ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

# Mitigation of DOS Attack using PGP

[1]Yogita N. Jore, [2]Prof. Sachin S. Deshpande
[1] M.E. in Computer Engineering, [2] Associate Professor and Head of Computer Engineering Department
Vidyalanakar Institute of Technology, Mumbai
[1]yogita.khandagale@vpt.edu.in,[2] sachin.deshpande@vit.edu.in

***Abstract*: Denial-of-Service (DoS) attacks are a essential threat to the web. These attacks are targeting the application level. Detecting application layer DOS attack is not a straightforward task. A more refined mechanism is needed to distinguish the malicious ensue the legitimate ones. This paper implements a detection scheme primarily based on the PGP cryptography and PGP decoding technique, in which the users will transfer the file. The user can transfer the file primarily based on the random generated key of a private user. Pretty Good Privacy (PGP) is a encryption and decoding worm that gives scientific discipline privacy and authentication for electronic communication. PGP is often used for language, encrypting, and decrypting texts, e-mails, files, and directories**

***Index Terms*— DES, PGP encryption, PGP decryption, RSA algorithm, Cryptography, Secret key**

## I. INTRODUCTION

PGP, Pretty Good Privacy, is a "public key cryptosystem." (Also known as PKC.) In PGP, each person has 2 "keys": a "public key" that you simply provide to others, and a "private key" that only you apprehend. You use public keys to encrypt messages and files for others or to feature users to PGP Virtual Disk volumes. You use your private key to rewrite files and message that area unit encrypted along with your public key [10].

In computer networks, the sensitive data area unit encrypted on the sender aspect in order to own them hidden and guarded from unauthorized access so sent via the network [9]. When the information area unit received they're decrypted counting on rule and nil or additional cryptography keys. The existence of many applications on the web, for example e-commerce (selling and buying through the Internet) relies on network security. In a developing country like India, a majority of its local organizations stay victimization firewall alone as a methodology of protective their server from the intrusion problems.

However, it can be define that being dependent via this methodology alone for enhancing the protection level while not having different further protection may not be adequate enough to safeguard the server from being accessed by intruders; the construct of Pretty Good Privacy (PGP) is related to problems with pc security. While there have been various developments to confirm pc security like Intrusion hindrance, network device hardening, and router based firewalls and etc., the PGP concept could conjointly partly aid in providing valuable enhancements to problems regarding pc security. Cryptosystem consists of cryptographic algorithmic program, keys and protocols that make it work. A cryptographic algorithmic program is a function used for the secret writing and decipherment method. This algorithm works in combination with a key, which will be a word, number or phrase, used for encryption of plaintext into cipher text. The size of keys is measured in bits. The bigger the key, the more secure the cipher text. There are 2 varieties of encryption: symmetric and asymmetric. In symmetric (also referred to as secret key secret writing) one key is used for encryption and decipherment. This key is shared secret between communicating parties. Usually the size of secret's up to 128 bits. One example of this type is encryption commonplace (DES). It is in no time, but it will be terribly dearly-won owing to problem of secure key distribution.

This problem is resolved by asymmetric cryptography (also referred to as public-key encryption). It uses the pair of keys, one for encryption and one for cryptography. One is published and referred to as the public key; the opposite is unbroken secret and referred to as the private key. It is computationally infeasible to deduce the private key from the public key. The size of keys is up to 1024 bits.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

## II. LITERATURE REVIEW

PGP stands for "Pretty Good Privacy," and its most often utilized for sending encrypted messages between two people. This system ascertains that it's facile to send encrypted communications, because the only thing needed to encrypt a message is a public key and the opportune PGP program. But it's withal quite safe, as messages can only be decrypted with privately kenned keys that are password-for fended.

In advisement to encryption, PGP withal sanctions for digital signatures. By signing your encrypted message with your private key, you provide a way for the recipient of the message to optically discern if the content of the message has been transmuted. If even a single letter in the message is transmuted afore its decrypted, the signature will be invalidated, alerting the recipient to foul play.

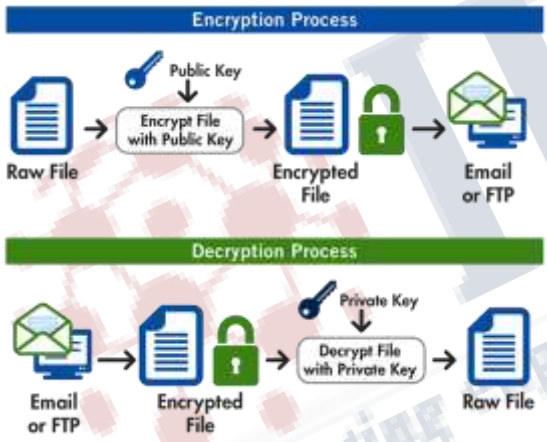


***Fig 1: PGP encryption and PGPdecryption process***

The mathematical mechanics of PGP are extremely complicated, but the diagram below will give you a general idea of how the system works [3].

### *a. How PGP Works*

PGP provides two main functions, encryption and digital signatures. PGP uses a standard public key encryption scheme, wherein it uses encoding and decoding algorithms to create a public key and a private key. The public key is used by other people to encrypt messages that they send to you, and the private key is used by you to decrypt messages that were encrypted with your public key. The idea is that you are the only person with access to your private key, so you are the only person that can decrypt messages that were encrypted using your public key.

PGP uses a combination of algorithms to perform encryption. The first step in PGP's encryption process is to compress the text that is to be encrypted, called plaintext. Next, the International Data Encryption Algorithm is used to generate a random session key, which is used to encrypt the compressed file, producing what is called the ciphertext. Continuing, the well-known RSA (Rivest, Shamir, and Adleman) public key encryption algorithm [4] is used to encrypt the session key using the recipient's public key. This encrypted session key is then placed at the front of the ciphertext file, which is now ready for sending. To decrypt messages, this process is essentially reversed using the private key though, instead of the public key.

### *b. Standards support for PGP encryption and PGP decryption:*

Asymmetric Encryption Algorithms

- Diffie-Hellman
- DSA
- RSA

The key sizes supported are 512, 1024, 2048 and 4096 bits.

Ciphers (Symmetric Encryption Algorithms)

- AES-128
- AES-192
- AES-256 (default)
- Blowfish
- CAST5
- DES
- IDEA
- Triple DES(DESede)
- Twofish

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

The default symmetric algorithm is AES-256, which can be changed by the user.

Hash Algorithms

- MD2
- MD5
- RIPEMD-160
- SHA1 (default)
- SHA-256
- SHA-384
- SHA-512

The default hash algorithm is SHA1, which can be changed by the user.

In the world of encryption there are many different names for encryption, but probably the two most common would have to be AES and PGP. But not everyone knows what these acronyms stand for.

AES is a symmetric key encryption algorithm, which essentially means that the same key is used for the encryption and decryption of the data. A computer program takes clear text and processes it through an encryption key and returns ciphertext. If the data needs to be decrypted, the program processes it again with the same key and is able to reproduce the clear text. This method required less computational resources for the program to complete its cipher process, which means lower performance impact. AES encryption is a good method to protect sensitive data stored in large databases [2].

There is, however, a time when AES will not be your go-to encryption process. When you need to share sensitive information with trading partners or transfer information across networks, using AES has one downside when it comes to security: You would have to share your encryption key with your trading partners. Sure, they'd be able to decrypt the information you sent them, but they would also be able to decrypt anything else encrypted with that key, and if the key itself became compromised anyone in possession of it could decrypt your data.

***c. Why PGP?***

No one wants his or her private or confidential documents to be read by anyone else other than the intended recipient. This is the same messages reason that traditionally most mail is sent in an envelope addressed to the recipient and not simply filled out on a postcard.

By providing the ability to encrypt messages, PGP enables the user to add an "envelope" to the electronic letter or document in form of encryption and decryption.

## III. SYSTEM ANALYSIS

***A. Proposed System***

You may be required to store or transmit files that contain sensitive information such as personal data, bank account numbers, financial information or health records. If not properly protected, these files could be vulnerable to attacks by hackers and other unauthorized users. By first encrypting those files with PGP encryption and decryption algorithm, you can add one level of security to this data. Other users could view the files in encrypted format.

Following figure describes the idea of mitigation of DoS attack system using PGP encryption and decryption technique.

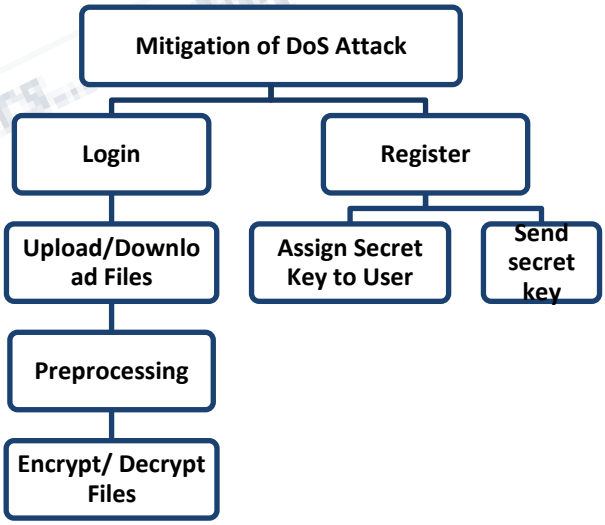


***Fig 2: Work flow of Mitigation of DoS attack using PGP***

The modules in proposed system are as follows:

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

1. Register: New user has to register with all details including e-mail account (Gmail account). As soon as register to this system, system will generate a secret key and mail to respective user account. This key is useful when user wants to download the file(s).

2. Login: Login the page to entered in system. After this, user can upload the file(s), manage files and download the files.

3. Key Recovery: If user forgot the key, then with the help of secret question's answer he/she could able to recover a key.

4. Uploading/ Downloading: While uploading and downloading the files, files are encrypted and decrypted and save. So unauthenticated users can not access others user's information.

***B. Database Design***

**XAMPP** is a free and open source cross-platform web server solution stack package developed by Apache Friends, consisting mainly of the Apache HTTP Server, MariaDB database, and interpreters for scripts written in the PHP and Perl programming languages. XAMPP stands for Cross-Platform (X), Apache (A), MariaDB (M), PHP (P) and Perl (P). It is a simple, lightweight Apache distribution that makes it extremely easy for developers to create a local web server for testing and deployment purposes. Everything needed to set up a web server – server application (Apache), database (MariaDB), and scripting language (PHP) – is included in an extractable file. XAMPP is also cross-platform, which means it works equally well on Linux, Mac and Windows. Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server extremely easy as well.
In this system, XAMPP 2.5 version is used. In this design, following are four tables are focused:

1. Department: contain only department id and department name. Following is the screenshot.

| id | name |
|---|---|
| 1 | Java |
| 2 | Php |
| 3 | .Net |
| 4 | MySQL |

***Fig 3: dept table***

2. Files: contain the information about downloaded files along with user id and time of downloading. Following is the screenshot.

| id | fname | user_id | time |
|---|---|---|---|
| 1 | rose.txt | 3 | 2014-08-04 16:26:52 |
| 2 | rushalinfo.txt | 3 | 2014-08-04 16:27:09 |
| 3 | tmp.txt | 2 | 2014-08-04 16:28:01 |
| 4 | decoy.txt | 1 | 2014-08-04 16:28:58 |
| 5 | pravin.txt | 4 | 2014-08-04 16:12:09 |
| 6 | decoyFile.txt | 1 | 2014-08-04 16:45:19 |
| 7 | decoy2.txt | 1 | 2014-10-25 20:09:25 |
| 8 | database.txt | 3 | 2014-10-25 20:12:50 |
| 9 | Testing.txt | 5 | 2015-06-04 13:55:36 |
| 10 | text.txt | 2 | 2015-07-31 16:29:07 |
| 11 | file.txt | 6 | 2015-07-31 17:05:26 |
| 12 | Car.docx | 1 | 2015-08-05 16:53:45 |

***Fig 4: files table***

3. Log details: contain the information about user id, action (File downloaded, login, invalid key). Following is the screenshot.

| id | user_id | action | status | time |
|---|---|---|---|---|
| 206 | 1 | Login | invalid | 2016-05-18 12:32:39 |
| 205 | 1 | File downloaded | invalid | 2016-05-18 12:23:14 |
| 204 | 1 | Login | invalid | 2016-05-18 12:22:48 |
| 203 | 10 | File downloaded | invalid | 2016-05-18 12:22:26 |
| 202 | 10 | File downloaded | invalid | 2016-05-18 12:22:22 |
| 201 | 10 | File downloaded | invalid | 2016-05-18 12:20:29 |
| 200 | 10 | File downloaded | invalid | 2016-05-18 12:19:40 |
| 199 | 10 | File downloaded | invalid | 2016-05-18 12:19:22 |
| 198 | 10 | File downloaded | invalid | 2016-05-18 12:19:01 |
| 197 | 10 | Login | invalid | 2016-05-18 11:58:16 |
| 196 | 1 | Login | invalid | 2016-05-17 21:53:29 |
| 195 | 13 | File downloaded | valid | 2016-05-17 21:32:00 |
| 194 | 9 | Login | invalid | 2016-05-17 10:12:03 |

***Fig 5: log details table***

4. Users: contain name, password, key, age, contact number, email id, dept id, secret question, answer of that question, ip address of system, and

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 7, July 2016

time and date of user creation. Following is the screenshot.

***Fig 6: users table***

## IV. CONCLUSION

In this paper, it is practical implementation of cryptographic techniques have been presented and analyzed in order to make encryption algorithms used in PGP .Pretty Good Privacy (PGP) is data encryption and decryption software that provides cryptographic privacy and authentication for data communication and also used for signing, encrypting and decrypting texts, e-mails, files. Pretty Good Privacy (PGP) perception can be applied to increase the level of security for a digital file. Using PGP encryption and decryption mechanism, little bit level of security is increased.

## REFERENCES

[1] Shihab A. Hameed; Habib Yuchoh; Wajdi F. Al-khateeb, "A model for ensuring data confidentiality: In healthcare and medical emergency**",** Print ISBN: 978-1-61284-435-0, 2011, IEEE

[2] http://web.townsendsecurity.com/bid/66064/AES-vs PGP-What-is-the-Difference

[3] http://www.goanywhere.com/products/mft/encryption

[4] Saranya, Vinothini, Vasumathi, "A Study on RSA Algorithm for Cryptography", International Journal of Computer Science and Information Technologies, Vol. 5 (4) 2014

[5] https://www.javacodegeeks.com/2011/06/java-pretty-good-privacy-pgp.html

[6] http://www.bouncycastle.org/java.html

[7] https://en.wikipedia.org/wiki/ Bouncy_Castle_ (cryptography)

[8] https://www.bouncycastle.org/documentation.html

[9] Veronika Durcekova, Ladislav Schwartz and Nahod Shahmehri, "Sophistucated Denial of Service Attacks Aimed at Application Layer", Print ISBN: 978-1-4673-1179-3,2012, IEEE

[10] Bharatratna Pralhadrao Gaikwad, "Cryptographi Process For Cyber Safeguard by using PGP, ISSN Print: 2320-9798, 2014, IJIRCCE

[11] Kamarudin Shafinah, Mohammad Mohd Ikram, "File Security based on Pretty Good Privacy (PGP) Concept", Computer and Information Science, Vol. 4, No. 4; July 2011