ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

An ISO 3297: 2007 Certified Organization Vol.5, Special Issue 2, April 2017

An International Conference on Recent Trends in IT Innovations - Tec'afe 2017

Organized by

Dept. of Computer Science, Garden City University, Bangalore-560049, India

Enhancing Privacy Using Hidden Inbox in E-Mail Services

S.Meenakshi Ganesh, Vikash Kumar

Dept. of Master of Computer Applications, JAIN University, Bangalore, India

Dept. of Computer Science & IT, JAIN University, Bangalore, India

ABSTRACT: We live in a world that makes us very vulnerable online to predators, who seek out everyday to steal our identities, account numbers, social security numbers and many other various forms of sensitive Personal Identifying Information (PII) [1][5]. Email security refers to the measures used to secure and access the content of an email account or service.[6] It allows an organization to protect the overall access to one or more email addresses, accounts and the contents of it. Providing security is very crucial because sensitive data can be communicated through emails such as bank or login credentials or passport details. The current security we have in using emails is that the data is sent and received on the either ends in an encrypted form. The email account is also protected with the help of a password associated with a username. There is nothing much left to be done if that password and username falls into wrong hands. Anyone can be threatened to reveal their password and thus the access to the account can be gained. To enhance the security and privacy further, the implementation of a hidden inbox can help. In this approach, we can classify some email addresses as senders of very sensitive data and can be added to a list. All the emails from those addresses contained in the lost would be automatically delivered into a hidden inbox, which will never indicate its presence anywhere on the email page, which could be accessed only with the help of a special password typed on the screen. This is adding up another great layer of security and privacy to the sensitive data that we have and that we are expecting to receive.

KEYWORDS: HTTPS, encryption, decryption, hidden interface.

I. INTRODUCTION

Electronic mail [7] or email has become a very important part of the world such as WhatsApp and phone calls. E-mail is a very important service and security along with privacy in sending and receiving emails can never be compromised as it can contain crucial data. It’s not necessary that every email should contain sensitive data, but many of the users want privacy and security for their personal information contained in e-mails. For using e-mail services, one should have an account from the e-mail service provider, which is authenticated with a username and a password, which would be known only to that user. The username and password should be kept a secret because anyone who knows it can access the account easily, which may lead to leakage of crucial data to the organization or any personal information, which is not a desired condition.[8] Information such as client information,[9] payment information, personal files, bank account details - all of this information can be hard to replace and potentially dangerous if it falls into the wrong hands. Therefore, ensuring privacy and security is very important while using any e-mail services.

II. EXISTING SYSTEM

Currently, encryption[10] and decryption[11] is the security measure provided by web hosting services using certain protocols such as HTTPS (Hyper Text Transfer Protocol Secure[4]).[2] The usernames and passwords too are encrypted and decrypted at either ends of communication using this https protocol. The messages sent through an email as such is not encrypted or decrypted with 128 or 256 bits mostly and this does not provide us with much data security.[3] Data security is very important because crucial data for any business, if leaked could cause serious damage to business continuity, and thus effect the whole business organization. Even if the data security is ensured in an email, privacy is yet another important factor that must be kept in mind while providing and using such services bases on the web environment. In emails, protecting one’s account with a username and password ensures privacy. Someone needs to have the correct username and password to access the e-mails that have come to that address and even to send one the access to this account is needed. The feature of single sign on also lets us to link multiple accounts to one e-mail address, which is a great feature if implemented securely. Having said that, if this username and password fall into a wrong hand, if could be misused in many ways.

Several measures[12] can be taken to keep it safe but unfortunately, if that gets leaked, all the security and data privacy is compromised. The use of digital data has been increased to a very huge extent and it is very important to ensure security to the data that we have. For most of us, the email messages we send wouldn't be classified as sensitive. They can be personal, yes, and occasionally you'll want to make sure the content of a message is kept confidential between sender and receiver. But sometimes, sending sensitive information such as passport or credit-card numbers, for instance via email is necessary. At such points, we would consider sending an encrypted email message.

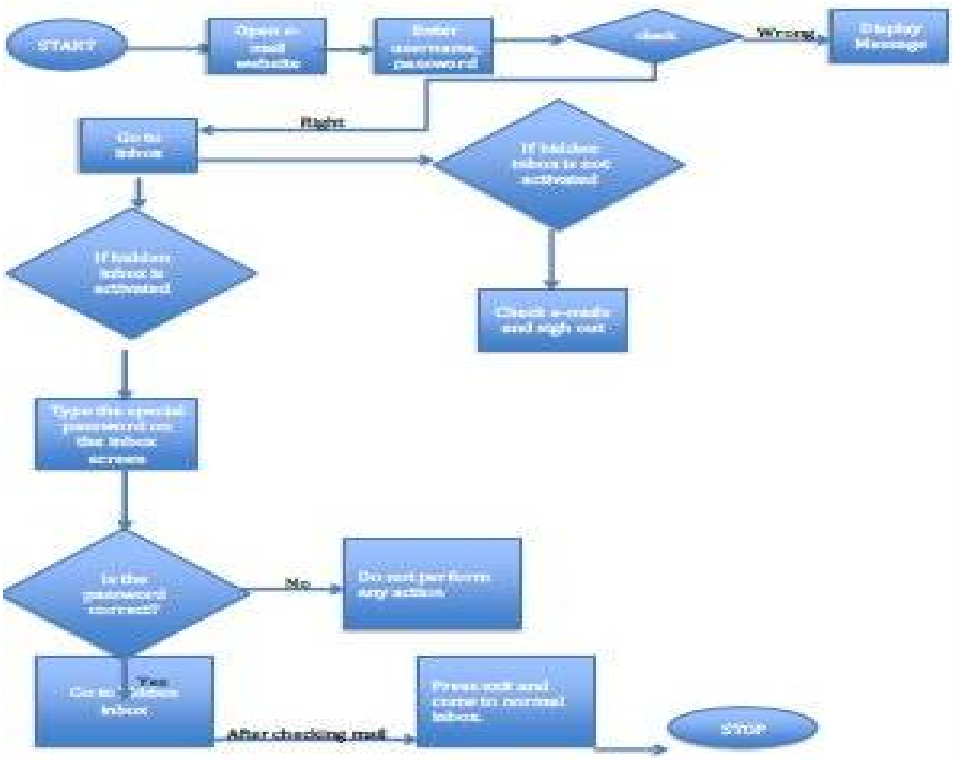
Standard email messages are sent in plain text, so it's possible for someone else to snoop on you and read them. When you encrypt mail, on the other hand, it makes the messages completely unreadable to anyone who doesn't possess the decryption key. The real threat arises when the username and password that protects an account has fallen into the wrong hands. They could easily access all the content and related accounts that has been synced with this email address.

Since data can be compromised in many ways, the best security against misuse or theft involves a combination of technical measures, physical security and a well-educated staff.

III. PROPOSED SYSTEM

Above mentioned are the problems that could arise if a person's username and associated password has been compromised. Let me now introduce a new measure to enhance the existing security and privacy. A hidden interface in an email account can provide an additional layer of security to the emails and the data we need to double protect. This can be implemented with the help of a hidden inbox. This inbox page would be hidden behind the actual page that shows all the emails that we have received, which is generally termed as our Inbox, which could be accessed only by entering a special password consisting of a combination of keys that do not perform any other function on the web page that has been opened. In the proposed method, the page would never ask to enter the special password to reveal the e-mails in the hidden interface/ inbox, which makes sure that only the one who has activated a hidden inbox associated with his email knows about the existence of such an inbox, which builds a great wall of security. This approach is very helpful in hiding very sensitive e-mails.

IV. FLOWCHART


START
Open e-mail website
Enter username, password
check
Wrong
Display Message
Right
Go to inbox
If hidden inbox is not activated
Check e-mails and sign out
If hidden inbox is activated
Type the special password on the inbox screen
Is the password correct?
No
Do not perform any action
Yes
Go to hidden inbox
After checking mail
Press exit and come to normal inbox.
STOP

V. IMPLEMENTATION

These are the steps to implement the hidden inbox concept.

1. First create a list of emails, from which the mails should be categorized as hidden ones and those emails should be accessible only from the hidden inbox.
2. Activate the hidden inbox feature from settings
3. Create a list and add the email addresses from which the emails should be hidden.
4. Set the special password for the hidden inbox.
5. Type this password to access the hidden e-mails in future.
6. The current password cannot be changed without providing the hidden inbox password in conjunction with the current or general password associated with the account.
7. If tried to change password illegally, do not let to enter the wrong special password more than two times.

VI.CONCLUSION

In this research, we have showed the privacy enhancement that can be done. This shows that we can have a secondary inbox, which is more secured, and safe. This secondary inbox is hidden from plain sight and can be accessed through a special password. This is useful when we have people around us who can peep over and see our passwords and get access to sensitive information. In the current world having privacy is as important as having a safe place to store data. In the IT industry information plays the key role and securing it is a vital part of the job. Having a secondary inbox provides a two-tier security

REFERENCES

[1] https://neocertified.com/why-is-secure-email-important/
[2] http://www.bitpipe.com/tlist/Data-Encryption-Standard.html
[3] https://digitalguardian.com/blog/what-email-encryption
[4] http://www.w3.org/Protocols/rfc2616/rfc2616.html
[5] http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information
[6] https://www.sonicwall.com/products/email-security-appliance/
[7] http://searchexchange.techtarget.com/definition/e-mail-electronic-mail-or-email
[8] http://smallbusiness.chron.com/use-email-business-communication-118.html
[9] http://www.statcan.gc.ca/eng/about/client
[10] https://www.checkmarx.com/2016/08/18/encryption-security-news-brief-history/
[11] http://www.encyclopedia.com/science-and-technology/mathematics/mathematics/decryption
[12] http://www.ibtimes.co.uk/how-protect-your-email-account-hackers-six-tips-help-you-stay-safe-1543332