A Work Paper on Email Server using 3DES

Dubbewar prasad[1], Dornal akshay[2], Manisha K.M[3]

[1,2]Student: Computer Science & Engineering Department, Sanjay Ghodawat Group of Institutions
[3]Assistant Professor: Computer Science & Engineering Department, Sanjay Ghodawat University

---

Abstract: *Any network is vulnerable to malicious use and accidental damage unless it's properly secured. Hackers, disgruntled members, or poor security practices within the organization can leave private information exposed, including trade secrets and customers private details. Losing confidential research such as, the potentially cost an organization millions of dollars by taking away competitive advantages it paid to gain. While hackers stealing customers' information, and selling them to be used in fraud, creates negative publicity and public misuse of the organization. So security is a must to keep data safe.*

Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are used for three times to every data block. The key size is increased in Triple DES to check additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are mentioned as bundle keys with 56 bits per key. Here the user entered key is distributed to receiver or sender via SMS or EMAIL.

Keywords: 3DES algorithm, SSL Security, 3DES Encryption , OTP Authentication , 3DES Decryption

1. Introduction

Email It's in common use to share data with help of server offering services with other users, friends etc. E.g. Such sharing the data or vice versa (e.g. Profile information, health or property records, etc.). It's always the users responsibility to safeguard own data and avoid misuse of it. It becomes a challenge for user to protect self-data on email network, to overcome this scenario it is important to design and allocate secured access control to the data until the expiry period. Basic can be to store the data in encrypted format but disadvantage with classic encryption is the owner should know what information the users wants to share and with whom this makes the process to sharing the data to many a bit hectic. To overcome this disadvantage we have Triple DES encryption which enables one to many encryptions Triple DES has the ability to provide data security as well as access control to the minimum level.

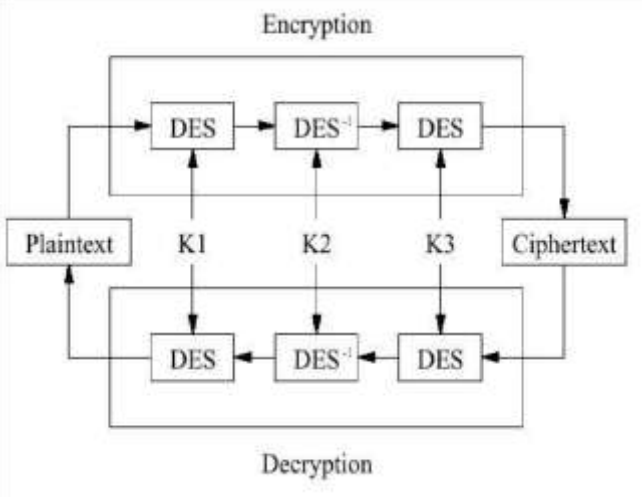

Fig 2: General Depiction of 3DES

2. Literature Survey

In order to know in detail about this survey the previous research work done in this direction, several studies dedicated to the topic were referred. The literature survey is done in chronological order from 1996-2016.

Chris J. Mitchell in 2016, [1] has stated that an encryption technique that remains widely used despite recently being de-standardised and constituting the first advance in cryptanalysis of 2-key triple DES since 1990. They give future attack

enhancements that together implies that mostly used estimate that 2-key 3 DES provides 80 bits of securities can no more be regard as conservativation. Finally whilst not completely broken, the margin of safety for 2-key triple DES is slim, and efforts to replace it, at least with its 3-key variant, should be pursued with some urgency.

Mohamed hamdy Eldefrawy, khurram Khan has used Two-factor authentication (2FA) provides protection, since cutomers are encouraged to provide something they observe and something they have it. That technique deliver a higher-level of authentication assurance, which is easy for online banking securities. They presented a two-factor authentication scheme whereby a user's device produces multiples OTPs from an initial seed using the proposed scheme. The initial seeds is produced by the communications partners' unique parameters. They applied many from one function to a certain seed removes the requirement of sending SMS-based OTPs to users, and reduces the restrictions caused by SMS.

D. Coppersmith and D. B. Johnson proposed a next mode of multiple encryption 3-DES external feedback cipher block chaining including output feedbacks masking. They provided protection against certain attacks which exploit the short message-block size of DES. They implemented secret mask value which is derived from a fourth encryption operation per message block, in addition to the three used in previous mode. The new mode is part of encryption mode proposed in the ANSI X9.F.1 #-DES draft standards (X9.52).

Devashish Kumar Amit Agrawal they shown that the OTP which was developed as a part of two factor authentication is weak point to attacks. In this paper, they represented a new framework for improving authentication during online transaction which secures our OTP.

Table 1.1 Comparasion between DES and 3DES Encryption

Factors	DES	3DES
Key Length	56 bits	112 bits(2 key) 168 bits(3 key)
Block Size	64 bits	64 bits
Possible key	2^56	2^112
Cipher type	Symmetric Block	Symmetric Block
Weakness to hacking	• Cryptanalysis • Brute Force • Linear	• Cryptanalysis • Brute Force • Linear
Security	Weak	Strong
Keys	1	2 or 3
Rounds run through algorithm	16	48

3. Triple DES(3 DES)

3DES is a symmetric-key block cipher, inherited from the DES and it make use of three different keys that means which applies the DES three times to every data block. uses a 56-bit key and is not view as sufficient to encrypt sensitive

Information .3 DES simply increase key size of DES
by applying the algorithm three times in succession with three different keys. The grouped key size is 168bits because of 56bits with 3 times

4. Existing System:

In today's technology popular email services such as Gmail, Yahoo, Hotmail or Outlook commonly uses the 2 factor authentication. Besides 2 step verification outlook.com features a recovery code that you can use if you lose access to your security information(your phone number and alternate email address).This recovery code is generated once and for

security reasons is never viewable again within Outlook.com itself but is not efficient to use. You can also manage the trusted device.

Most used and popular Email Service – GMAIL

- IMAP(Internet Message Access Protocol)
- POP3(Post Office Protocol)
- TLS, SSL
- SHA, MD5
- One Time Password (optional)

5. Proposed System:

In this system we encrypted the content in the transport layer and we also encrypted the message at the front end of the system i.e the timeline of the user. For example, Suppose one user is login into his account all the emails are displayed in encrypted format and the emails are decrypt only when the user will enter the key.

6. Implementation:

We have used the 3-DES algorithm for the contents of the message i.e every message will be encrypted and sent in the encrypted format.

Hence it will be difficult for the hacker to hack the message. In our system then connection between the client and server is encrypted using the SSL (Secured Socket Layer) protocol. SSL is the standard security protocol for establishing the encrypted links between the server and client. we have also implemented the IMAP and SMTP protocol.

When the user wants to use our system, he needs to register first after that he need to login into the system with the help of one time password. The OTP is sent to the registered mobile number of user. When sender wants to send a email, he simply need to compose the email and click on send button. The email is encrypted with the help of 3-DES algorithm. While transmitting the email is in the encrypted format. When receiver receive the email, the email display in the encrypted format. The key is send to the receiver's mobile number when sender sends the email. When the key is entered only then the email is decrypt. Means if the account is hacked and hacker opens the mail of any user he is not able to read the data because it's in the encrypted format. And hacker doesn't know the key to decrypt the email.

6.1 Modules:

Module 1: Login Module

- In this module the user should enter user id, password.
- At the login time, if the user forgets his/her password, then after clicking at the forget password link, the security question will be asked, after getting the correct answer, the server will mail the user his/her password. User can get the password from that email.
- The 2 step verification is done. The user will get a message on the mobile no provided at the registration time. User will get a verification code which he has to enter.
- This verification code is generated using the username and the mobile no and again 'random' function is used for this purpose.

Module 2: Email Server

- In this module a user profile page is available.
- The sub modules such as Compose Mail which contains fields such as To (receiver's email address), Cc (carbon copy), Subject, Description, Key (which user will use to encrypt), Encrypted Message (Description of Encrypted message after given key is applied) and also Send, Reset and Cancel Email.
- In Sent Mail we include the messages sent by user previously with email address, description and duration.
- Inbox – Here we have incoming messages from other users which we have to perform decryption

- Decrypted Message – Here we include the messages which we have received and Decryption has done.
- Contact List – Where we can add email addresses of other user whom we have to send.
- Drafts – Here we can save specific message which we may want to refer in future
- HTTPS – Implementation of encrypted email transfer using TLS (Transport Layer Security) or SSL (Secure Sockets Layer).

Module 3: Triple DES Encryption

- Understanding the working and implementation of the Basic DES and Triple DES.
- Implementation of Algorithm in Code Format
- Using the 56 bit key to Encryption
- Encryption of Plain Text, Image or any other format if possible
- Implementation of Decryption with given key
- Send of Senders key to receiver using SMS or EMAIL.

Snapshots:-

1. Login

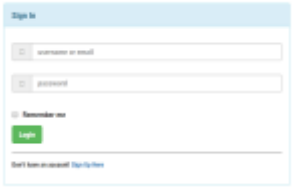

Fig No. 6.1.1 Login

Fig No.6.1.1 shows the Login snapshot which we have implemented .In this, the user has to enter his/her details along with the OTP in order to access to our server.

2. Compose Mail

Fig No. 6.1.2 :- Compose Mail

The above Fig No. 6.1.2 shows the snapshot of Compose Mail. The user can compose mail to another user just by specifying the email id of the user and mobile number for receiving the key through SMS.

3. Decrypt Mail

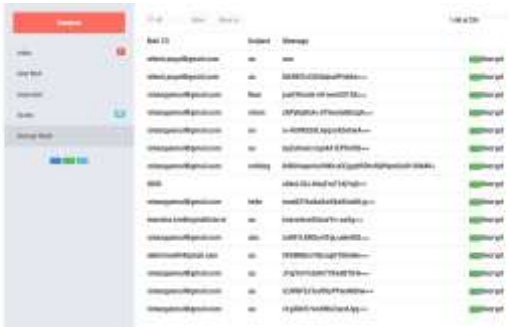

Fig No. 6.1.3 :- Decrypt Mail

The above Fig No. 6.1.3 shows the snapshot of Decrypt Mail in which the user can decrypt all the encrypted mails. After decryption the user can view the mail in the plain text format.

7. CONCLUSION

The main aim of this tool is to provide security. This tool can be best used at the organizational level. It provides high level security wherein even if the data is hacked; the hacker will not be able to access the account because of the Triple DES technique used. Hence, this tool is the best to be used for security. To prevent the users of Gmail, rapid share, PayPal, eBay, etc. getting hacked. To prevent the users loss of data in Internet. The two factor authentication gives boost to the security.

8. References

1. "A proposed mode for triple-DES encryption" by D. Coppersmith, D. B. Johnson and S. M. Matyas.
2. "On the Security of 2-Key Triple DES" by Chris J. Mitchell.
3. "OTP-Based Two-Factor Authentication Using Mobile Phones" by Mohamed Hamdy Eldefrawy, Khaled Alghathbar and Muhammad Khurram Khan.
4. "Efficiently improving the security of OTP" by Devashish Kumar, Amit Agrawal and Puneet Goyal
5. Tingyuan Nie, Chuanwang Song and Xulong Zhi, "Performance Evaluation of DES and Blowfish
6. Algorithms", IEEE International Conference on Biomedical Engineering and Computer Science
7. Diaa Salama Abdul. Elminaam, Hatem Mohamed Abdul Kader and Mohie Mohamed Hadhoud,"Performance Evaluation of Symmetric EncryptionAlgorithms", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.12, pp. 280-286, December 2008.
8. Electronic Frontier Foundation. Cracking DES: Secrets of encryption research, wiretap politics and chip design. O'Reilly and Associates,