IJCSI International Journal of Computer Science Issues, Volume 13, Issue 6, November 2016
ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784
www.IJCSI.org https://doi.org/10.20943/01201606.113119

Implementation of Email Security using PGP at Zimbramail Server

Made Sudarma[1], Dandy Pramana Hostiadi[2]

[1] Department of Electrical and Computer Engineering, Faculty of Engineering, University University Jimbaran Campus, Bali – Indonesia, *Tel./Fax: +62361 703315*

[2] Department of Computer System, STIMIK STIKOM BALI
Jl. Raya Puputan No. 86, Denpasar, Bali 80234, Indonesia. *Tel./Fax: +62361 244445*

Abstract

The Electronic mail is a fundamental communication model in globalization era. It is seen that every form of data registration or information needs electronic mail data. The use of e-mail itself cannot be separated from the abuse from some parties so it needs security form in e-mail communication. Communication security on mail server such as ZIMBRA mail server has been well-implemented, such as the use of ssl certificate. But the security is still standard. So, when user and password has been found out by third party, e-mail content will be read easily (in cryptography technique it is called plaintext reading). On research that was conducted with pretty good privacy (PGP) method email communication security was focused on the e-mail content by encrypting mail text along with the attachment file. The research uses some software tools that were used in implementation at Zimbra mail server such as Cleopatra and Mozilla thunderbird. Result of research shows that PGP security is able to secure e-mail content whether the text or the attachment, showing difference of attachment file size is bigger on PGP using and change mail header from the standard mail.

Keywords: *E-mail, Zimbra Mail Server, PGP, Encryption*

1. Introduction

The E-mail is a form of communication that is said to be fundamental in the globalization era[1]. It can be seen that at present time almost communication utilization always require to put e-mail address. For example is on social media registration where registration form requires putting e-mail address. Communication in some companies or governments in long distance communication across the land or country also need e-mail address. It can be concluded that e-mail is a primary information/data for communication doer in global era.

As e-mail using developed as communication form, it cannot be separated from any party that abuse e-mail use and it aimed at violation of law[2]. For example, there are deceptions by using false mail account or password robbing and e-mail account piracy. So, it needs to conduct security to communication. There are some techniques of internet communication security including the e-mail communication such as cryptography technique, with different algorithm[3]. For example is Zimbra mail server that has implemented ssl certificate security. The Zimbra mail server itself is an engine mail that has been used widely in some companies with flexible and simple feature to be used and it has characteristic as an open source. But the security with ssl certificate has not yet fully guaranteed the security on mail server[4,5]. As in the robbing of mail account, when someone who is not in concerned succeeded to get user mail and password, then he/she will be easily to read e-mail content and found out crucial information in the e-mail. To prevent such a thing it needs to improve e-mail communication security and one of the methods is by PGP (Pretty Good Privacy) security. With PGP the e-mail communication security focuses on security of e-mail content (to anticipate mail content reading easily by not in concerned party) including attachment file. There is review about previous research such as performed by Tarek Salah Sobh and Mohamed Ibrahiem Amer in 2011 with the title of PGP Modification for Securing Digital Envelope Mail Using COM+ and Web Services. In their research it produced standardized digital certificate for communication protocol standard with encryption technique of PGP technique by combining encryption and sign in digital through web service, but result of difference analysis to mail engine use and the communication result has not yet explained in detail. So the difference to PGP use that has effect to the change of e-mail content at mail engine has not yet found out and it needs to be re-investigated.

On the research performed, where implemented PGP security at Zimbra mail server will see to what extent the security conducted by observing from PGP result, analysis to attachment file and e-mail header. By using supporting application such as Cleopatra and mail client Mozilla

thunderbird, the research will be more maximal in analysis performed to e-mail communication security at Zimbra mail server by using PGP technique.

2. Literature Review

1.1 Zimbra Mail Server

Mail server (also known as mail transfer agent or MTA, mail router or mailer Internet) is an application that will receive incoming e-mail from local user (people in one domain) and sender long distance and forward outgoing e-mail for sending[6]. A computer that is dedicated to run the application is also called as mail server. (Danphi, 2008) Microsoft Exchange, qmail, Exim, and sendmail are more common amongst mail server programs. Mail server is one of server functions that most to be used at companies. This is considering e-mail function itself that can reduce correspondence cost, more efficient than manual communication and it can include useful attachment as complement and additional document related to e-mail content[7].

Zimbra is a groupware product made by Zimbra, Inc. located at Palo Alto, California, United States of America. In the early years this company was bought by Yahoo! precisely at September 2007. Basically, Zimbra is at the same class with Microsoft Exchange Server application. The difference is that Zimbra is available in 2 editions those are the Open source Edition and Network Edition. Zimbra Open source Edition uses license of Mozilla Public License which one of the license points states that the change or modification performed to Zimbra source code should be returned to community. (Danphi, 2008) In transition process toward open source era, that back office shift should be done in the earliest where endusers need become attention. To fulfill the demand one of open source products related to e-mail which meet the requirement is Zimbra Collaboration Suite. (Zaida, 2010) Zimbra Collaboration Suite is collaboration from some open source software applications, among others Apache Jetty, Postfix, OpenLDAP, and MySQL. This collaboration produced powerful e-mail server with complete features. (Zaida, 2010). The following are open source applications used by Zimbra Collaboration Suite which have become standard application used in industrial world (Zaida, 2010):

1. Jetty, web server application that runs Zimbra application. Postfix, MTA (Mail Transfer Agent) open source application that runs Zimbra e-mail server.
2. OpenLDAP, open source application as Lightweight Directory Access Protocol (LDAP) that is useful for user authentication.
3. MySQL, database application.
4. Lucane, index text powerful open-source application and search engine.
5. Anti-Virus and anti-spam, open source applications that consist of: Clamav antivirus scanner that protects file from virus attack, SpamAssasin mail filter that identify Spam and Amivisd-new as interface between MTA with the other.
6. James/Sieve filtering, to make filter for e-mail

1.2 Cryptography

Cryptography is a branch of science that study about the method to keep secure data or message when they are sent, from sender to receiver through communication transmission mechanism without any disturbance from third party. According to Bruce Scheiner in his book “Applied Cryptography”, cryptography is science and art to keep message secure[8].

Concept of cryptography itself has been used for a long time by human for example during Egypt and Roman civilization even though it was still simple. Principles that base cryptography are:

- Confidentiality that is a service in order that message content sent keep in secret and cannot be found out by other party (except the sender, receiver/permitted parties). Generally, this is done by making a mathematic algorithm that can change data so it will become difficult to be read and understood[9].
- Data integrity that is a service that can identify/detect illegal manipulation (erasing, changing or adding) of data (by other party).
- Authentication that is a service related to identification. It is whether authentication of involved parties in data sending or authentication of data/information originality.
- Non-repudiation that is a service that can prevent a party to deny his/her previous action (denying that the message came from him/her).

Terms used in cryptography field:

- Plaintext (M) is message that want to be sent (containing original data).
- Ciphertext (C) is encrypted (coded) message which is the result of encryption.
- Encryption (E function) is a process of plaintext change into ciphertext.
- Decryption (D function) is the opposite of encryption that is to change chipertext to be plaintext, so it is in the form of original/initial data.

The cryptography itself consists of two main processes those are the encryption process and the decryption process. The encryption process change the plaintext into chipertext (by using certain key) so information content on the message will be difficult to be understood .

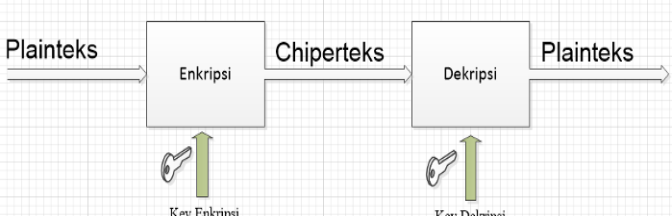


Figure 1 Encryption and Decryption Flow

Mathematic base that underlie the encryption and decryption process is the relation between two associations those are that contain plaintext/clear text elements and that contain chipertext/code text elements which is shown in the following mathematic:

Encryption :

$$E(M) = C \quad (1)$$

Decryption :

$$D(C) = M \text{ or } D(E(M)) = M \quad (2)$$

Encryption and decryption are transformation functions between the associations. If the clear text elements are notated with M, code text elements are notated with C, whereas for encryption process is notated with E, the decryption is notated with D.

1.3 Pretty Good Privacy (PGP)

PGP (Pretty Good Privacy) is an information encryption program method that has quite high confidential security level by using "Private-Public Key" as the base of the authentication so it won't be easy to be found out by other people who have no right. PGP was developed by Phill Zimmermann at the end of 1980[10]. Program made by Phill Zimmermann has two versions those are the "USA Version" and the "International Version". The USA version PGP in only is able to be used in USA territory and only by USA citizens. This USA version PGP uses RSA algorithm (which has been a patent right) in its encryption. Whereas the international version uses MPILIB algorithm that was specially created by Phill Zimmermann himself. The International Version PGP can be used by the whole world.

PGP (Pretty Good Privacy) was made based on Private Key Cryptography concept as the basic of its authorization. This Private Key Cryptography is used to encrypt in a communication relation between two machines. PGP works by combining some best parts from the conventional keys and public keys cryptography, so this PGP is a hybrid cryptosystem[11]. When a user encrypts a plaintext by using PGP, then initial PGP will compress this plaintext. Compressed data will save time and transmission media and the more important is the strong cryptographic security. Most code analysis technique exploit patterns found in plaintext to crack the chiper. Compression will reduce these patterns in plaintext, so by this way the improvement is better to hamper codes analysis[12].

PGP makes a key session, where the key is a secret at that time. Key is a random number resulted from random movement of mouse and key you pushed. This Session Key works very safely, the conventional encryption algorithm is fast to encrypt plaintext. The result is the chipper text. This session key then to be re-encrypted by using receiver public key, once data is encrypted. Session key that is encrypted by receiver public key was sent with chipertext to the receiver. The decryption process works in opposite. The receiver receives the message then open the message by his/her private key, but the message is still encrypted by session key. By using PGP, the receiver decrypts the encrypted chipertext conventionally[13].

Combination of 2 encryption methods combines the reliability of public key encryption with speed to conventional encryption. The conventional encryption is more less 1000x faster than key public encryption[14]. So, key public encryption gives a solution to key distribution and data transmission problem. By using both, key distribution and performance can be improved without sacrificing anything in security[15].

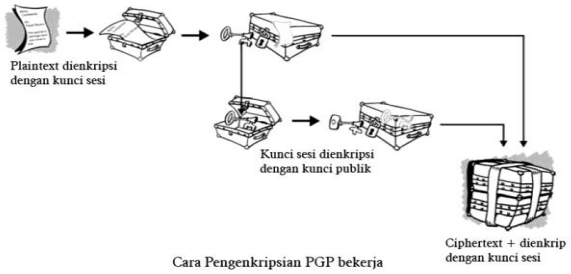


Figure 2 PGP Work Flow.

Working principles of PGP itself are::

a. PGP uses a technique called Public-key encryption with two codes that intrinsically related to each other, but it is impossible to separate one and another.
b. If making a key, it automatically will produce a pair of key those are the public key and the secret key. The receiver can give the public key to any destination he/she desired, through telephone, internet, keyserver, etc. Secret key that is kept on sending machine and using messager dechiper will be sent to the receiver by the sender on other side. So, the one who will use the public key (which is only be able to be decrypted by the secret key), sends the message to the receiver, and the receiver will use secret key to read message from the sender.
c. PGP uses two keys those are the public key (the encryption process) and the private (decryption process). It uses those two keys because there is conventional crypto, during transferring of key information, one secure channel is needed.

3. Research Method

In this research it is performed research methodology flow described at the following scheme:

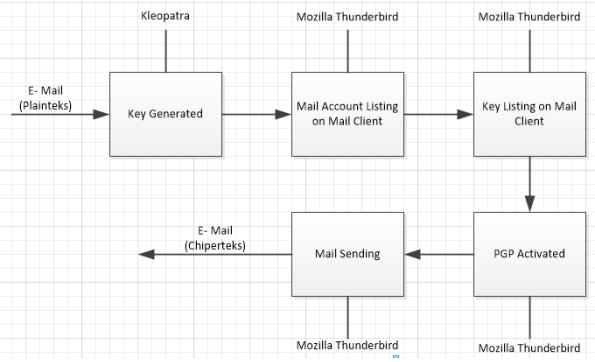


Figure 3 Methodology Flow

A. Key Generated

Key Generated is a stage where PGP key is made and later will be used in the security of e-mail sending. On the key making, it uses Cleopatra application. The Cleopatra application itself is a package application from gpg4win. Key produced by Cleopatra has some superiority among others it is able to be limited for expired data from generated key.

After private key was made by using Cleopatra application, it needs passphrase that later is used to decrypt message during sending and on the receiver side when reading received message. The private key that has been made should also be owned by the receiver, it can be done manually or sending conventionally to the message receiver. It needs to be remembered that from the receiver side if he/she uses different key list (not the same key between sender and receiver) then the key used on the message receiver side will not be able to be used before the same key is sent by the sender. And the Cleopatra application form is as the following:

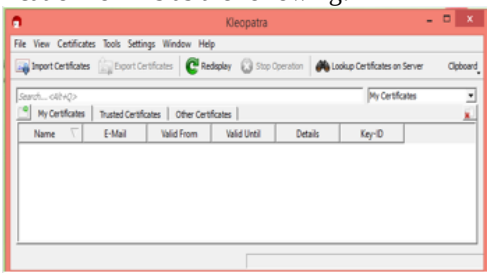


Figure 4 The Cleopatra Application

Result of output key generated by Cleopatra application is in the form of file extension as .asc

B. Mail Accounting Listing on Client Mail

Mail account that is used is the mail account with Zimbra mail engine. Mail account with Zimbra engine uses configuration of SMTP IMAP. In the research performed, to read e-mail and sending that encrypt with private key that was made uses the Mozilla thunder bird application. Mail account on the list into mail client of Mozilla Thunderbird.

C. Key Listing on Zimbra Mail Account

Result of key that was made in file extension result is as .asc, imported into client mail. Imported key should accord to the existing identity when generating initial key with Cleopatra application. In this stage it should be assured that key used by the sender and the receiver are same. The use of different key will have impact to e-mail reading received where the e-mail was read in the form of chipertext (coded and cannot be read).

D. PGP Activated

In this stage, PGP was activated by giving authorization to mail text. Activation form is by printing enigmail choice in the sending. Activation performed is also valid for sending attachment file. And digital module sign is activated. If it is activated then final process is to do e-mail sending.

E. Mail Sending

E-mail sending performed is by sending mail text and attachment file. Testing and analysis were performed by comparing e-mail sending result by e-mail receiver side. That is, for sending the mail text is compared to text mail reading with standard browser application and to be compared with mail text reading by using Mozilla Thunderbird application. For attachment file, it is done by analyzing the size created from PGP security result and to measure how much is the difference that emerged. In addition, it is also performed analyzing to existing mail header on both acceptance whether by using standard reading in the form of default browser and mail client application.

4. Result and Discussion

In research performed, before performing testing based on research methodology which has been discussed earlier, planning was performed in the form of research architecture design making. Design that was meant is as the following :

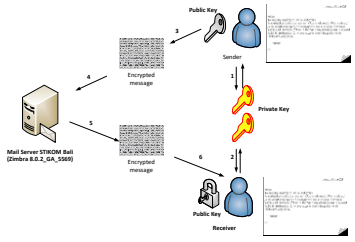
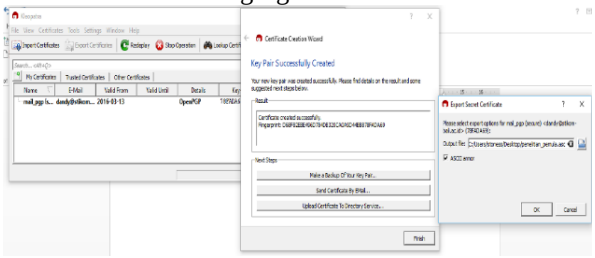


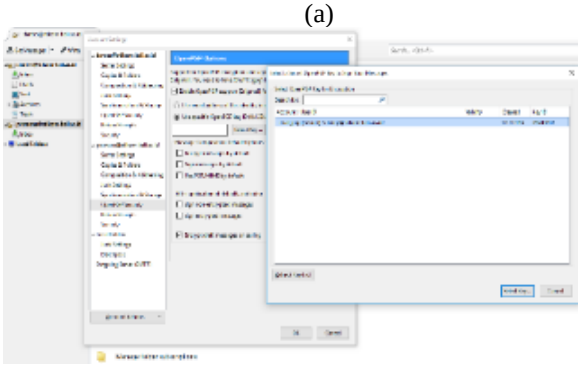
Figure 5 Architecture Design

As discussed earlier that e-mail communication security uses PGP technique was begun with the existing of private key ownership. This private key was owned by both actors those are the e-mail sender and e-mail receiver. This key has to exist before sending the e-mail (process 1 and 2 on figure 5). After private key was sent by both actors, message was sent by sender. So, the message sent is in the form of chipertext (coded message). And coding process performed is by using public key. Sending was performed above zimbra machine platform. From receiver side, the receiver will receive in the form of chipertext. Chipertext received will be re-decrypted by using private key owned in the beginning of communication. By private key ownership, the message will be able to be displayed again. If private key that is used to decrypt is not the same with sender's private key, then the message cannot be read.

The making of private key uses the Cleopatra application and the use of private key on mail client is shown on the following figure:



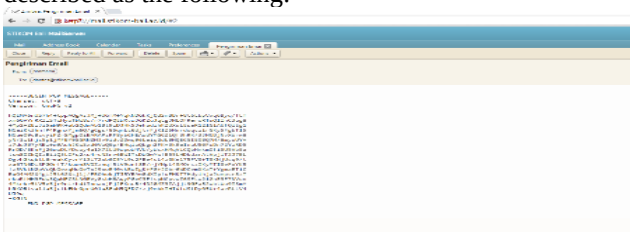
(a)



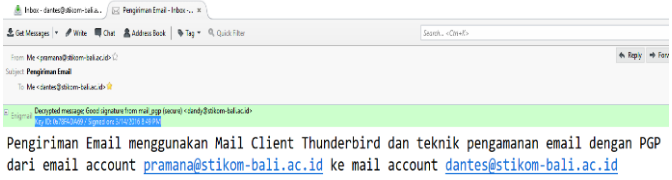
(b)

Figure 6 (a). Key Making (b). Key Using

Testing performed in this research is by comparing the e-mail sending and receiving mechanism between the standard e-mail sending and sending using PGP technique. The first testing result is comparing the PGP form that is described as the following:



(a)



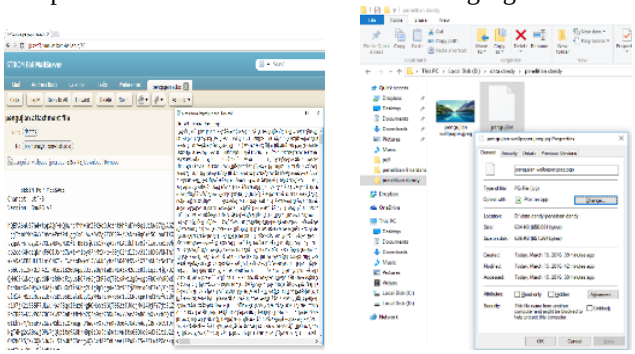
(b)

Figure 7 a. Reading with browser (without PGP)
b. Reading with mail client (with PGP)

From figure 7 it can be seen that there are two forms of mail reading, those are by using common browser without using private key (7a.) and that is using mail client with private key (7b.). When using browser, if third party (non interested party) is able to get user mail and password mail account, without using private key it will not be able to read the content of mail account. So, to be able to read in plaintext it needs private key (the same key with the sender) and mail client as interface that can identify PGP private key (shown in figure 7 b.).

The second testing was performed by comparing attachment file on e-mail sending with PGP and without PGP. File that was used for sending is the picture file with file size of 649,556 bytes.

After sending done the attachment file was analyzed from the acceptance form and changing of attachment file size. Result of PGP file acceptance with browser and comparison of size is shown in the following figure :



(a) (b)

Figure 8 a. Mail reading with browser
b. Comparison of attachment file

On figure 8 a. is mail that is read with browser without using private key and it is seen that the text content was encrypted, and attachment file is also seen as unknown file. When it is downloaded the unknown file is shown in figure 8 b. and it is seen as unknown file. If it is analyzed from size to attachment file with PGP and without PGP, it is shown in the following figure

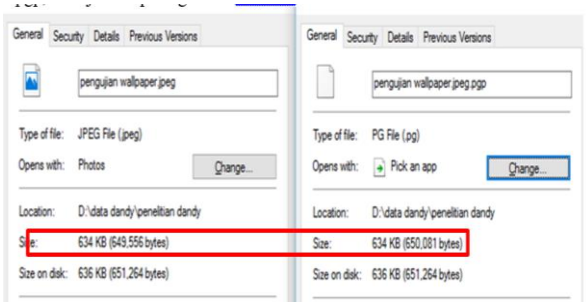


Figure 9 Size comparison

Difference appear that is shown in figure 6 is the existing of data size compression form. It is from the original data size of 649,556 bytes to be 650,081 bytes after being sent in PGP form, or it can be said that the data size difference is 525 bytes or 0,086% bigger from the size of original data.

The next testing is carried out by analyzing the e-mail header between mail sent with PGP technique and without PGP

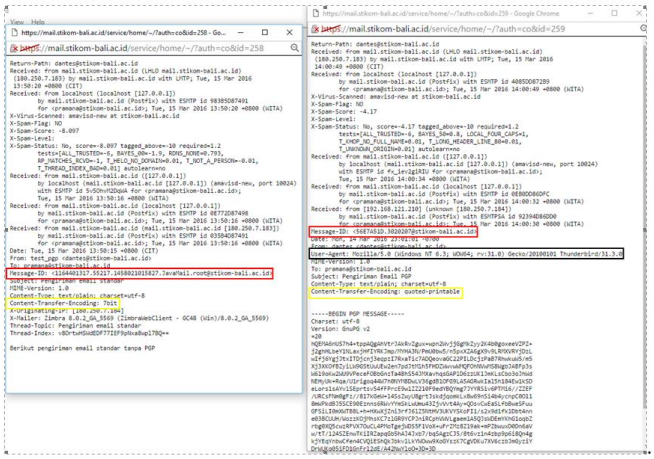


Figure 10 Mail Header

From figure 7 it can be described that e-mail that uses PGP has information of user_agent using (black line) that describes the using of Mozilla Thunderbird mail client. Information of sending Message ID also has difference where e-mail without PGP gives information of detailed postfix message detail, whereas mail with PGP is not detail. This is because it uses the Mozilla Thunderbird mail client application. The encoding technique information shown (yellow colored block) to mail with PGP interprets that encryption result is printed, whereas without PGP it only uses sending standard encoding of 7 bytes (STIKOM default mail server). Discussion to research result and testing obtained is presented in the form of theoretic description, qualitatively and quantitatively. Testing result is better to be shown in the form of graphic or table. For graphic, it can follow format for diagram and picture.

5. Conclusions

Based on result performed, it can be concluded that security by using the PGP technique can secure e-mail communication. The non interested parties might steal and find out the user mail account and password, but he/she can't read the e-mail content because it has been encrypted. Analysis result also shows that there is size difference of attachment file that use PGP security, where the file size becomes big because there is encryption process with private key. On the other side, it is seen the difference of mail header where PGP security gives encryption identity than mail without PGP. But analysis of mail header also shows the lack of postfix mail information detail on security with PGP technique.

As the developmental material on the next research, it can develop analysis to the difference of attachment file type, influence of file header of the encryption result and testing to other mail engine.

Acknowledgments

The appreciation is delivered to the Department of Electrical and Computer Engineering – Udayana University and STIMIK-STIKOM Bali that has given opportunity to perform the research, and also for all parties that always give support directly and indirectly in the finishing of this scientific journal especially we would like to thank you again.

References

[1]. A. Silbersachatz, P. Galvin, G. Gagne, "Operating System Concepts Essentials", John Wiley & SonsInc,2011

[2]. Ankur Dumka, Ravi Tomar, J.C.Patni, Abhineet Anand.Taxonomy of E-Mail Security Protocol .International Journal of Innovative Research in Computer and Communication Engineering.Vol. 2, Issue 4, April 2014.ISSN(Online): 2320-9801 ISSN (Print): 2320-9798

[3]. Bacard, A. (1995). The computer privacy handbook. Berkeley, CA: Peachpit Press.

[4]. Banday, M.T., Qadri, J.A. (2010). "A Study of E-mail Security Protocols," eBritian, ISSN: 1755-9200, British Institute of Technology and E-commerce, UK, Issue 5,Summer 2010, pp. 55-60, available online at: http://www.bite.ac.uk/ebritain/ebritain_summer_10.pdf.

[5]. Data Encryption Standard. (1999). FIPS PUB 46-3 Data Encryption Standard (DES). Retrieved from

[6]. E. Zaida, "Panduan praktis Membangun *Server E-mail* Enterprise Dengan *Zimbra*", Info Linux Dian Rakyat, Jakarta, 2010.
[7]. F. Danphi, "*Zimbra* Mail *Server* with Ubuntu 8.04", Informatika, Jakarta, 2010.
[8]. Richard A. Mollin, An introduction to Cryptography (Discrete Mathematics and Its Applications), Chapman and Ha11/CRC; 2nd edition
[9]. Stallings, W. (2002). Network security essentials: application and standards. (2nd ed.). New Jersey: Prentice-Hall
[10]. Henry, K. (2000). Getting started with *PGP*. Crossroads: The ACM magazine for students. 6 (5) .doi:10.1145/ 345107.345119, http:// dx.doi.org/ 10.1145/ 345107.345119.
[11]. Kamarudin Shafinah & Mohammad Mohd Ikram.2011.File Security based on Pretty Good Privacy (PGP) Concept.Computer and Information Science Vol. 4, No. 4; July 2011 .ISSN 1913-8989 E-ISSN 1913-8997
[12]. Mangkukusumo, dkk.2013.Analisa dan Perancangan Keamanan Mail Server Zimbra pada Sistem Operasi Ubuntu 8.04.e-journal Teknik Elektro dan Komputer
[13]. M. Tariq Banday,"Effectiveness and limitation of email security protocol", International Journal of Distributed and Parallel Systems (IJDPS)Vol.2, No.3, May 2011
[14]. Suni Awasthi,Praveen Tripathi,Akhilesh Kosta.2013. Stegno PGP with Enhance Security.International Journal of Advanced Research in Computer Science and Software Engineering.Volume 3, Issue 12, December 2013 ISSN: 2277 128X
[15]. Z. Durumeric, J. Kasten, M. Bailey, and J. A. Halderman.Analysis of the HTTPS Certificate Ecosystem. In Proc. ACM Internet Measurement Conference, Oct. 2013.

Author Biographies

Dr. Ir. Made Sudarma, M.A.Sc.
Department of Electrical and Computer Engineering
Faculty of Engineering, Udayana University
Bukit Jimbaran Campus, Bali, Indonesia
Tel./Fax : +62361703315

Dandy Pramana Hostiadi, S.Kom, MT.
Department of Computer System
STIMIK STIKOM BALI
Jl. Raya Puputan No. 86, Denpasar,
Bali 80234, Indonesia. Tel./Fax: +62361 244445