S-WET: Secured Web Email Tunneling (S-WET)

T. Dhanalakshmi
Student: Computer Science
Sree Sakthi Engineering College
Coimbatore, India

R. VIjai
Student: Computer Science
Sree Sakthi Engineering College
Coimbatore, India

S. Kiran
Student: Computer Science
Sree Sakthi Engineering College
Coimbatore, India

Mrs. Biruntha
Assistant Professor: Computer Science
Sree Sakthi Engineering College
Coimbatore, India

***Abstract*— An Internet is a standard communication between number of peers or system that used to share the information, news and managing the phenomenon's, Under the control of using various technologies, from IP address blocking and domain name seizing and Deep Packet Inspection (DPI).To improve the resource demand, we propose Secured Web Email Tunneling, in this user's signals hidden by sharing secrets in priory and adjustment to the Internet. To use this application for progressing ,a client necessary to have a public email account also needs to know about S-WET's application. And area coverage is increased by including special techniques for send and receives email between peers. First method is AlienMail server which is in an encrypted format. Another one is DomesticMail to hide the enclosed contents through steganography technique. Domestic method is improved by adding own domain address and the intrusion is reduced.**

***Index Terms*— Email Communications, Signal Encapsulation.**

I. INTRODUCTION

The Internet is used to share news and information, diverges and manages the events and challenges. Open communications on the Internet cause injurious to the users. Network can be used to interconnect multiple private networks with addition of security techniques, In spite of that hazards can take place to affect the network systems. For Email threatening is serious issue now a day's such as phishing, spam, content hijacking, Domain address breaching etc. As a result, these kinds of activities are monitoring the citizens' access to the Internet with the use of modern technologies, a different type of systems were developed to maintain the frankness for the users living under repressive so for to improve the reliability of the DNS security, We implement Secured Web Email Tunneling (S-WET), in which is highly obtainable resistant infrastructure.

The earliest tools are such as HTTP proxies that simply manipulate a client's HTTP requests with DNS hijacking techniques. Even though the most effective systems or technologies are applied, the use of HTTP proxies can arise the defects to the users. This led to the advent of more advanced tools such as **GTunnel** and **GPASS** which is a Windows application that works as a local HTTP or SOCKS proxy server While these circumvention tools have helped, they face several challenges. Due to the lack of *availability*, censor can disrupt their service frequently the reason is that

Traffic in a network made by these systems can be distinguished from regular Internet traffic by censors.

In general the popular Tor network works by having users connect to an ensemble of nodes with public IP addresses, which proxy users' traffic to the requested, censored destinations. To improve availability, censors by pre-sharing secrets with their clients .To conceal building by making infrastructure modifications to the Internet.

Internet security is widespread objective and issues in a current world. It causes serious issues to the data, information and personal. To conceal the problems security that word is often applied everywhere. The current remedy and precaution is focused on protection against serious threats as much on real time .These activities are actually get places on network, data, systems and etc. And issues are directly involved by malicious software like Key logger, Trojan, spyware etc. Also it can be done just send a code that contains worms and viruses to create an impact on the target. Application is used to obtain the security vulnerabilities or authentication checks.

The mail message protocols that are includes SSL and succeeded by transport security .The mail process that is initialized by composition and followed by deliver and store .After the mail transmission , the client connects to a mail transfer agent in which is also named as mail user agent .The client agent that provide the identity of the receiver to the server by using the mail server commands .The connection establishment is provided for supplying the messages .The server and client in a mutual connection until the end of a transmission .The mail message's data files to be stored using encryption algorithm.

However, it is secured technologies, those systems are breakable. Since current protocol imitations are inefficient in various places. An attacks like DOS are extracted to make the resource unavailable .The efficient efforts is used to prevent the internet sites or service To overcome those kinds of problems, we implement secured tunneling between end users. In this paper, we find better way to hide

the content in genuine manner. We design and implement S-WET, that provides protective email communications. Fig. 1 shows the Basic Architecture of S-WET. An S-WET client, narrow by a censoring ISP and its traffic is carried over a public email server to make a series of email messages that are exchanged.

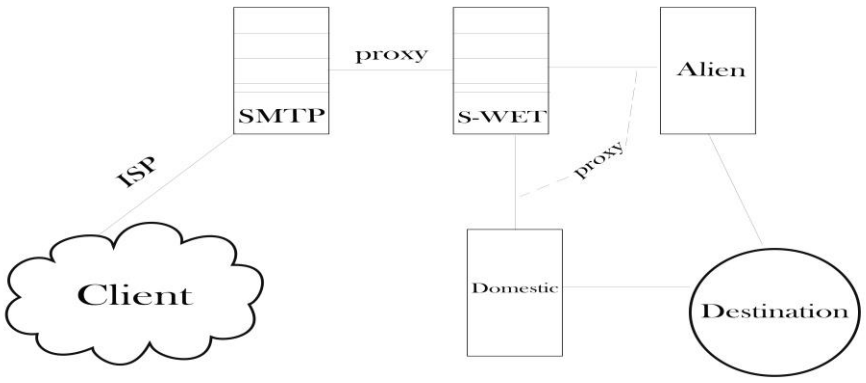

Fig. 1. Basic Architecture of S-WET.

In above figure, Client send a secured mail over the internet by using exploiting email tunnels. To use this application, end user must have public email account for progress. Two options are available to send and receive a mail *(i.e) AlienMail* and *DomesticMail.* We implement this technique, censors will not be able to obtain the mails in between since it's proxied. The Destination will receive the encrypted and hidden mail with notification about the source.

We implement this process by using *W3* recommendations for wide area communications. The area coverage is extended by W3 which are considered the web standards. To provide the secured communications between peers and SWET server to destination, Secured Socket Layer (SSL) certification is applied in which is also referred as transport Layer Security (TLS).It establish the secure connection over the network.

1) *AlienMail* a non-domestic email that encrypts emails (e.g., Gmail for users in China), and 2) *DomesticMail* a domestic email account. As described in above Section, when AlienMail is used by a client all of its S-WET emails are sent to a landing place in an encrypted format; a censor will not be able to identify these emails since they are *proxied* by the AlienMail server. In a use of tis application, intruder cannot observe the recipient's mail even though they can obtain the sender's place. The Alien Mail can obtain the messages and formatted to encrypted type. For example, original mail address is *swet@gmail.com* and while using Alien method, it will be translated in the form of encryption. And this encryption is done by the use of Triple Data encryption Standard (3DES).To notify the authorized sender, alert message will be sent to the recipient.

In the case of Domestic Mail, end user necessary to create a confidential secondary mail address. To obtain and utilize the Domestic purpose, a custom mail id is required. From the above example *swet@gmail.com* is additionally need an another mail like *123@abc.com* .The primary address is actually overlapped by secondary mail in which is referred as text hiding in Steganography. Censors cannot be able to grass the address since the Domestic method uses own domain name. The secondary mail address is carried over by the primary address. The top level mechanism are used to provide

the domestic and non-domestic access to all the end users but now a days the openness to the people as well as to the users cause impacts such as dangerous discussion on knowledge, data authentication, illegal activities on personal information

etc. Client required to connect with the server through the internet service provider (ISP) to the public mail server and the proxied communication is established between the S-WET server and public mail authorizer .Then from the S-WET server it will be separated as two different modes such as Alien and Domestic .As per the user selection message will be passed under the two existing modes .The destination is confirmed by the SSL to ensure the original sender's address.

Prototype implementation: To validate and evaluate the S-WET server, we implement prototypes for performance measuring. . At the client side email communication is done by protocols such as POP3 and SMTP as usual to the server. For sending a mail, interface is used (i.e) S-WET application is installed which is carried over through the internet via server.

By the Simple Mail Transfer Protocol (SMTP) in which is standard prototype for electronic transmissions .In general, SMTP is used as mail agent for sending a mail messages from the client. To receive the mail message at recipient side Post Office Protocol (POP3) is used in which is referred as application layer protocol to retrieve from a remote server over a TCP/IP connection .We propose an infrastructure by scaling the components for both method. Server that provide a virtual tunneling between peers for mail management.

Mail that is processed by a server based on request and response When the request is knocking the server it will send to the message queue if server is busy and it will wait for some time in the queue until the server become ideal .Once the server is free message in a queue will be responsed based on priority in which is finished in short amount of time. The virtual server that store the particulars of the mail messages.

We described the architectures and its related work about Alien Mail and Domestic Mail in extended pages. The work contains the number of components, process of components and place of components. To compare Alien and Domestic mails, Domestic is preferred or recommended since its own and custom domain name address in which is not censored by the circumvention. Alien mail that convert the mail in an encryption format and alert message will be sent separately because of this separation user should have aware about the message content and its notification. And notification will be sent to the target with domain address in which contains the originality. Finally it can be reached to the destination via internet service with returned ip address.

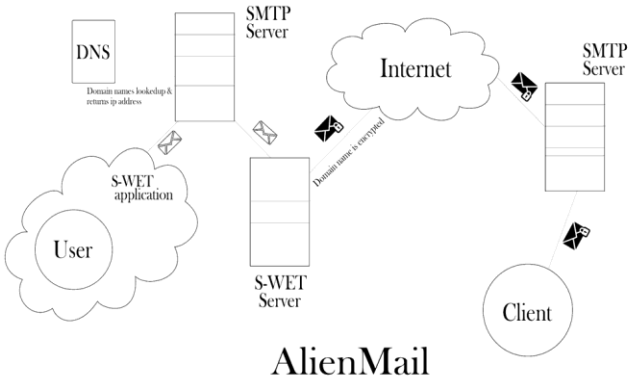

Fig.2.S-WET Architecture for AlienMail

DESIGN OF ALIENMAIL

In this proposed work, we have two methods Alien and Domestic in which are used to protect the peer communication .The above architecture referred to Alien process with the surveillance of S-WET server. This can be achieved by encrypting the domain address.

The encryption was done by applying Triple DES (3DES) where the process is done by private key ciphering algorithm. It applies the cipher mode in each block for three times .The simple DES has carry 56 bits for each blocks which is sufficient for simple computational mode .But it can be vulnerable for Brute force attack .Since it is feasible for that attack, the number of bits in a key is increased to protect against attacks where the structure is transferred into new block cipher algorithm.it encrypt with short length of two key bits for blocks instead of one .It would be vulnerable for meet in the middle attack .Therefore,3DES uses a key pairs with 56 bits in three times without considering the parity bits .All three keys are independent .It encrypt the messages with three keys (i.e) Encrypt-Decrypt-Encrypt for encoding at sender side. The reverse process of encoding will be applied in recipients side (I.e) Decrypt-Encrypt-Decrypt .Each triple encoding encodes the message one block of 64 bits of data .This #DES is used to regulate the encryption process .The 8 bits is used for parity control to ensure the proper transmission.

The architecture that contains application user and end peer for communicating through the message via internet the S-WET user need to login with their credential if they are already authorized by the server. In case for guest users, necessary to register with their details such as mail and password .After the creation and authorization, user can be logged into a S-WET application to send and receive the mail from or to peers .The process of Alien Mail includes message passing from user to public mail provider .The message is transferred to DNS to ensure and return the IP address where the DNS locate the destination address from the database. If it's not present then it tries another database to achieve the work .The SMTP server that transfer the message to the neighborhood servers until it reach the destination .The Alien Mail provide the highly secured communication between among the users because it shows only the unreadable format address instead of original domain name .User can know the original address only if user received the notification .Until they won't predict the sender's details.

From this work, the remaining method in which provide the high availability to the end user via overlapping technique which is named as Domestic Mail. The structure of a Domestic mode will be exposed in Figure 3.

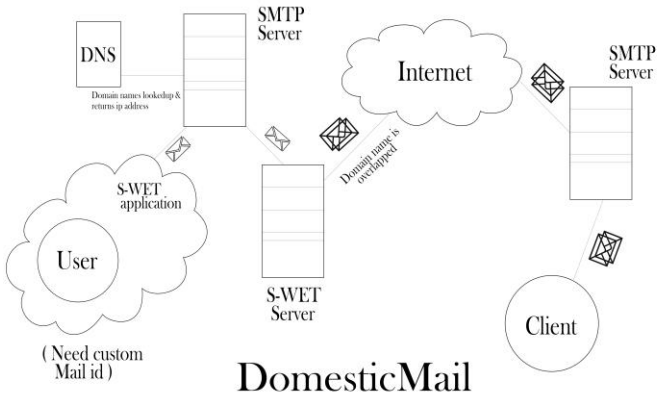

Fig.3.S-WET Architecture for DomesticMail

DESIGN OF DOMESTICMAIL

In this section, we implemented the Domestic mail method in which is used to communicate with the user via internet in secured manner. Domestic mode that contains the technique is text hiding in Steganography .The process of text hiding is overlapping the secondary mail address with original mail id. The mail that hidden over the domain address to establish the peer security. Steganography is a method that used to hide the information or message .It conceal the original message that is invisible to the unauthorized person while it's traveling on the internet. The domestic is mail exchanged only between the particular clients that is to the authorized users. The process of a message conceal provide high security to the persons to share their communications. In early systems, the intrusion is mostly taken places in mail or messages. To overcome those types of problems network security or internet layer

security was implemented but due to irregularity or poor connection it will be attacked by the third parties without the knowledge of system owner. Even though the now a days public mail providers provide the encryption, digital signature, certificate authority (CA) among the messages in mail services, it is not completely secured due to lack of time and distance. Also it is only conceal the message s inside the mail service in which can be accessed and attacked very easily and quickly. The unauthorized access is done on mail's domain name or address to know the original information about sender and receiver. However it is happening some technologies that not applicable for all access over the mail services such as S-WET server where the domain name and address is encrypted and concealed by applying two techniques Alien and Domestic modes. In Domestic, mail is completely hidden to the third parties since it under the control of text hiding in Steganography. S-WET server helps to protect the mail services as well as to avoid the domain address access without knowing of owner is avoided. It can be used in wide are by w3 recommendation's with the security policy in which is called SSL between the end peers .The MySQL database is used for both Alien and Domestic mail methods for storing and retrieving the details about registered and logged users while they are using S-WET application. The encryption and its reverse conversion will be stored and retrieved in database to provide the high security in mail service. From the two methods Alien and Domestic, high security guarantee is provided to the user. To ensure and improve the reliability users are recommended to use the Domestic mail to send their communication or messages to the recipient. Because Domestic is flexible and provide the customization to the users by adding the secondary mail address field form client.

The end users are required to aware about the S-WET application and its modules which is registration, logging and mail service where the two methods are implemented. The mail service provide the modes for users as per their selection while entering their details in application. The S-WET application is used the database for storing the mail of the clients when they are register with their public mails. This application is completely base on windows operating system where the layer communication is smooth and ecofriendly to the users and platform. The S-WET application provide the session expiry to ensure and provide the reliability to the end users (i.e) if the user forgot to logout their account in the systems or browsers, it will be automatically logout from the browser or system which is based on cookies. The cookie is set for reliability insurance and period limitation was set and done in the application. The cookie time is customizable and allow to modify the period limitation if the users is authorized by the application and server owner as well by the server.

From the above structure and its definition, S-WET that guarantee the secure communication among the mail users and assure the reliability.

COCLUSION

This is a secured communication among the multiple users over the internet .The mail service is ensured that high availability and provide the reliability to the end users. The new way of encrypting and hiding the domain address

Provide the surety of safe mail communication and intrusion can be reduced since intruder doesn't judge the source detail. This is applicable for wide area exchange of messages without lacking of time and latency in communication. The overhead of servers are reduced .The mail system that simplifying the deployment .The use of 3DES has taken quite high peek memory space while since it has been triple cycled for encryption. Through this implementations simplified deployment and wide area access is extended.

REFERENCES

[1] C. S. Leberknight, M. Chiang, H. V. Poor, and F. Wong. (2010). A Taxonomy of Internet Censorship and Anti-Censorship.

[2] Ruthfield, Scott. "The Internet's History and Development: From Wartime Tool to the Fish-Cam", September 1995.

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

[4] S. Burnett, N. Feamster, and S. Vempala, "Chipping away at censorship firewalls with user-generated content," in Proc. USENIX Secur. Symp., 2010, pp. 463–468.

[5] Michael J. Freedman and Robert Morris.Tarzan:A peer-to-peer anonymizing network layer.In Proceedings of the 9th ACM Conference on Computer and Communications Security, Washington, D.C., November 2002.