JES
Journal of Engineering Sciences

Vol 11, Issue 1, Jan /2020
ISSN NO:0377-9254

EMAIL COMMUNICATION WITH CIRCUMVENTION TOOL

[1]P.SIDDHARTHA & [2]LAVANYA VEMULAPALLI

[1]M-Tech, Dept of IT CNIS, VNRVJIET, Email id: - siddu0454@gmail.com

[2]Assistant professor, Dept of IT CNIS, VNRVJIET, Email id: - lavanya_v@vnrvjiet.in

Abstract

In our current online generation, we have many types communication system, in those we are mainly using social sites and for all official, professional, financial communication system we're using email services. In the email system we also required some third party protocol to send the email from a machine due to bulk emails like salary statements, announcement etc. Using these third party services we also have problem of phishing, spam email etc. By taking these problems in this paper, we proposing monitor of email by using the CIRCUMVENTION, a specifically to be had censorship-resistant infrastructure. We capture this transaction by monitor the sender websites who are sending mails using public third party email service like Gmail, Yahoo etc. Our system we check the each and every email sending transaction through our server and verify the sender details and deliver to the user by using proxy server. We demonstrated our model by using of the web application. We got the expected and best results by comparing with literature.

Keywords: - CIRCUMVENTION server, Email agent, Converter, Web Browser

1. INTRODUCTION

In the current generation emails are used for the very formal transactions like financial statements, official announcement from the companies like job offers etc. It is very difficult forward a notification email like reminder of the credit card payment by the person to person, so based pn these reasons mail service providers provide some third party gateway to send mails using programs or applications. For example when user not paid bill application will send a mail reminder to user email. Application itself prepare mail body, subject and sender email. But using this public protocol we have few disadvantages also like phishing, spam email. We need to prepare a system which will filter those emails. As a quit end result, repressive regimes extensively show their citizens' get entry to the Internet and restrict open get right of entry to public networks [1] by means of the use of distinct era, starting from easy IP address blocking off and DNS hijacking to the extra complicated and resource-in depth Deep Packet Inspection (DPI) [2], [3]. In literature network based application will track the every incoming mail IP address. Comparing

with our proposed system its completely opposite like our system will track the mails at sender side but in the network based it's be receiver based model. In test based by the help of the data mining technique like term frequency inverse document frequency (tf-idf) or naïve bayees algorithms used to predict any email text like body text is genuine or not. For this there were using data collection of spam emails with body content, created models and prediction the every incoming mail but this vey impractical because of the huge data. Next in the domain based models is also verify the each and every email by the time of incoming to the receiver. Here proposed algorithms will compare the every incoming email with their own host address and domain of the email like @xyz.com. These survey won't satisfy the ecurity of the email communication. Public domains of Gmail, yahoo etc will help to send emails to the user using the third party services, these are oblivious servers which doesn't monitor the email distribution. Based on these we are proposing an architecture called SWEET server for prediction of the email verification. SWEET server is a third party server which will in between users and email servers like. When email send from the sender, here Sender may user or application our agent serve0r will verify the email by converting email, it will verify the with register emails, if everything was clear then only proxy server send that email to user.

2. RELATED WORK

Existing System

In literature, means in existing systems there are few technologies were used to track and filter emails in network based, domain based, and text based. In Network based application will track the every incoming mail IP address. Verify the every incoming mail IP address and filter to be spam or not. In text based by the help of the data mining technique like term frequency inverse document frequency (tf-idf) or naïve bayees algorithms used to predict any email text like body text is genuine or not. In the domain based models is also verify the every email by the time of receiving stage. Here algorithms will compare the every incoming email with their own host address and domain of the email like @xyz.com. These survey won't satisfy the security of the email communication.

Proposed machine

By taking disadvantages from the literature we are proposing an architecture called SWEET server for prediction of the email verification. SWEET server is a third party

Vol 11, Issue 1, Jan /2020
ISSN NO:0377-9254

server which will in between users and email servers like public domains of Gmail, yahoo etc. When email send from the sender, here Sender may user or application our agent server will verify the email by converting email, it will verify the with register emails, if every thing was clear then only proxy server send that email to user.

3. IMPLEMENTATION

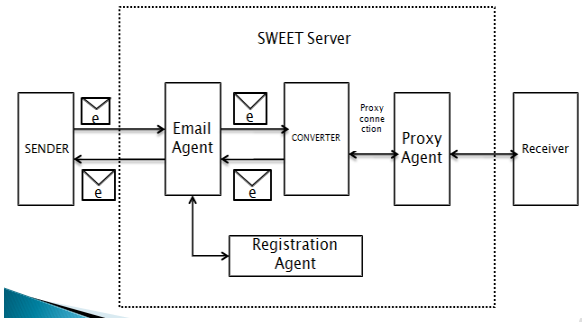

Fig:-1 System Architecture

SWEET server

Our proposed model SWEET server will verify the emails from the oblivious servers. Generally the mail servers which doesn't verify the application sending emails using SMTP protocols, we are preparing this architecture using few modules listed below as per our architecture mentioned in fig 1.

Email agent

Email agent receives the emails from the public oblivious server using MAP or SMTP protocol's, email agent will verify the email with registration agents. Email agent will forward the email to the converter, converter after it's process forward email to the proxy server through proxy connection.

Converter

The converter techniques the emails handed by the e-mail agent, and extracts the tunneled community packets. It then forwards the extracted facts to some other thing, the proxy agent. Also, the converter receives community packets from the proxy agent and converts them into emails which can be targeted to the e-mail cope with of corresponding customers. The converter then passes these emails to the e-mail agent for delivery to their intended recipients. As described later, the converter encrypts/decrypts the email attachments of a consumer using a secret key shared with that character.

Proxy agent

The proxy agent proxies the community packets of customers that are extracted through the converter, and sends them to the Internet destination requested by using the clients. It also sends packets from the vacation spot again to the converter.

Registration agent

Here Registration Agent nothing but the user who register to the SWEET server called SWEET user, SWEET user will have a secrete key to verify his own account. Which will helps to prevent the DOS

attacks. This secrete key will help to encrypt the tunneled data in the server in the transaction of sender and receiver of the emails.

Client registration

Before the first actual use of the CIRCUMVENTION provider, a patron wishes to sign in her email cope with with the machine. This is routinely finished thru the customer's CIRCUMVENTION software program. The goal of patron registration is twofold: to prevent denial-of-provider (DoS) assaults and to percentage a mystery key among a customer and the server.

Circumvention Client

In this module, a consumer wants to achieve a replica of CIRCUMVENTION's purchaser software and installation it on her gadget. The purchaser moreover needs to create one or e-mail account (depending on if she uses an Alien Mail or a Domestic Mail for her primary email).A client wants to configure the established CIRCUMVENTION's software with facts approximately her e-mail account. Prior to the number one use of CIRCUMVENTION through a customer, the patron software registers the e-mail cope with of its client with the CIRCUMVENTION server and obtains shared mystery key.

Web Browser

Our application is a web based, web based application will works on the only web browsers like chrome, opera, safari etc. Depends on the some frontend code like CSS and javascript some versions may required or recommended to the web application. Whenever a request raise from the browser it will forward to the proxy server.

Converter

Converter will help to convert to emails in to the packets in the SWEET architecture. It will convert the emails in between agent and proxy servers. Converter will use the secrete key to convert encryption data decryption data and vice versa.

Email Agent

It sends and gets CIRCUMVENTION emails thorough the consumer's e mail account. The consumer wants to configure it with the settings of the SMTP and IMAP/POP3 servers of her e mail account. The purchaser additionally needs to offer it with the account login records.

Proxy Protocol

In this module, the CIRCUMVENTION server makes use of a proxy agent to get hold of the tunneled web page visitors of customers and to set up connections to the asked locations. We remember the usage of

every SOCKS and HTTP proxies inside the format, as each offers specific blessings. After conversion of the emails proxy protocol will send the emails to the intended users. In evaluation, an HTTP proxy simplest allows access to HTTP places. However, an HTTP proxy may additionally boost up connections thru the usage of HTTP-layer optimizations along side caching or pre-fetching of net objects.

4. EXPERIMENTAL RESULTS

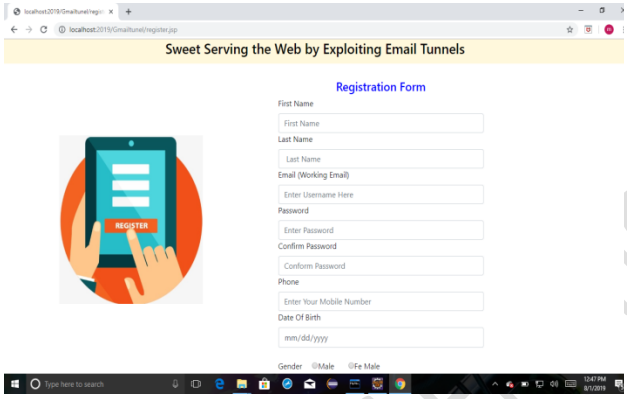

Fig:-2 Registration

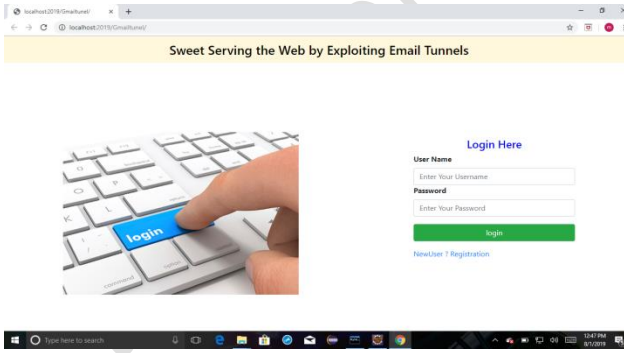

Fig:-3 Login

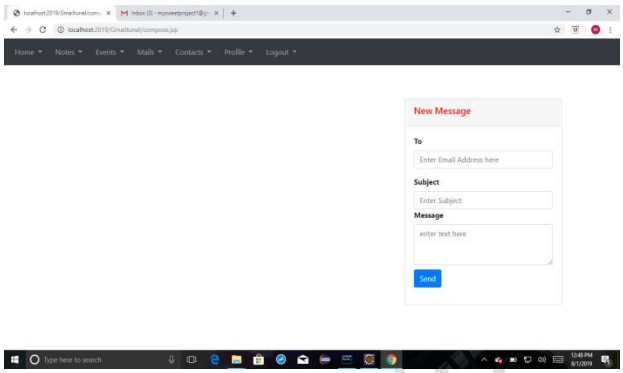

Fig:-4 Email sending

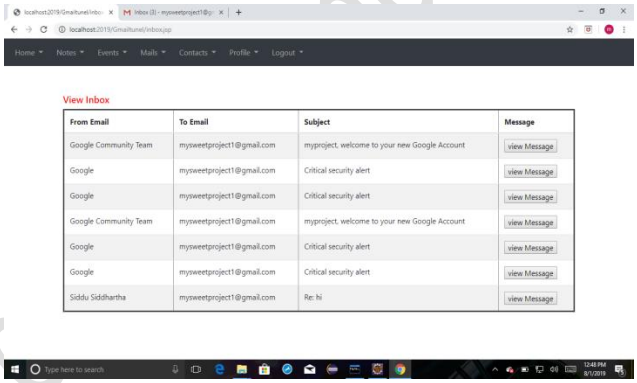

Fig:-5 Email inbox

5. CONCLUSION

In our current generation, we are using email services in official, professional, financial communication systems. In the email system we also required some third party protocol to send the email from a machine due to bulk emails like salary statements, announcement etc. By providing third party services to send email in bulk by the providers specially like Gmail, Yahoo By taking these problems in this paper, we proposing monitor of email by using the CIRCUMVENTION, a specifically to be had censorship-resistant infrastructure. Our system we checked the each and every email

sending transaction through our server and verify the sender details and deliver to the user by using proxy server. We demonstrated our model by using of the web application. We got the expected and best results by comparing with literature.

6. REFERENCES

[1] J. Zittrain and B. Edelman, "Internet filtering in China," *IEEE InternetComput.*, vol. 7, no. 2, pp. 70–77, Mar. 2003.

[2] (Nov. 2007). *Defeat Internet Censorship: Overview ofAdvanced Technologies and Products*. [Online]. Available: http://www.internetfreedom.org/archive/DefeatInternet Censorship WhitePaper.pd

[3] C. S. Leberknight, M. Chiang, H. V. Poor, and F. Wong.(2010).*A Taxonomy of Internet Censorship and Anti-Censorship*.[Online].Available: http://www.princeton.edu/ chiangm/anticensorship.pdf

[4] I. Clarke, S. G. Miller, T. W. Hong, O. Sandberg, and B. Wiley,"Protecting free expression online with freenet," *IEEE Internet Comput.*,vol. 6, no. 1, pp. 40–49, Jan. 2002.

[5] *Ultrasurf*, accessed on Jan. 7, 2017. [Online]. Available:https://ultrasurf.us/

[6] J. Jia and P. Smith. (2004). *Psiphon: Analysis and Estimation*.[Online]. Available: http://www.cdf.toronto.edu/ csc494h/reports/2004-fall/psiphon_ae.html

[7] I. Cooper and J. Dilley, "Known HTTP proxy/caching problems," IETF,Fremont, CA, USA, Tech. Rep. Internet RFC 3143, Jun. 2001.

[8] R. Dingledine, N. Mathewson, and P. Syverson, "Tor: The secondgenerationonion router," in *Proc. USENIX Secur. Symp.*, 2004,pp. 21–37.

[9] J. Boyan, "The anonymizer: Protecting user privacy on the Web,"*Comput.-Mediated Commun. Mag.*, vol. 4, no. 9, pp. 1–6, Sep. 1997.

[10] *DynaWeb*, accessed on Jan. 7, 2017. [Online]. Available:http://www.dongtaiwang.com/home_en.php