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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

ENHANCED EMAIL DISPERSION ENFORCE USING MAIL SERVER

Sumathi Sivaraj[1], L.Dhanam[2], Yasotha Mohankumar[3], M.S.Vinu[4]

M.E Computer Science and Engineering, Sri Eshwar College of Engineering, Anna University, India[1,2]

M.E., (Ph.D.) Assistant professor, Sri Eshwar College of Engineering, India[3]

M.E., Assistant professor, Sri Eshwar College of Engineering, India[4]

Abstract: E-Mail service details with the web site that manages the electronic way of communication. Through this paper, we will produce our own domain, user id, sends mails to any user and manage inbox, folder lock options within E-mail and Set permissions for employer ids under a private concern (or domain). DNS is a relatively simple, text-based protocol, within which one or a lot of recipients of a message are specified along with the message text and possibly other encoded objects. The information message is then transferred to a remote server using a procedure of queries and responses between the client and server. An email client knows the outgoing mail SMTP server from its configuration. A relaying server usually determines which SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name (the part of the email address to the right of the at (@) sign).The DNS client initiates a TCP connection to server's port 25 (unless overridden by configuration). DNS is a "push" protocol that does not allow one to "pull" messages from a remote server on demand. The core module of our project is to provide an efficient way of Intrusion Detection using Trust + Awareness methodology by which if any intruder attempts in accessing a client's account, the owner will be notified of it at his next successful login session with details of Attack time, Attack Date, Attacker's IP address, Attacker's guess at the wrong password.

Keywords: Mail Exchange; E-Mail; Mail Server; IP address; TCP connection

I. INTRODUCTION

The communication across the world is must in the modern age communications through postal may take longer. It's going to be days or weeks to form the message available to others. E-Mail service details with the web site that manage the electronic way of communication. Through this project we can create our own user id, sends mails to other user and manage inbox. In addition greetings can be sending to friends. We can view incoming mails and greetings and even delete them. Resume will be keeping and adjusted whenever necessary. Any mail connected report will be viewed through the positioning. Deletion of unwanted mails will be created to manage memory. This is one of the problem in the existing system is said as detecting denial of service attacks.

DNS is a relatively simple, text-based protocol, in which one or more recipients of a message are specified along with the message text and possibly
Other encoded objects. The message is then moved to a remote server using a procedure of queries and responses between the client and server. Either an end-user's email client provided. MUA (Mail User Agent), or a relaying server's MTA (Mail Transport Agents) can act as an SMTP client. This design can also can be implemented in wireless sensor networks. An email client knows the outgoing mail SMTP server from its configuration. A relaying server generally determines
That SMTP server to connect to by looking up the MX (Mail eXchange) DNS record for each recipient's domain name (the part of the email address to the right of the at (@) sign). Conformant MTAs (not all) fall back to a simple A record in the case of no MX. Some current mail transfer agents also will use SRV records, a lot of general style of Maxwell, although these are not widely adopted.

The DNS client initiates a TCP connection to server's port 25. It's quite terribly straightforward to envision associate degree SMTP server using the telnet program. DNS could be a "push" protocol that doesn't enable one to "pull" messages from a remote server on demand.
There are two main components available in this thesis trust and aware routing, So that according to the procedure trust is implemented for user rights, in order to provide a user authentication mode. These authentication modes are in the customized format in order to provide rights to the appropriate users from the admin side. In added with aware routing is working under the principle of IDS (Intrusion detection system) which detects the third part authorization, hackers, attackers and data privacy with their corresponding IP address with their date and time.

II. OBJECTIVE

The main objective of this project is to develop a trust aware routing environment using SMTP server. Here an email environment is developed for a organization, trust is implemented for user rights as well as aware routing is

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

implemented for security purpose. For special security purpose here we introducing a latest method called as IDS (Intrusion detection system), which identified the third party intruder or hacker from other networks. The basic IDS can able capture the IP details; here we using an advanced IDS method which can capture IP address of the hacker, data, time and the password which he try to hack. In added with the trust method will provide the user rights within the organization.

MESSAGE ARCHITECTURE

E-MAIL SERVER consists of core modules

- Folder Lock
- Intruder list
- IP Address tracker

COMPONENTS

1. Company Creation using DNS
2. User Creation for DNS
3. User Rights for trust
4. Intruder list for Awareness Routing using IDS

Company Creation

This is the entry level module which consists of entering username, password and other basic details to create a company, this module is only enabled for admin those who creates the company. While creating company all the basic company details should be entered with the password for creating a company, so that the admin can able to log in to the user creation wizard. This is the basic work for creating a basic SMTP environment as well as the further process. A server id and a DNS name will be created here for company authorization.

User Creation

Using the DNS company users can be created. Each user will get their ids with the company domain name. Here the admin can create various users for their company, as well as they can able to share the group mails inside the group of companies. These mails will not be stored in the junk mails, because these all are confidential mails inside their companies. It might be a pdf file, doc file or image file.

User Rights

According to the trust procedure user can not able access any options like compose mail, inbox, sent items and etc. After creating the user admin should give the right for their ids according to their role of work inside the company. This is because programmer or document handler could not able to access or send the file to anyone. Admin wants to create the right for the users according to their role. The right can be updated according to their trust level.

Intruder list

Hacker list is the instruction detection method, which helps the user to find out the other users entering into the network. It contains a IP tracker, password checker, date of attack and time of hacking. So the customer can identify who is the other user intruding into the network. So that user can identify the hackers easily through their IP address.

MAIL PROCESSING MODEL

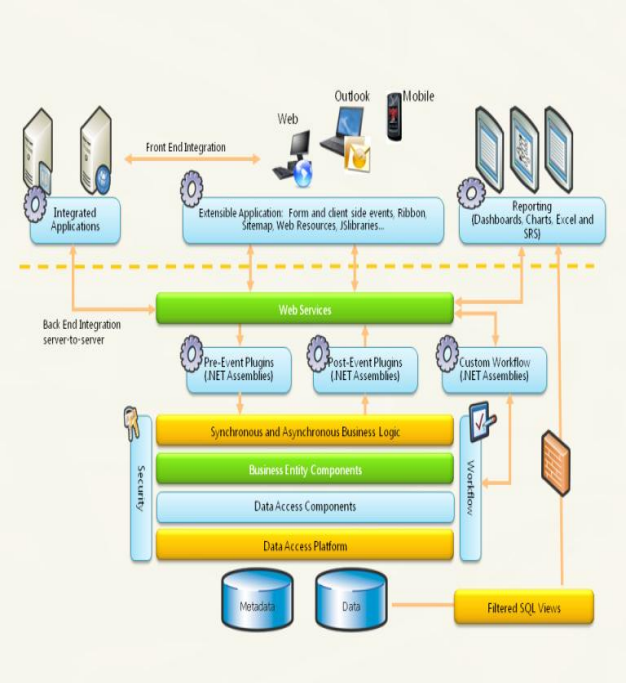

Figure 1.1 Mail Processing Model

III. EXISTING SYSTEM

The Existing System lags behind in following aspects that have been included in our proposed system,

- No IDS to detect Intruders
- No IP Tracker Facility
- No Intruder List, Password Combination used by Intruders, Date of Attack, Time of Attack provided
- No Customized E-Mail Web Service Management
- **No ways to ensure Data Security – Folder Lock**

The existing system introduces a trust model for mobile ad hoc networks. Initially each node is assigned a trust level. Then we use several approaches to dynamically update trust levels by using reports from threat detection tools, such as intrusion detection systems (IDS), located on all nodes in the network.

The nodes neighboring to a node exhibiting suspicious behavior initiate trust reports. These trust reports square measure propagated through the network using one of our proposed ways. A supply node will use the trust levels it establishes for other nodes to evaluate the security of routes to destination nodes. Mistreatment these trust levels as a guide, the supply node will then choose a route that meets the security requirements of the message to be transmitted. This paper demonstrates vital ideas for

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

establishing a collaborative, dynamic trust model and for victimization this model as an example to enhance the security of message routing in mobile ad hoc networks.

IV. PROPOSED SYSTEM

- Advanced DNS /POP3 Email Server with tons of features, such mailing lists, multiple DNS gateways, security, and compatibility with any email program. Are often used an obsessive mail server, or as a personal local SMTP server.
- A free DNS relay server. Allows relay emails sent thereto, on to their destination, bypassing your provider's email server. If you wish to send massive quantities of email, created a number of of those servers on completely different computers.
- DNS server program to send email messages without help of your ISP, directly from your local PC to recipient mailboxes and use your favorite email client along with this software the way you used to do it before.
- DNS relay software allows putting emails directly to receiver mailbox. This is much faster and reliable than using DNS server provided by your ISP. Remailer. Powerful direct remailer set of project act as DNS relay.

Core Modules in our Proposal System are as follows

- IDS to detect Intruders
- IP Tracker Facility
- Intruder List, Password Combination used by Intruders, Date of Attack, Time of Attack provided
- Customized E-Mail Web Service Management
- ways to ensure Data Security – Folder Lock

V. IMPLEMENTATION

Implementation is the stage in this paper where the theoretical design is turned into a working system. The foremost crucial stage is achieving a prospering new system & giving the user confidence in that the new system will work efficiently & effectively in the implementation state.

The stage consists of

- Testing the developed program with simple data.
- Detection's and correction of error.
- Creating whether the system meets user requirements.
- Testing whether the system.
- Making necessary changes as desired by the user.
- Training user personnel.

VI. CONCLUSION

It is concluded that the application works well and satisfy the users. The application software is tested alright and errors are properly debugged. The positioning is at the same time accessed from more than one system. Synchronic login from quite one place is tested. The site works according to the restrictions provided in their respective browsers. Further enhancements can be made to the application, in order that the net web site functions terribly engaging and useful manner than the present one. The speed of the transactions become more enough now.

VII. SCOPE FOR FUTURE DEVELOPMENT

Every application has its own merits and demerits. The thesis has covered almost all the requirements. Any necessities and enhancements will easily be done since the coding is mainly structured or modular in nature. Dynamical the prevailing modules or adding new modules can append improvements. Further additional enhancements are created to the application, in order that the online web site functions very attractive and useful manner than the present one.

REFERENCES

[1] Andrew Stellman 'Head First C#', 2nd Edition, O'Reilly Media Incorporated.
[2] Banff, Alberta, Canada (2004) 'International conference on Machine learning table of contents', page 46, Learning (IDEAL04), UK.
[3] Brian Nolan (2004); GIAC Security Essentials Certification 'Identity Theft Attacks & Countermeasure
[4] David Flanagan (1997) 'Java in a Nutshell' , 2nd Edition, May.
[5] Guoxing Zhan, Weisong shi, Julia Deng (2010) 'TARF : A Trust-Aware Routing Framework for wireless sensor Networks.
[6] Herbert Schildt (2010) 'C# 4.0 The Complete reference' , Tata McGraw-Hill publishing Company Limited.
[7] Michael Walfish, Hari balakrishnan, Scott Shenker (2004) 'Untangling the Web from DNS.
[8] Miles Tracy, Wayne Jansen, Karen Scarfone, Jason Butterfield (2007) ' Recommendations of national Institute of Standards and Technology – Guidelines on Electronic mail Security.
[9] Patrick Naughton, Herbert Schildt, 'Java™ 2: The Complete Reference', Third Edition, Tata McGraw Hill Publishing Company Limited.
[10] Theodore Zahariadis, Helen Leligou,Panagiotis karkazis, Panagiotis Trakadas, Ioannis Papaefstathiou, Charalambos Vangelatos, Lionel Besson (2010) 'Design and Implementation Of A Trust-Aware Routing Protocol For Large WANs.
[11] Vladimir V.Riabov ; Rivier College (2005) ' SMTP (Simple Mail Transfer Protocol)'.

BIOGRAPHY

S. SUMATHI received her MCA Degree from Bharathiyar University Coimbatore, Tamilnadu, India and pursuing M.E (Computer Science and Engineering) degree from Sri Eshwar College of Engineering Coimbatore, India. Her area of interest is Network security and Cloud Computing.

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 1, January 2014

S.YASOTHA obtained her B.E (Computer Hardware and Software engineering) from Avinashilingam University for Women, Coimbatore (Tamilnadu, India) and received her M.E (Faculty of Information and Communication Engineering in VLSI Design) from Anna University of Technology, Coimbatore. She is pursuing Ph.D (Information and Communication Engineering in ECE Department). She is currently serving as Assistant professor of Computer Science and Engineering at Sri Eshwar college of Engineering, Coimbatore (Tamilnadu,

L.DHANAM received her B.E(CSE) Degree from Hindusthan college of Engineering and Technology, Coimbatore, Tamilnadu, India and pursuing M.E (CSE) Degree from Sri Eshwar College of Engineering, Coimbatore, India. Her field of Interest is Network security, Operating system and Theory of Computation.

M.S.VINU has obtained her Post Graduate degree, M.E.(Computer Science and Engineering) in Nandha College of Engineering, Erode and obtained her Graduate degree B.E., (Computer Science and Engineering) from VSB College of Engineering, Karur. She is currently serving as Assistant Professor of Department of Computer Science and Engineering at Sri Eshwar College of Engineering, Coimbatore, Tamil Nadu with a teaching experience of 2 years. She is specializing in the area of Network Security. India). Her area is Network Security and Wireless Sensor Network.