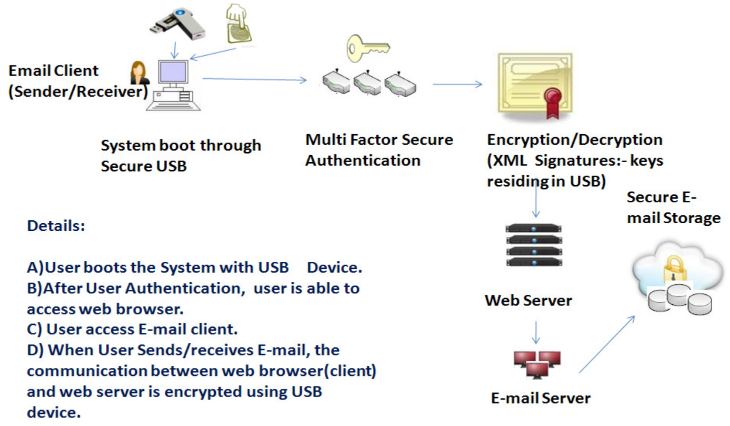
2. GOAL

To provide E-mail Security [7,8] application through USB device. The basic features like Confidentiality, Integrity, Authentication, Non-Repudiation and Availability have to be taken under the security head.

3. SOFTWARE COMPONENTS

The secure email security solution uses POP3 [5,6] for retrieving the emails and SMTP [3] for sending the emails. The Software works in a 3 tier architecture mode:

1. Web browser as client (HID Device)
2. Web Server as middle tier
3. E-mail Server as third tier



Details:

A)User boots the System with USB Device.
B)After User Authentication, user is able to access web browser.
C) User access E-mail client.
D) When User Sends/receives E-mail, the communication between web browser(client) and web server is encrypted using USB device.

Fig. 1. Flow diagram

4. SOFTWARE FEATURES

4.1. Single Hop Email

The emails, which are sent under this category, can only be read. Such emails cannot be forwarded further and gets deleted after a certain span of time. Such mails cannot be saved. The contents cannot be copied. Copy and paste and other such keys are disabled in case of single hop emails. Even the print screen facility is also disabled for such emails. We tried to get the print screen figure of this facility to show how it works but could not as the print screen facility was not working in this case.

4.2. Speech Mode

The Emails, which are marked as speaking mails, will be read aloud when opened at the client side. This facility can be used for persons who are blind. The output speech of such emails can be taken onto a headset (a Bluetooth or a normal headset). The emails which are read are not visible and only the voice can be heard. Two accents for voiceare available, namely British and American English. These accents can be selected before the start of the software. The security is fully taken care in this mode. In speech mode the security is taken care with the speech content being decrypted at client side.

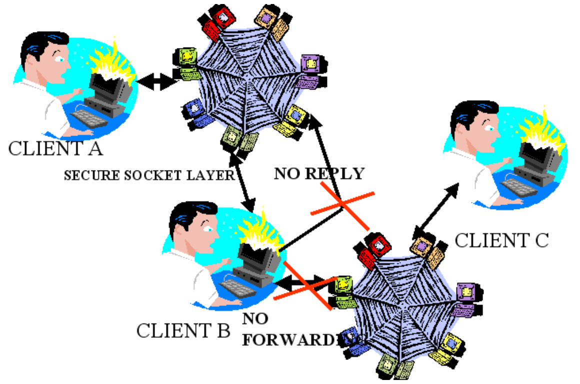


Fig. 2. Single Hop Email

Permission can be set to make the contents viewable in case of speaking emails.

4.3. Spam filter

It takes care of the Spam and unsolicited mails. The facility of content filtering is incorporated to remove any unwanted contents like attachments with extension exe, com, pif etc. Contents with attachments like exe/zip/com/pif etc. can be stripped right before entering the user inbox.

4.4. Attachments

For sending the attachments there is no limit on the size and the number of attachments. But the same can be set, by the administrator based on the policy of the organization/clients.

4.5. Vacation Mail

The facility of vacation message is provided for taking care of the client’s emails when he/she is on leave. If a particular client is on vacation then he can set default reply to all mails and same reply will be sent to all mails received.

4.6. Acknowledgement

To confirm the receipt of the e-mail, sender is prompted with an option of acknowledging the sent mails.

4.7. Auditing/logging

It is done at the administrator level by recording each and every minutest detail of the operations done by each client. Such log files can be mined for retrieving important information.

5. SECURITY ASPECT

Strong user authentication is the paramount requirement for web computing that restrict illegal access of web server. The proposed Secure Web server Application framework provides identity management, multi factor client authentication, user privacy, session key establishment between the users and the web server through Authentication Server. Since a web server is generally vulnerable to several hacking attacks which means, it is more efficient to split the authentication process of the client between the web server and an Authentication Server.

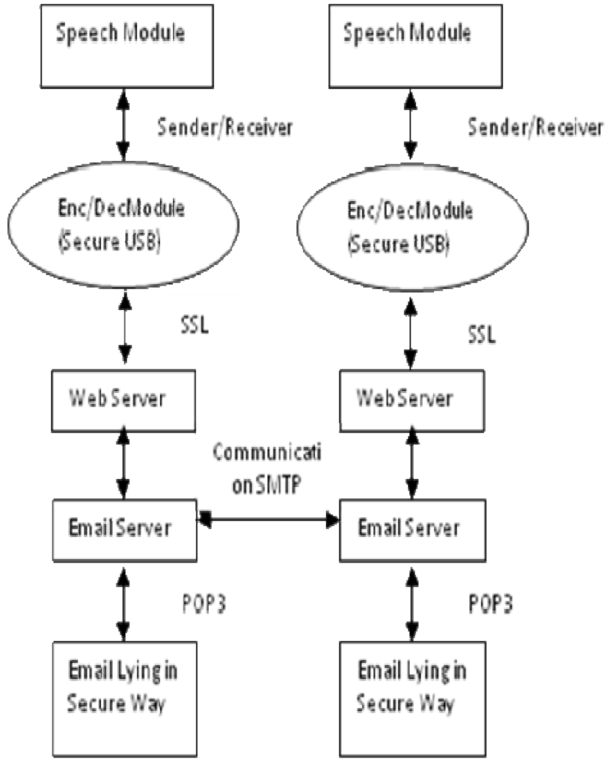


Fig. 3. Sequence/Data Flow diagram

The security of the software is taken care with SSL and security plug-in between the client and the web server. SSL, Secure Socket Layer protocol works on the default port of 443 and provides end to end security between any client and web server. It uses 128 bit key for internal encryption. The protocol works on the transport layer and hence is application independent. SSL takes care of the basic security considerations of integrity, privacy, confidentiality and non-repudiation. Apart from this security plug-in form the second layer of security. The security plug-in form the end to end security using an indigenous symmetric key block cipher algorithm. Third and last layer consists of the security in the form of symmetric block cipher (with key size 448 bits) in a CBC mode with changed IV (initialization vector) with Base-64 encoding. Present framework strengthens security without compromising usability and ubiquity. The solution approaches classical forms of shared-secret as username, password, hashing with see. It also implements multifactor authentication.

Multifactor authentication refers to a compound implementation of two or more classes of human-authentication factors:

- Something known to only the user—Knowledge-based (password).
- Something held by only the user—Possession-based (USB Dongle)

.

- Something inherent to only the user—Biological or behavior biometric traits (fingerprint).

Apart from SSL an additional layer of security is incorporated in the application. All the mails communicated/transferred are encrypted at the web browser level (in USB [14]) and further decrypted in the web browser only. This step strengthens the security independent of the web server. Here whatever mail is transferred on the network channel is itself encrypted apart from SSL. Security is ensured between each mail communication (mail sender and mail receiver). A Symmetric key is generated at each transaction between server and client. The data is encrypted with the symmetric key and cipher text is transmitted. The symmetric key is encrypted by RSA key to enhance the security measures. Asymmetric Key pairs are hard coded on the USB device at the time of its customization.

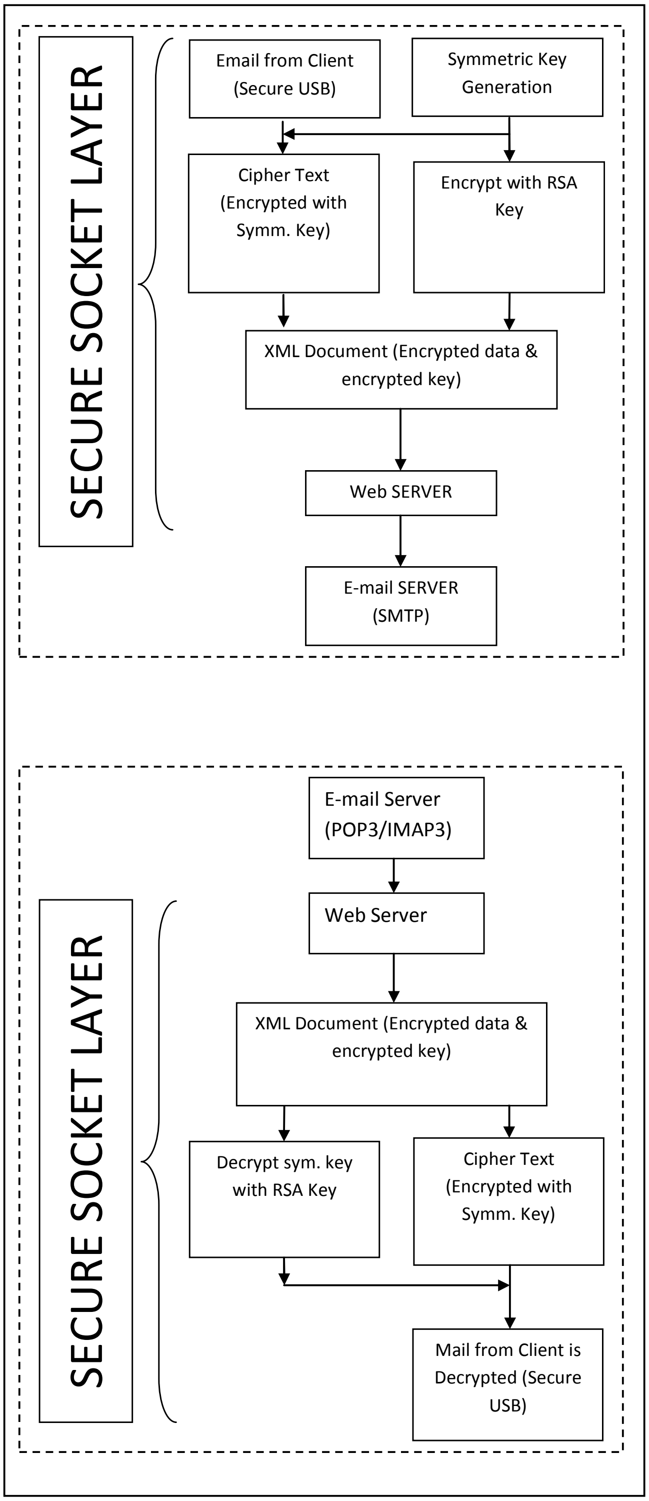

SECURE SOCKET LAYER
Email from Client (Secure USB)
Symmetric Key Generation
Cipher Text (Encrypted with Symm. Key)
Encrypt with RSA Key
XML Document (Encrypted data & encrypted key)
Web SERVER
E-mail SERVER (SMTP)
SECURE SOCKET LAYER
E-mail Server (POP3/IMAP3)
Web Server
XML Document (Encrypted data & encrypted key)
Decrypt sym. key with RSA Key
Cipher Text (Encrypted with Symm. Key)
Mail from Client is Decrypted (Secure USB)

Fig. 4. Encryption of the mail at the client and send to the web server along with decryption of the mail received.

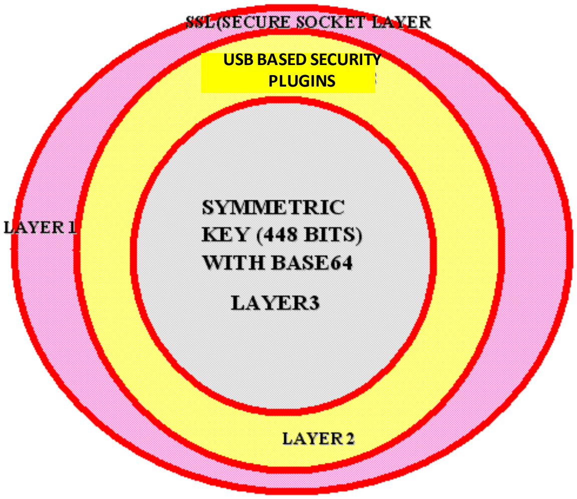

SSL(SECURE SOCKET LAYER
USB BASED SECURITY PLUGINS
LAYER 1
SYMMETRIC KEY (448 BITS) WITH BASE64
LAYER3
LAYER 2

Fig. 5. Security Aspects

5.1. XML Signatures

XML is used for communication between client and server. Since the whole communication is secure, the need is of trustable and secure XML messages for transactions. One key to enables

```
<mail>
<encdata>
            3A:A4:EF:23:E9:C7:AD:93:4D:9F:5A:C4:E7:B3:AF:C0:2
B:92:B3:0D:9D:D3:38:8E:30:D0:67:06:A7:F3:96:32:32:31:FE:66:F1:
A8:40:64:C6:4D:56:B4:D7:F5:1F:20:77:C9:AC:7E:69:76:39:E4:15:1B
:D1:6C:0A:12:F0:92:D6:00:E7:98:34:B0:2E:13:0D:06:FF:80:2C:9F:C
7:F1
</encdata>
<keydata>
            51:47:7B:AA:C2:6E:E1:79:19:60:2F:12:3E:4F:63:43:55:9E
:AD:4A:EE:97:39:64:2D:F3:20:1A:CD:60:B4:FE:FB:FA:18:54:E9:2B
:E4:D3:6F:B9:94:1E:99:F0:AF:F0:A3:10:73:81:E7:49:75:0A:21:F9:E
E:3A:BB:65:06:13:A2:6E:BD:85:E5:EB:48:0F:49:D1:3F:D7:CE:1F:5
F:DF:2F:55:72:37:C2:99:4A:BE:F6:29:DC:86:ED:B7:FB:BD:27:71:6
7:50:22:69:47:80:08:9D:4C:98:65:0D:47:91:F7:15:E9:8A:A5:EC:97:1
0:28:A7:71:1B:75:B6:5D:33
      </keydata>
</mail>
```

Fig. 6 Cipher Text through XML Encryption

secure transactions is the concept of a digital signature, ensuring the integrity and authenticity of origin for documents. XML signatures are digital signatures which add authentication, data integrity, and support for non-repudiation to the data that they sign. They address the special issues and requirements that XML presents for signing operations and uses.

XML syntax for capturing the result, simplifying its integration into XML applications. XML Encryption provides end-to-end security and is the natural way to handle complex requirements for security in data interchange applications. It addresses following areas: - Encrypting part of the data being exchanged and securing the sessions. Figure 6 shows a typical Cipher Text through XML encryption.

6. SECURITY ANALYSIS

6.1. User privacy

The framework never transmits emails in plaintext form[8]. All the messages are transmitted over the public channel in encrypted form.

6.2. Multi Factor Authentication:

User requires both simple credentials (user id and password) and hardware tokens (USB Device) in order to gain access. The combination of the "known", "held" and "biometric factors" [9] makes up the multifactor authentication method, and significantly improves the authentication strength, as it curtails the threat of stolen digital identities.

6.3. Transaction key management:

A session is established between the user and the server after authentication process. The transaction key is different in every client-server communication throughout the session.

6.4. Man in the middle attack:

The client private keys are not known to anybody else as they are present in the USB device only. Similarly ID and PW are with the client only. Three wrong finger print scan will destroy the device (Tamper proof).

6.5. Impersonation attack:

The framework never transmits user ID and PW directly through the public channel. Instead, ID and PW are transmitted in encrypted form. The hash value of unique id of the Secure USB Dongle is transmitted through out the communication (encrypted form). Also the framework stores the h(PW) and h(UID) at the server. And also the Secure USB device has tamper protection through biometric authentication (finger print scan).

6.6.Password guessing attack:

The framework allows user to have only strong passwords. Weak passwords or easily guessable passwords are not allowed. Passwords should be minimum of 12 characters, must have at least one number, one special character, no blank space and first character should not be an alphabet. Moreover three wrong password attempts will block the Secure USB device for next 24hrs.

6.7. Insider attack:

Insider attack is the most hazardous threat to any inter-networking system. In the application the password is never used openly, instead, it is digest h(PW). Moreover, attackers need the user private key, and the USB Device [15] to get access to the web server. Only a genuine user can provide private key, password and secure USB device (with biometric authentication) simultaneously.

6.8. Fiestel Cipher:

The block cipher uses the operations, which are performed on both the halves of the data (i.e. 32 bits each) in each round. This enhances the cryptographic strength (additional operation is linear XOR).

6.9. Brute Force Attack:

It is quite invulnerable as the key length can go up to 448 bits [2]. To add to this the sub key process is very length with 521 executions required for a single key test.

6.10. Cryptanalysis:

Some tests have been done to cryptanalyse the algorithm but till now no practical weaknesses have been found [10].

7. CONCLUSIONS

The application was developed with objective of providing E-mail security [11] in a restricted secure environment. The application uses POP3, SMTP and has been tested to work for IMAP3 [6], POP3S, SMTPS and IMAP3S. The Standard HID provides Limited network accessibility without any need of antivirus. On the top of it no trace of user actions either on host system or the USB device are left. This further strengthens the security and maintains the privacy of the user/client. Last but not the least ultimate goal is carrying the Secure E-mail access device along with.

REFERENCES

[1] How to: Perform Actions When an E-Mail Message Is Received [http://msdn.microsoft.com/en-us/library/ms268998(VS.80).aspx].

[2] Bruce Schneier, "Applied Cryptography—Second Edition," pg. 8.

[3] Postel, J.,"Simple Mail Transfer Protocol", STD 10, RFC 821, USC/Information Sciences Institute, August 1982. [http://www.faqs.org/rfcs/rfc821.html]

[4] Crocker, D., "Standard for the Format of ARPA-Internet Text Messages", STD 11, RFC 822, University of Delaware, August 1982. [http://www.faqs.org/rfcs/rfc822.html]

[5] Dover Beach Consulting, Inc. "Post Office Protocol - Version 3", RFC 1725, Carnegie Mellon, November 1994. [http://www.faqs.org/rfcs/rfc1725.html]

[6] M. Crispin, University of Washington "Internet Message Access Protocol – Version 4", RFC 1730, December 1994. [http://www.faqs.org/rfcs/rfc1730.html]

[7] Douglas R. Stinson,"Cryptography Theory and Practice".

[8] Bruce Schneier, David Banisar," The Electronic Privacy Papers: Documents on the Battle for Privacy".

[9] Bruce Schneier," E-mail Security: How to Keep Your Electronic Messages Private".

[10] Bruce Schneier," E-mail Security".

[11] Bradley F Shimmin,"Effective E-mail Clearly Explained: File Transfer, Security, and Interoperability".
[12] [http://news.cnet.com/IBM-brains-capture-a-PCs-soul/2100-1041_3-5830870.html]
[13] Boot from a USB Drive Even if your BIOS Won't Let You (How-To Geek)
[14] [http://www.pendrivelinux.com/2007/11/21/use-a-floppy-to-boot-usb-pendrive-linux/ boot floppy for live USB]
[15] [http://www.pendrivelinux.com/usb-minime-2008-install-from-windows]

Authors

Rakesh Shukla is working in the Systems Engineering Group, ADRIN, Dept. of Space, as Sci./Engg. "SE" and involved in developing applications on network and data security. He can be contacted at *rakesh@adrin.res.in*

Garima Kuchhal is presently working in Systems Engineering Group, ADRIN, Department of Space, as Sci/Engr. 'SC' and involved in development of secure web based applications. She can be contacted at garimakuchhal07@gmail.com

Mr. R.Phani Bhushan is working as Section Head, Data Security Section under the Systems Engineering Group, ADRIN, Dept. of Space. He is involved in developing applications on Mobile Ph ones based on GSM/GPRS technology besides leading a group involved in development activities in both host based and network based security. He can be contacted at phani@ *adrin.res.in*

Dr. S. Venkataraman, is the Group Director and heading the Systems Engineering Group. He can be contacted at kalka@ *adrin.res.in*

Mrs. Geeta Varadan is Director, ADRIN, Dept. of Space. She can be contacted at geeta@ *adrin.res.in*