Impact Factor (SJIF): 4.542

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 4, Issue 4, April-2017

A Review on Secure Email Communications in E-commerce

Dimple D. Valia[1],Ravi K. Sheth[2]

[1] *Department of Information Technology & Telecommunications, Raksha Shakti University*

[2]*Department of Information Technology & Telecommunications, Raksha Shakti University*

Abstract: The growth of e-commerce business is very high now days. E-commerce allows the exchange of goods and services over the internet. Shopping of goods like electronics, groceries, fashion accessories and even vehicles through e-commerce has become popular now. With the rapid growth of internet, mobiles and other computing devices has made e-commerce easy to use. With the use of e-commerce, the use of emails for the communication purpose has also become popular. E-mail has become very common means of communication now days. Many companies and other organizations use email as a primary means of communication. The main drawback is that it makes very easy for criminals to fulfill their malicious intentions. This paper provides the method to secure and encrypt the e-mail using OpenPGP and GnuPG in e-commerce websites. This method will secure the data which are transmitted through email at the time of placing order and will improve customers' confidence in online shopping.

Keywords: email security, email threats, e-commerce, openpgp and gnupg

I. INTRODUCTION

E-commerce is an electronically conducted commercial transactions using computer over a large network. It involves the exchange of business information, customer details and even transaction details using emails. As e-mail system influence our life so much today in a positive way, on the other way cyber criminals are also using e-mail as tool to fulfill their malicious intentions. Recently available e-mail standards provide protection of e-mail messages using standard cryptographic techniques and formats like PGP and S/MIME. PGP is the popular program used to encrypt and decrypt the text files, emails, data files, directories and disk partitions. It also authenticates the messages with digital signature to keep data secure. PGP is useful in encrypting text files, emails, data files, directories and disk partitions. PGP had some licensing issues and so Zimmerman, one of the original PGP developers, developed an open-source version of PGP encryption (OpenPGP). OpenPGP is an open and free version of the Pretty Good Privacy (PGP) standard that contains encryption formats and also helps the users to send private messages through emails.

II. EMAIL SECURITY THREATS

2.1 Spam

Email spam is also known as junk emails, where unsolicited or unwanted messages are sent by emails. Spammers gets email addresses from newsletters, malwares that are transmitted from hacked email accounts, and website operators that sell email addresses. Spam emails can cause:

A. Network Congestion

Spam clogs the network. Although the emails are in smaller in size but receiving it in bulk can cause network congestion.

B. Malware

Spammers also send the links in emails which contains malwares. If the receiver clicks the link the malware will be harvested to his system.

2.2 Spoofing

E-mail spoofing occurs when an attacker sends you an e-mail pretending to be someone you know. Spoofing is like sending a letter to someone and forging the return address on the envelope. Email spoofing is easy to do, and very difficult to trace to its real sender.

2.3 Phishing

Phishing e-mails have become a favorite weapon of identity thieves, and they are becoming increasingly difficult to spot. Most phishing e-mails claim to be from a banking or other financial institution and send an e-mail pretending to be from your bank. There may even be a link that actually takes you to your bank's Web site. Even if you don't enter any personal information, clicking the link can infect your computer with data-stealing malware. Given below is the phishing sites detected from October 2015 to march 2016.

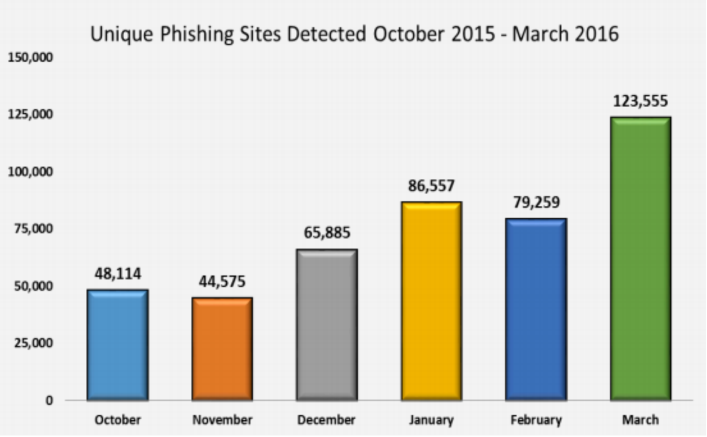

Figure 1: Chart Of Unique Phishing Sites Detected

III. CURRENT EMAIL SECURITY TECHNOLOGIES

Email security is the technique for keeping sensitive information in emails secure from unauthorized access. As email is the popular mode of communication, criminals uses email as a medium to spread malware, spam, phishing attacks and many more malicious activities to reveal the sensitive information. And thus email security becomes a necessary part for both individual and business email accounts to keep the data secure. Below are some current technologies used for securing emails:

2.1 Secure/Multipurpose Internet Mail Extensions (S/MIME)

S/MIME is the standard for public key encryption and signing MIME data. It ensures the recipient that you actually sent the email. It verifies the owner's identity and also provides sender's authentication, non-repudiation and message confidentiality using encryption and digital signature.

2.2 Sender Policy Framework (SPF)

Sender Policy Framework (SPF) is an email-validation system to detect email spoofing. Email spam and phishing uses fake "From:" addresses. The goal of SPF is to reduce the amount of spam and phishing which is used to forge the emails and pretending to be from that domain.

2.3 Domain Keys Identified Mail (DKIM)

DKIM is the method for email authentication to detect email spoofing. It ensures the receiver that the email came from specific domain was authorized by the sender of that domain. Here the sender adds the digital signature to the email header and receiver verifies it

2.4 Pretty Good Privacy (PGP)

Pretty Good Privacy or PGP is a program used to encrypt and decrypt email. PGP uses public key system where user has the public key that is known only to that user or sender. The message is then encrypted using receiver's public key. When the receiver receives the message he can decrypt it using his private key. It's actually very good privacy. It can protect the contents of your emails and files from the attackers or even the government surveillance programs.

A. How PGP works?

Pretty Good Privacy creates and uses public and private keys. You can create a public/private key pair, private key will be password-protected, and then to encrypt and sign the text one needs to use that password-protected private key and public key. It will also let you download other people's public keys, and upload your public keys to “public key servers”.

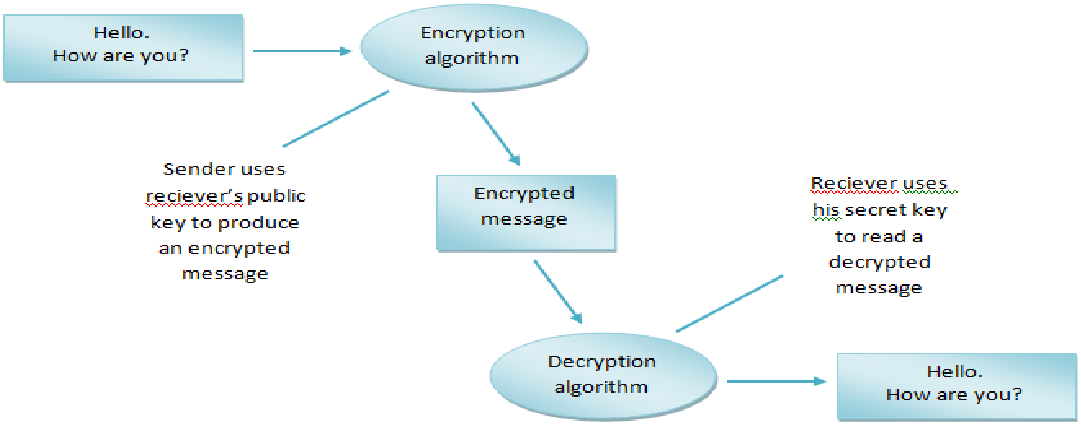
Hello.
How are you?
Encryption algorithm
Sender uses reciever's public key to produce an encrypted message
Encrypted message
Reciever uses his secret key to read a decrypted message
Decryption algorithm
Hello.
How are you?

Figure 1: How PGP works?

IV. RELATED WORK

[1] Describes the use of PGP (Pretty Good Privacy) and PEM (Privacy-Enhanced Mail). PGP is the program used to encrypt and decrypt the emails. PGP provides two services: encryption and digital signatures. It can also be used to send an encrypted digital signature that verify the sender's identity and ensures that the message was not changed en route. PEM provides the security features such as authentication, message confidentiality, and data integrity.

[5] This paper describes the system to wide-spread the deployment of OpenPGP compliant email encryption across platforms and mail user agents which perform the required encryption and decryption work and assist in key management.

[7] This paper provides overview of relevant security standards and proposed a solution for email authentication and encryption for e-commerce sites to protect potentially sensitive customer email communication. The solution is based on OpenPGP and public key encryption. This paper also demonstrated an implementation of email encryption module for an open source e-commerce platform.

[8] This paper proposed a solution to improve and enhance the security of email. The solutions include a particular enhancement such as authenticated e-mail systems and the confidentially and Privacy e-mail Systems. It also states that integrity and non-repudiation, needs to integrated with other enhancements to provide the solution with high level of security.

V. SECURING EMAILS USING OPENPGP AND GNUPG

A. OpenPGP

Zimmerman, the one who developed original PGP, worked on an open-source version of PGP encryption that employed encryption algorithms that had no licensing issues. OpenPGP is an open and free version of the Pretty Good Privacy (PGP) standard that contains encryption formats and also helps the users to send private messages through emails. In OpenPGP you can apply two different keys: primary keys and subkeys.

At the time of the generation of OpenPGP keys, a primary key with at least one subkey is created. Only the primary key can be used for certification, that is, to certify the credibility of other keys. The primary key is also used to sign payloads. The subkey is used to encrypt payloads.

B. GnuPG

GnuPG is a complete and free implementation of the OpenPGP standard as defined by RFC4880. GnuPG allow encrypting and signing your data and communication, features a versatile key management system as well as access modules for all kinds of public key directories. GPG (GnuPG) is a command line tool with features for easy integration with other applications.

GPG allows user to generate public and private keys using the command gpg – gen-key. The encryption and signing commands are:

Table 1: GnuPG encryption and signing commands

Command	Description
gpg –encrypt Recipient [Data]	Encryption
gpg [--decrypt] [Data]	Decryption
gpg –clearsign [Data]	Creates a human readable signature using a private key from keyring
gpg [--verify] [Data]	Verifies the signature (requires access to signers public key)

VI. CONCLUSION

This paper gives an overview of relevant security standards and solution for email authentication and encryption for web shops to protect potentially sensitive customer email communication. An end-to-end secure channel for sending information from e-commerce sites to customers is needed. Although standards and tools for securing email communication exist, there is still the gap between the systems. Thus the solution based on OpenPGP and GnuPG can be used to secure the email communications of e-commerce websites.

ACKNOWLEDGEMENT

I express my very profound gratitude to everyone for providing me with unfailing support and continuous encouragement throughout the process of researching and writing this thesis. Thank you.

REFERENCES

[1] Konstantinos Raptistis, E-Mail Security: PGP (Pretty Good Privacy) & PEM (Privacy-Enhanced Mail), European Intensive Programme on Information and Communication Technologies Security IPICS'99

[2] Denison James Parreno, Simple Secure Email (SSE) - Email Security For Ecommerce Sites

[3] https://www.techopedia.com/definition/29704/email-security

[4] http://searchsecurity.techtarget.com/definition/Pretty-Good-Privacy

[5] https://digitalguardian.com/blog/what-email-security-data-protection-101

[6] Dan Berger, ARKE: A Proposal for Simplified OpenPGP E-mail Security, March 2003

[7] http://www.viacorp.com/crypto.html

[8] Andres Ojamaa, Uku-Rasmus Lind, Securing Customer Email Communication in E-Commerce, 2013 Sixth International Conference on Developments in eSystems Engineering

[9] Afnan S. Babrahem, Eman T. Alharbi, Aisha M. Alshiky, Saja S. Alqurashi, Jayaprakash Kar, Study of the Security Enhancements in Various E-Mail Systems, Journal of Information Security, 1-11,2015

[10] https://ssd.eff.org/en/module/introduction-public-key-cryptography-and-pgp

[11] http://www.dummies.com/computers/computer-networking/network-security/types-of-threats-to-e-mail-security-on-a-home-network