IJARCCE

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Approaches for Securing Email Authentication Process – A Review

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

M.E. Dept CSE Shankaracharya Group of Institutions, Bhilai (C.G.), India[1]

Assistant Professor, Dept. CSE Shankaracharya Group of Institutions, Bhilai (C.G.), India[2]

Abstract: Email, sometimes written as e mail, is simply the reduced form of "electronic mail" a system for receiving, sending, and holding electronic messages. It has gained practically universal acceptance around the world with the spread of the World Wide Web. In many cases, email has become the preferred method for both personal and business communication. Consequently, improve the security provision in necessary to maintain integrity and confidentiality of data. Passwords are by far the most used and the most conveniently subverted method of personal authentication. If a business institutes policies to guarantee secure passwords (such since frequently changed alphanumeric upper/lower case combo of by least 10 characters) the inconvenience is so high that such an plan will probably be broken in an overwhelming amount of instances.

Keywords: Handshaking Protocol, OTP, Captcha, Visual Cryptography.

I. INTRODUCTION

In present circumstance we are having both manual voting and 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. Secure email transactions have become a necessity for preserving privacy of user information currently the system offers only OTP as an additional verification during email transactions.

So, enhance the security provision in essential to maintain integrity and confidentiality of data. Proposed work aims to add an additional security framework for securing email login as well as email data storage.

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export. In some jurisdictions where the use of cryptography is legal, laws permit investigators to compel the disclosure of encryption keys for documents relevant to an investigation. Cryptography also 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 using some kind of networking tool. 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 completed before completing 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 response. A handshake can be a single-query-response 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 basic 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

An important usability goal for authentication systems is to support users in selecting better passwords. Users often create memorable passwords that are easy for attackers to guess, but strong system assigned passwords are difficult for users to remember. In a work a click based graphical password scheme called Persuasive Cued click Points is presented. In this system a password consists of sequence of some images in which user can select one click point per a specific region of an image. In addition user receives a OTP through Email in order to verify himself to the system [1].

In another work an image based authentication using Visual Cryptography (VC) and the encryption algorithm (RSA) is used [2]. Visual cryptography is mainly done by splitting the original image into two shares one with user database and one with the server database. A new approach is named as "Anti-phishing structure based on visual cryptography and RSA algorithm" to solve the

problem of phishing. Thus security of image can be achieved by visual cryptography and RSA algorithm. Phishing can be basically defined as one kind of attack in which various attackers acquire the confidential and sensitive information of the victims. In another approach DCT is applied to 2 color images for the DCT transformed images LSB is applied with the bits of the shares which got from VC [3] . First level of security is achieved by using visual cryptography for the information to be transmitted and this is embedded onto images by using Steganography. The approach mainly uses transform based Steganography (DCT) and visual cryptography for hiding data.

III.EMAIL SECURITY

In Email security refers to the collective measures used to secure the access and content of an email account or service. It allows an individual or organization to protect the overall access to one or more email addresses/accounts. Email security is a broad term that encompasses multiple techniques used to secure an email service. From an individual/end user standpoint, proactive email security measures include strong password rotations and spam filters. Desktop-based anti-virus/anti-spam applications. Similarly, a service provider ensures email security by using strong password and access control mechanisms on an email server; encrypting and digitally signing email messages when in the inbox or in transit to or from a subscriber email address. It also implements firewall and software-based spam filtering applications to restrict unsolicited, untrustworthy and malicious email messages from delivery to a user's inbox.

IV. EMAIL SECURITY CHALLENGES

An email service provider implements email security to secure subscriber email accounts and data from hackers - at rest and in transit.Current Email systems still faces a number of risks and challenges. These include:
Login /Password: Can be fetched by different sources. The traditional login/password technique is easily accessed by unauthorized users. It can be easily be guessed.

OTP (One Time Password): Dependent on mobile networks & if in any case we loose our mobile we might not get the OTP.OTP based systems are also dependent upon network strength. If network is weak user may not get OTP.

Captcha: Only verifies whether the login is human or robot. The captacha technique is unable to verify whether the user is authorized or not.

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

So overall the existing system is generalized but not user based. The security approaches are not customized according to user's choice.

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 and 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] Design & Implementation of K-Split Segmentation Approach for Visual Cryptography, Puja Devi Rana,Anita Singhvora,Suman Deaswal,IJ of Scientific & Research Publication (IJSRP) ISSN:2250-3153,VOL-2,Issue-8,Aug-2012.

[4] Double Layer Security using Visual Cryptography & Transform Based Steganography,Pallavi B, Vishala I L,IJ of Research in Engineering & Technology (IJRET) ISSN:2319-1163,VOL-3,Spl Issue-03,May-2014.

[5] An Improved (8,8) Color Visual Cryptography Scheme using Floyd Error Diffusion,Anantha Kumar Kondra,Smt U.V.Ratna Kumari ,IJ of Engineering Research & Application (IJERA) ISSN:2248-9622,VOL-2,Issue-5,Sep-Oct-2012.

DOI 10.17148/IJARCCE.2016.54159