Proposing Enhanced E-Mail Security Mechanism (EEMSM) for Reducing Cyber Crimes

Prabhdeep Kaur
Department of Computer
Science & Engineering
Sri Sai College of Engg
and Technology,
Mannawala (Amritsar)

ABSTRACT

Now a days, Criminals use various methods for launching sophisticated attacks via internet. Most commonly e-mail channel is preferred by the attackers for launching phishing attacks by sending fake or junk emails. As authors studied due to absence of privacy, authentication and integrity of email message somewhere SMTP (Simple Mail Transfer Protocol) lacks security. So, for making more secure email communication channel, authors designed a new methodology "EEMSM" that is named as Enhanced E-Mail Security Mechanism whose function is to provide "Content Base Encryption" (CBE) on a simple mouse button click on email body before sending email to receiver end. The working of EEMSM is based on the type of encryption algorithm applied on the type of content carried by email body viz. text based content, image based content and audio/video based content etc. The motive of this new designed methodology is to keep data safe or private from the third party without data stolen on the time of data sending on the network. That ultimately helps to improve email body content security on the network. This paper also discusses about the current scenario used by the G-mail for sending E-mail. And at the end, authors compares how new designed methodology provides more secure results than the present scenario.

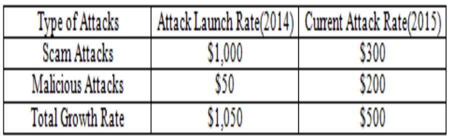
Keywords

Cybercrime, phishing, attacks, attackers, email, encryption algorithm, Content based encryption.

1. INTRODUCTION

E-Mail security is a global security issue [17] now a days because of most of the attackers preferred to launch attack through several channels. The most preferable channel used by the attackers is E-mail channel. They usually launch attack through sending fake or junk mails. Some of the popular attacks through emails are shown in the given table 1 below:

Table.1:Growth of Cybercriminal Activites[19]



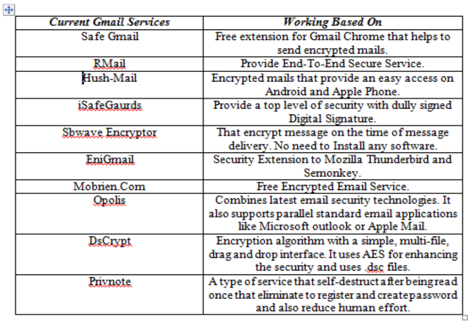
Type of Attacks	Attack Launch Rate(2014)	Current Attack Rate(2015)
Scam Attacks	$1,000	$300
Malicious Attacks	$50	$200
Total Growth Rate	$1,050	$500

The reason for choosing E-Mail channel is its maximum usage of official data transference. As authors surveyed, most commonly they preferred spear phishing method [19][13][6] for launching phishing[22] through email [21]. The benefit to utilize this method is it is very easy to perform and less time consuming. and the additional benefit to utilize this method is its simple working that can be only held on a single mouse button click. For reducing phishing through email several security practitioners [8] are designed new methods and strategies in different fields[39]. At first, they surveyed the current protocols and methods that are presently uses in E-Mailing and how they manage its all functionality [39]. This survey gives the complete details of Email flow, Email Storage and access at user level or server level by utilizing various advanced security tools[15][5]. In addition, email management group [39] also gives detailed information about the different security policies currently implemented in the given scenario like general email policy and email retention policy[38][42] used by the Gmail. After completed their studies authors concluded now a days, only 4 web service providers are most commonly provide email service like Google, Yahoo, Microsoft and AOL [12].The basic principle used by every web email service provider is to filter each email through its classification on the basis of message bodies [7].And the working of Email exchange information is based on email server and email client. Each has its own function:

1. The function of email server is to deliver, store and forward.
2. The function of email client is to provide interface and allow users to read, compose, send and store email messages. [11]

While sending email each one follows a simple path SMTP (Simple Mail Transfer Protocol) [3] [31] for sending and receiving email [43]. Due to lack of privacy and authentication on SMTP attackers launch attack on it. For stopping spam emails [41] security practitioners [8] mostly uses real time monitoring device like CYBEROAM [32]. The major purpose to utilize this policy behind this is to fight against viruses and spams [4] [38]. So, security practitioners [8] generally uses the concept of threat intelligence [9]. By utilizing threat intelligence [9] content based encryption [16] concept is easily implemented on the time of email sending. Such type of content based security can be implemented in two separate ends viz. client end and server end [20]. As authors studied conventional encryption schemes [10][14][28] like lavabit [25] on fortimail platform[37] are missing in Gmail Service that is the only reason for easy attack on Gmail server. After completed the literature survey from different papers, they concluded if content based encryption [16] is applied on the metadata of Gmail service [23] then the chances of attacks will be reduced up to some context. The other benefit of these conventional encryption schemes is it provides more tighten security to PGP tools [35] as an example in our daily life Gmail users noticed the secondary mail option in Gmail account [40] that actually protects us form threat prevention[34]. As several types of services are currently provided by our Gmail Team that can be shown in table.2:

Table.2:Nomenclature for Different Types of E-Mail Services[25][37]



Current Gmail Services	*Working Based On*
Safe Gmail	Free extension for Gmail Chrome that helps to send encrypted mails.
RMail	Provide End-To-End Secure Service.
Hush-Mail	Encrypted mails that provide an easy access on Android and Apple Phone.
iSafeGaurds	Provide a top level of security with dully signed Digital Signature.
Sbwave Encryptor	That encrypt message on the time of message delivery. No need to Install any software.
EniGmail	Security Extension to Mozilla Thunderbird and Semonkey.
Mobrien.Com	Free Encrypted Email Service.
Opolis	Combines latest email security technologies. It also supports parallel standard email applications like Microsoft outlook or Apple Mail.
DsCrypt	Encryption algorithm with a simple, multi-file, drag and drop interface. It uses AES for enhancing the security and uses .dsc files.
Privnote	A type of service that self-destruct after being read once that eliminate to register and create password and also reduce human effort.

As studied several types of Gmail Services in table 1 , the most common service is used by Gmail Team is Barracuda email service[25][37]. The main reason to prefer this service is its comprehensive nature and cost effectiveness [33]. Similarly, different platforms may uses different types of services as an example cloud email service providers uses TrendMicroTM[36] like services those have self-capabilities for avoiding unwanted messages in the account corresponding they also helps to ignore as well as stop spam [18][29] emails.

For providing national security through email channel authors designed a new methodology EEMSM that is termed as Enhanced E-Mail Security Mechanism". This new designed methodology uses the concept of "encryption without decryption. That shows one way encryption mechanism [24] at sender end. The complete working of this new designed methodology is only handled at sender end. At first, sender choose the category of the mail viz. Official,Personnel,Entertainment mail after that apply encryption algorithm(AES,DES,SHA-512)[30] on a simple mouse button click at sender end. Users may apply different types of encryption methods on different type of email content viz. text, image and multimedia etc type messages as an example for applying multimedia encryption [26] compression algorithms plays an important role. The most interesting thing is that there is no need to apply decryption at receiver end because of when client was log_in in his/her account for reading emails then what Gmail User noticed when sender entered email in email body then the URL's [27] is auto-saved with the email message body and when receiver will be log_in then Gmail user automatically receive that specific URL address. Gmail user simple click on that address then the cipher text is converted into plaintext. Hence, email will become in readable form by following Secure Path Communication Channel (SPCC).

2. REVIEW OF LITERATURE

(Chuchra et al. (May 2015): This paper discussed about different types of cyber-attacks and proposed a new methodology named OTBP-Using RRSA (Operational Technology Based Procedure Using Round Robin Scheduling Algorithm). This new designed methodology provides a secure path during client-server communication by utilizing the concept of automatic path encryption on auto-generated hash address This paper also discusses about two different types of path hacking; viz. on-path hacking and off-path hacking by following different mechanisms such as path based authorization; path based traversing and path based access rules etc.[1]

(Chuchra, Gujral and Sharma et al. (Dec 2013): Authors are discussed about the major threats of phishing attacks on worldwide financial transactions on enterprises. They contributed their efforts for analyzing the behavior of attacker at client end as well as at server end by proposing two new mechanisms viz. port scanning and rule induction. This new designed mechanisms may help potentially to reduce phishing attacks by analyzing the behavior of attacker during the transmission of data from the starting to end point while an attacker insert a malicious SQL query as an input to perform an unauthorized database operation.[2]

3. RESEARCH DESIGN

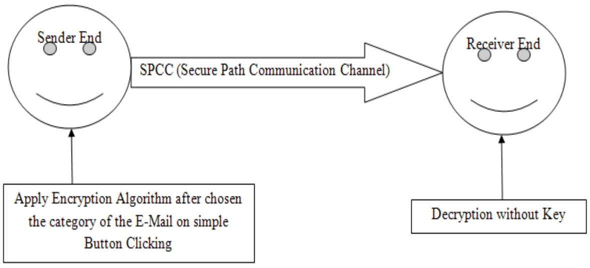
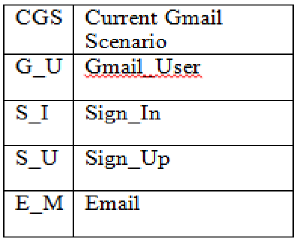

Sender End
SPCC (Secure Path Communication Channel)
Receiver End
Apply Encryption Algorithm after chosen the category of the E-Mail on simple Button Clicking
Decryption without Key

Fig.1: Proposed Client Server Communication- By using SPCC.

4. CURRENT SCNERIO USED BY GMAIL FOR SENDING EMAIL

Table 3: Nomenclature for CESM.



CGS	Current Gmail Scenario
G_U	Gmail_User
S_I	Sign_In
S_U	Sign_Up
E_M	Email

CGS (G_User,Sign_In,Sign_Up,E_Mail)

Step-1) Go for S_U. //Account successfully created.

Step-2) THEN Sign_I. // User Log_In own account for sending E-Mail.

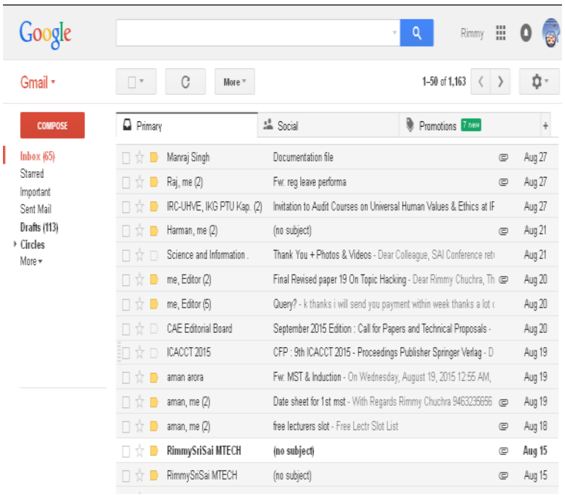
Step-3) G_U_Click = Compose_Btn. // for sending email (i.e. enter email address of receiver and also entered the content on email body).

Step-4) Finally Click_On:= Send_Button. //E-Mail Send Successfully.

Step-5) End.

Current Scenario Drawback: There is no additional security is provided at Sender End.

Current G-Mail Page:



Manraj Singh	Documentation file	Aug 27
Raj, me (2)	Fw: reg leave performa	Aug 27
IRC-UHVE, IKG PTU Kap. (2)	Invitation to Audit Courses on Universal Human Values & Ethics at IF	Aug 27
Harman, me (2)	(no subject)	Aug 21
Science and Information .	Thank You + Photos & Videos - Dear Colleague, SAI Conference ret	Aug 21
me, Editor (2)	Final Revised paper 19 On Topic Hacking - Dear Rimmy Chuchra, Th	Aug 20
me, Editor (5)	Query? - k thanks i will send you payment within week thanks a lot (	Aug 20
CAE Editorial Board	September 2015 Edition : Call for Papers and Technical Proposals -	Aug 20
ICACCT 2015	CFP : 9th ICACCT 2015 - Proceedings Publisher Springer Verlag - D	Aug 19
aman arora	Fw: MST & Induction - On Wednesday, August 19, 2015 12:55 AM,	Aug 19
aman, me (2)	Date sheet for 1st mst - With Regards Rimmy Chuchra 9463235656	Aug 19
aman, me (2)	free lecturers slot - Free Lectr Slot List	Aug 18
RimmySriSai MTECH	(no subject)	Aug 15
RimmySriSai MTECH	(no subject)	Aug 15

5. PROPOSED SCNERIO FOR GMAIL: - EEMSM

At Sender End:

Table.4: Nomenclature for EEMSM.

Sen_E	Sender_End
Rec_E	Reciver_End
MBC	Mail Body Content
S_UP	Sign _UP
S_IN	Sign_IN
E-Cat	E-Mail Category
OFF	Official
PER	Personnel
ENTER	Entertainment
Encr_A	Encryption Algorithm
SPC	Secure Path Encryption

EMSM (Sen_E, Rec_E, MBC, S_Up, S_In, E-Cat {OFF, PER, ENTER}, Encr_A, SPC)

Step-1) Go for Sign_Up. //Account successfully created.

Step-2) THEN Sign_In. // User Log_In own account for sending E-Mail.

Step-3) User_Click = Compose_Btn. // for sending email (i.e. enter email address of receiver and also entered the content on email body).

Step-4) After that Sen_Select: = E_Cat {OFF, PER, ENTER} // Apply Clustering Algorithm for filtering the emails that ultimately store it into a separate cluster.

Step-5) CHK_EBC :={ TEXT, IMAGE, MULTIMEDIA [AUDIO, VIDEO]}. //check the type of content carried by the email body.

Step-6) THEN APPLY ENCR_A:=On _E_Cat on Mouse_Btn_Clicking. // Hence, The Mail Body Content is successfully Encrypted.

Step-7) Finally Click_On:= Send_Button . //E-Mail Send Successfully.

Step-8) End.

Proposed Mechanism Advantage:

It provides an additional security on sender end through encryption.

Proposed G-Mail Page Design- By Using EEMSM:

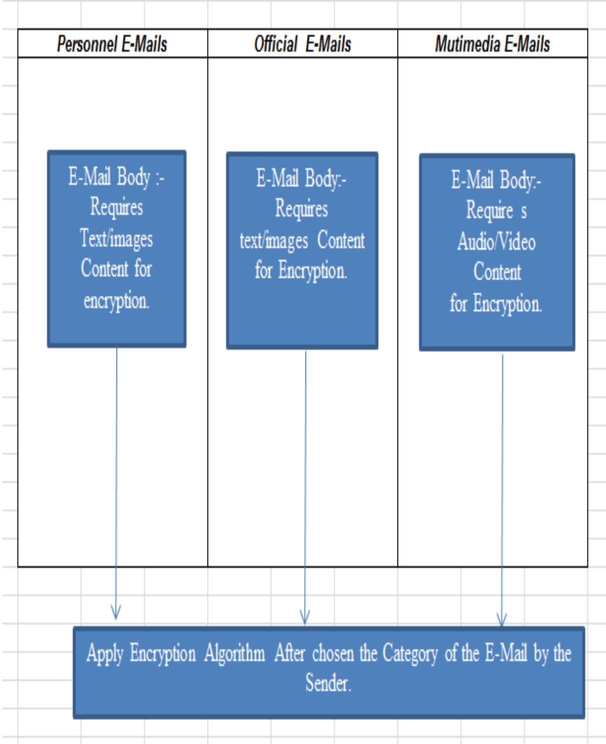
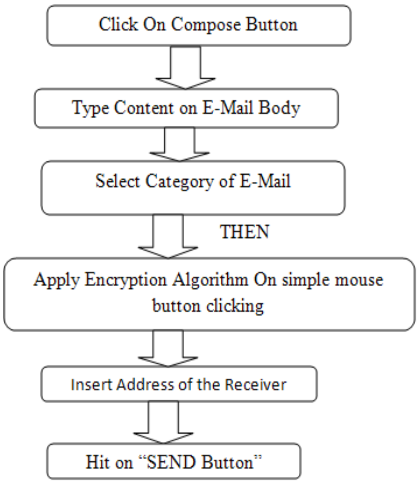

Personnel E-Mails
Official E-Mails
Mutimedia E-Mails
E-Mail Body :- Requires Text/images Content for encryption.
E-Mail Body:- Requires text/images Content for Encryption.
E-Mail Body:- Require s Audio/Video Content for Encryption.
Apply Encryption Algorithm After chosen the Category of the E-Mail by the Sender.

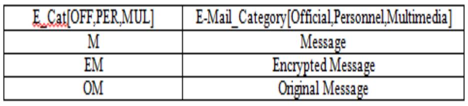
Table.5: Types of Encryption

TE/CE	Text Encryption
IE	Image Encryption
ME(AE/VE)	Multimedia Encryption(Audio/Video)


Click On Compose Button
Type Content on E-Mail Body
Select Category of E-Mail
THEN
Apply Encryption Algorithm On simple mouse button clicking
Insert Address of the Receiver
Hit on "SEND Button"

At Receiver End:

Table 6: Nomenclature for EEMSM.



E_Cat[OFF,PER,MUL]	E-Mail_Category[Official,Personnel,Multimedia]
M	Message
EM	Encrypted Message
OM	Original Message

EEMSM (Sign_In, E_Cat [OFF, PER, MUL],M,EM,OM)

Step-1)Sign_In.

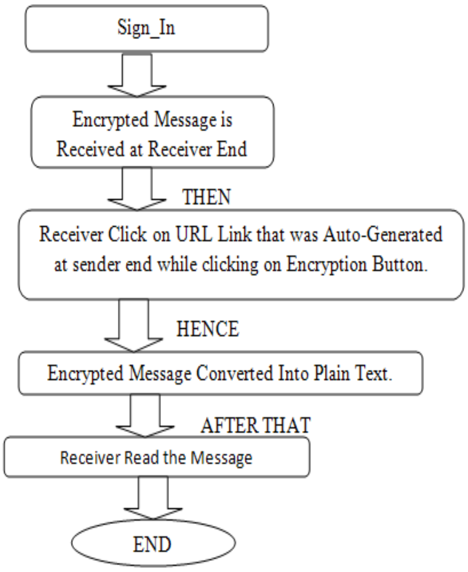
Step-2) SEARCH: = E_Cat [OFF, PER, MUL]// Looking for email form available categories.

Step-3) AFTER THAT CLICK_ON LINK AVAILABLE ON EMAIL_BODY with EM.

Step-4) Automatically M CONVERT FROM EM TO OM.

Step-5) M:=RF.   //Message read successfully.

Step-6) END.


Sign_In
Encrypted Message is Received at Receiver End
THEN
Receiver Click on URL Link that was Auto-Generated at sender end while clicking on Encryption Button.
HENCE
Encrypted Message Converted Into Plain Text.
AFTER THAT
Receiver Read the Message
END

6. CONCLUSIONS

A variety of cyber-attacks on emails have been reviewed and analyzed here. It may considerably be reduced by developing the mechanism "EEMSM" (Enhanced E-Mail Security Mechanism). The complete working of proposed mechanism is based on type of encryption algorithm is applied on type of content (say text, image, audio, video (Multimedia)) carried by the mail body. This paper also discussed about the current scenario used by the G-mail for sending E-mails and after that it compares with the proposed mechanism that shows the overcome the drawbacks of current scenario used by G-Mail and data will be further safely send over the network with encryption and can be used further at receiver end without decryption. Hence, this enhanced email security mechanism provides data safety at sender end (i.e. before sending E-Mail).

7. REFERENCES

[1] Rimmy Chuchra and Shubham Chuchra, May 2015. Proposing OTBP(Operational technology Based procedure) Using RRSA(Round Robin Scheduling Algorithm),International Journal of Computer Application.

[2] Rimmy Chuchra, Reenuka Gujral and Priyanka Sharma, December 2013.On the Mechanism of detection and prevention from Phishing attacks by analyzing the attacker behavior, International Journal of Advanced Research in Computer Science and software Engg.

[3] M.Tariq Banday, May 2011.Effectiveness and Limitations of email security protocols, International Journal of distributed and parallel systems.

[4] Pam Cocca, 2004. E-mail Security Threats, GIAC Security Essentials Certification (GSEC).

[5] Jon Oltsik, January 2013. Good Enough- E-Mail Security is no longer Good Enough.

[6] Shahira Banu.N, M.Mohammed Mohideen & Gori Mohamed J February 2014. E-Mail Phishing-An open threat to Everyone, International journal of Scientific & research Publications.

[7] A.S Deokar,Madhuri Baful,Rahul Jagtap,Vishakha Panjabi & Shrihari Ahire, January 2014. Secure E-Mail System for SOHO (small Office Home Office), International Journal of Advanced Research in Computer.

[8] White paper on Data security by the DMA E-Mail Marketing Council best Practice Hub, 2012.

[9] Analysis of cyber-attack and Incident data from IBM worldwide security operations, IBM Global Technology Service, Research Report 2014.

[10] Zix Crop, November 2010.A New Standard in Encrypted E-Mail.

[11] Wayne Jansen, Miles Hacy and Scott Bisker, 2002.Guidelines of mail security NIST (National Institute of Standards and Technology), US.

[12] Serge Egdman, A.J.Bernheim & Sturt Schechter, It's no Secret measuring the security and reliability of authentication via secret questions.

[13] Marti Hearst,J.D Tygar & Rachna Dhamya, April 2006.Why phishing works ,Conferences on human factors in computing systems.

[14] Traushi Sharma, January 2014. E-Mail Security using clustering algorithm ,International Journal of Computer Science and information security.

[15] Shufen Liu,Dongmei Han and Hui Wang, August 2010. Research on security architecture MSIS for defending insider threat, Proceedings of the third International Symposium on computer science and computational technology, China.

[16] Joan Feigenbaum, Nick Fermster, Loori Cranor and Jean Camp, 2009. Data for Cyber Security Research: Process and Wish List.

[17] Kimberly Marteen, 2015. Colloquium on Problems in International politics: International Security, Springer.

[18] endpointprotection.sftwareinsider.com/1/113/Symantec-E-Mail-Security-Cloud.

[19] E-Mail Attacks: This Time it's Personnel, CISCO Security White Paper.

[20] Yinglian Xie,Benjamin Livshits, Ulfar Erlingsson, End-to-End web application Security ,Microsoft Research.

[21] T.C Panda,Yerra Shankar Rao & Hemraj Saini, April 2012.Cyber-Crimes and Their impacts:- A Review ,International journal of engineering research and applications.

[22] Durgesh Pant and Sushell Chandra Bhatt, 2011.Study of Indian Banks websites for cybercrime safety mechanism ,International Journal of Advanced computer science and applications.

[23] Mark Ryan, Vincent Cheval & Ji Angshan Yu, Challenges With End-To-End Email Encryption, University of Birmingham, UK.

[24] Omer Reingold, Moni Naor and Cynthia Dwork, Immunizing Encryption Schemes from Decryption Errors, Microsoft Research.

[25] https://en.wikipedia.org/wiki/email-privacy.

[26] https://books.google.co.in/books?id=RQV7GCE7-PUC&rg=PA17 & lpg=PA17&dg=encryption without decryption & F= False.

[27] https://support.google.com/webmasters/answer/6033066!hl=en.

[28] www.quora.com/Is-it-Possible-to-decrypt-encryption-without-the-key.

[29] www.codeproject.com/Articles/796587/using-encrypted-files-without-decrypting-to-Disk.

[30] www.howtogeek.Com/135638/the-best-free-ways-to-sne-encrypted-email-and-secure-messages.

[31] en.citizendium.org/wiki/E-Mail-Processes-and-Protocols.

[32] www.cyberoam.Com/emailsecurity.html.

[33] https://www.barracuda.com/Products/emailsecurityservice

[34] https://www.fireeye.com/products/ex-mail-security-products.html.

[35] techcrunch.com/2014/12/12/the-founders-guide-to-email-security/.

[36] www.trendmicro.com/us/small-business/hosted-email-security/.

[37] www.fortinet.com/products/fortimail/.

[38] www.threattracksecurity.com/business-antivirus/vipre-email-security-for-exchange.aspx.

[39] www.net-security.org/article.php?id=816.

[40] https://lastpass.com/suppose.php?cmd=showfaq&Id=2465

[41] www.trendmicro.fr/media/as/hosted-email-security-datasheet-en.pdf.

[42] www.theemaillaundry.com/email-security-policy/.

[43] https://uxsci.com/blog/the-case-for-email-security.html.