IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

A Study on Security Approaches for Authentication Processes for Email Transactions

Shananda Dey[1], Ms. Jharna[2]

M.E. Computer Science & Engineering Dept, Shankaracharya Group of Institutions, Bhilai (C.G.), India[1]

Asst Professor, Computer Science & Engineering Dept, Shankaracharya Group of Institutions, Bhilai (C.G.), India[2]

Abstract: Email, sometimes written as e-mail, is simply the shortened form of "electronic mail," a system for receiving, sending, and storing electronic messages. It has gained nearly universal popularity around the world with the spread of the Internet. In many cases, email has become the preferred method for both personal and business communication. So, enhance the security provision in essential to maintain integrity and confidentiality of data. Currently the system offers only OTP as an additional verification during email transactions. The current paper focuses on conducting a study on concept of email security and challenges.

Keywords: Handshaking Protocol, OTP, Captcha, Email Security.

I. INTRODUCTION

In present circumstance we are having both manual message sending an Email, sometimes indited as e-mail, is simply the minimized form of "electronic mail," a system for receiving, sending, and storing electronic messages. It has gained approximately ecumenical popularity around the world with the spread of the Internet. In many cases, email has become the preferred method for both personal and business communication. Secure email transactions have become a desideratum for preserving privacy of utilized information currently the system offers only OTP as a supplemental verification during email transactions. So, enhance the security provision in essential to maintain integrity and confidentiality of data. Proposed work aims to integrate a security framework for securing email authenticate as well as email data storage.

The magnification of cryptographic technology has raised a number of licit issues in the information age. Cryptography's potential for utilize as an implement for espionage and sedition has led many regimes to relegate it as a weapon and to circumscribe or even proscribe its use and export. In some jurisdictions where the utilization of cryptography is licit, laws sanction investigators to compel the disclosure of encryption keys for documents pertinent to an investigation. Cryptography additionally plays a major role in digital rights management and piracy of digital media

A handshaking protocol is the method by which two computers on a network establish a connection utilizing some kind of networking implement. Each kind of network connection, such as a request from a Web browser to a Web server, or a file-sharing connection between two peer computers, has its own handshaking protocol that must be consummated before consummating the action requested by the user.

A handshaking protocol defines the method by which data is expected to be received, the content of the initial data sent and the parameters of the replication. A handshake can be a single-query-replication step, or it can be many such steps. A ping from one computer to another sends a single Internet packet and responds with another single packet; as this is the simplest possible handshake, it is often used to test fundamental network connections. On the other hand, a virtual private network connection request will have many handshaking steps as the VPN may verify the incoming IP address of the request, the user name and password and the requested access; meanwhile, the sending computer will evaluate the integrity of the VPN's security certificate.

II. RELATED WORK

A consequential usability goal for authentication systems is to fortify users in culling better passwords. Users often engender memorable passwords that are easy for hackers to conjecture, but vigorous system assigned passwords are arduous for users to recollect. In a work a click predicated graphical password scheme called Persuasive Cued click Points is presented. In this system a password consists of sequence of some images in which utilizer can cull one click point per a concrete region of an image. In integration utilizer receives an OTP through Email in order to verify himself to the system [1].

In one of models a Click-predicated graphical password scheme called Persuasive Cued Click Points (PCCP) is presented. In this system a password consists of sequence of some images in which utilizer can cull one click-point per a concrete region of an image. In additament utilizer receives a OTP through Email in order to verify himself to the system. The OTP is engendered utilizing arbitrary algorithm by which it is make unique for each and every time the utilizer requests for logins. If the utilizer culls the correct click a point on each region of set of images culled and has to verify the OTP sent to him in order to access his information [2]. In another work an image predicated authentication utilizing Visual Cryptography (VC) and the encryption algorithm (RSA) is utilized [3]. Visual cryptography is mainly done by splitting the pristine

image into two shares one with utilizer database and one with the server database. An incipient approach is designated as "Anti-phishing structure predicated on visual cryptography and RSA algorithm" to solve the quandary of phishing. Thus security of image can be achieved by visual cryptography and RSA algorithm. Phishing can be rudimentally defined as one kind of assailment in which sundry assailers acquire the confidential and sensitive information of the victims. In another approach DCT is applied to 2 colour images for the DCT transformed images LSB is applied with the bits of the portions which got from VC [4]. First level of security is achieved by utilizing visual cryptography for the information to be transmitted and this is embedded onto images by utilizing Steganography. The approach mainly uses transform predicated Steganography (DCT) and visual cryptography for obnubilating data.

III.EMAIL SECURITY

In Email security refers to the collective measures used to secure the access and content of an electronic mail account or accommodation. It sanctions an individual or organization to for fend the overall access to one or more email addresses/accounts. Email security is a broad term that encompasses multiple techniques used to secure an electronic mail accommodation. From an individual/end utilizer standpoint, proactive email security measures include vigorous password rotations and spam filters and desktop-predicated anti-virus/anti-spam applications. Similarly, an accommodation provider ascertains email security by utilizing vigorous password and access control mechanisms on an electronic mail server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber electronic mail address. It withal implements firewall and software-predicated spam filtering applications to restrict unsolicited, untrustworthy and malignant email messages from distribution to a user's inbox.

IV.EMAIL SECURITY CHALLENGES

An electronic mail provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit. Current Email systems still face a number of jeopardies and challenges. These include:

Authenticate /Password: Can be fetched by different sources. The traditional authenticate/password technique is facilely accessed by unauthorized users. It can be facilely be conjectured.

OTP (One Time Password): Dependent on mobile networks & if in any case we lose our mobile then we might not get the OTP. OTP predicated systems are withal dependent upon network. If network is not available utilizer may not get OTP.

Captcha: Only verifies whether the authenticate is human or robot. The captcha technique is unable to verify whether the utilizer is sanctioned or not.

Untrusted: No opportune mechanism to verify whether client or server is trusted or not other than 3rd party certification.

So overall the subsisting system is generalized but not utilizer predicated. The security approaches are not customized according to user's need.

V. CONCLUSION

In Emailing Systems can be trusted as a platform to secure information transfer provided that they are well implemented. User authentication, integrity, user anonymity and system accountability as some of the critical functional requirements that emailing Systems should have. It facilitates many features for the ease of users those are user friendly screens to enter the data, depending upon the category of user the security layers are decided. Web enabled and compatible with various systems.

REFERENCES

[1] Security Implementation of 3-level Security System Using Image Based Authentication, M. Manjunath, Mr.K.Ishtaq Ahamed & Ms.Suchitra, IJETT in Computer Science (IJETTCS) ISSN:2278-6856 VOL-2,Issue-2 (March-April 2015).

[2] Image Based Authentication Using Visual Cryptography & Encryption Algorithm, Shreya Zarkar, Sayali Vaidya, Arifa Tadvi, Tanashree Chavan, Prof.Achal Bharambe,IJ in Computer Science & Information Technology (IJCSIT) ISSN:0975-9646,VOL-6(2),Yr-2015.

[3] R. Dhamija and A. Perrig, "Deja Vu: A User Study Using Images for Authentication," in proceedings of 9th USENIX Security Symposium, 2000.

[5] S. Akula and V. Devisetty, "Image Based Registration and Authentication System," in Proceedings ojlv1idwes Instruction and Computing Symposium, 2004.

[6] L. Sobrado and J.-C. Birge!, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[7] Sonia chaisson, Alian Forget, Robert Biddle, P. C.van Oorschot, "User interface design affects security: patterns in click-based graphical passwords", Springer-Verlag 2009.

DOI 10.17148/IJARCCE.2016.5204