

Authentication and Curbing Based On Exaction by IMAP

D. Padma

M.Tech(CSE),

Vignan's Institute of Information Technology, Visakhapatnam.

Abstract

Managing network is a task where network traffic, security, authentication for users is a basic functionality. Administering networks cause problems of which main one is accidental failure. In this paper a new approach has been adopted in such a way that, the information on network status is gathered by an application, using Internet Message Access Protocol (commonly known as IMAP or IMAP4, and previously called Internet Mail Access Protocol, that allows a local client to access e-mail on a remote server. It will send the Server Information to network administrator by email and also it sends message to the administrator when unauthenticated user uses the confidential files. This approach also will allow network administrator to apply all necessary commands, using message. IMAP is used instead of SNMP because it provides detailed information and strong security i.e. IMAP does not allow unauthorized users to access the important data.

Keywords-*IMAP ,Modem, AT Commands, Email.*

1. Introduction

Data communication and computer networking facilities are increasing day by day. Due to this , problems relating to network administration are also increasing. Physical presence of network administrator or remote access via Internet are identified as common solution to this problem. In this approach the network administrator will investigate all aspects of network operation and under his access privilege intervene and apply necessary commands using IMAP. SNMP is not used because it is a simple protocol it does not provide enough

information to the administrator,exchanges are unacknowledged the management agent receives no confirmation that communications have successfully reached or not,and poor security is provided such that unauthorized users may access the data etc where as IMAP , It is an interactive client-server model such that there is no loss of data during communication. It provides detailed or enough information to the administrator, Allows message access and management from more than one computer and strong security is provided by not allowing unauthorized users to access .

In this paper a new approach to network administrator has been adopted which uses the IMAP protocol. In order to communicate, an application is installed on a system which has access to the network under administration.Upon the administrator request, all necessary information will be gathered by this application, using IMAP protocol and then is sent to the administrator via mail. In turn the administrator issues commands with certain format applicable to the mail, to the same application. At this stage the application with the collaboration of IMAP[1], the issued command will be applied to the target device.

2. Internet Message Access Protocol

IMAP Stands for "Internet Message Access Protocol" and is pronounced "eye-map." It is a method of accessing e-mail messages on a server without having to download them to your local hard drive. The advantage of using an IMAP mail server is that users can check their mail from multiple computers and always see the same messages. This is because the messages stay on the server until the user chooses to download them to his or her local drive. Most webmail systems are IMAP based, which allows

people to access to both their sent and received messages no matter what computer they use to check their mail.

2.1 Operations And States Of Imap Protocol

IMAP includes operations like creating, deleting, and renaming mailboxes, checking for new messages, permanently removing messages, setting and clearing flags, RFC 2822 and RFC 2045 parsing, searching, and selective fetching of message attributes, texts, and portions thereof. The IMAP connection will be in one of the following states:

Connection Established - we have a valid socket but no data has been exchanged yet, waiting for Server

Greeting Server Greeting - server has sent an initial greeting, for some servers this may take a few seconds.

Not Authenticated - server is waiting for client response, and the client has not yet been authenticated

Authenticated - server is waiting on client but we have valid authentication credentials, for PREAUTH state this may happen immediately after

Server Greeting-Selected - mailbox has been selected and we have valid context for commands

Logout - logout request has been issued, waiting for server response

Connection Closed - connection has been closed on both sides

2.2 Message State Information

The IMAP protocol, clients can keep track of message state: for example, whether or not the message has been read, replied to, or deleted. These flags are stored on the server, so different clients accessing the same mailbox at different times can detect state changes made by other clients.

3. To Send & Receive Messages From workstation

A GSM modem is required to send and receive email from work station[5]. In order to use modem, the workstation must use AT commands. For a limited network, the modem is placed with mobile phone

with USB port. When a mobile is connected to a workstation, first its driver must be installed, the driver acts as mediator to facilitate compatibility of applied commands to the hardware which is under use. In order to simplify AT commands and to avoid detail of coding messages, it uses libraries of email. The programmer can use these libraries to open port, for recognizing the devices that connected to workstation and to send/receive email.

4. Usage Of AT Commands

AT commands are instructions used to control a modem. AT is the abbreviation of Attention. .

Every command line starts with "AT" or "at". That's why modem commands are called AT commands. Starting AT is prefix that informs the modem about start of the line. It is not part of the AT command name. For example, D is the actual AT command name in ATD, and +CMGS is the actual AT command name in AT+CMGS. The general syntax of extended AT commands is straightforward. The syntax rules are provided below:
Syntax- all command lines must start with "AT" and end with a carriage return character. In a terminal program like the HyperTerminal of Microsoft Windows, you can press the Enter key on the keyboard to output a carriage return character[2].

4.1 List Of AT Commands

Some of the commands that are used to transmit are:

S.no	command	Description
1	+CMGS	To Send message
2	+CMGR	To Read message
3	+CMGL	To list message
4	+CMMI	Indicates new message
5	+CMGD	To delete message
6	+CMGW	To write into memory
7	+CMMS	To send more messages
8	+CMMA	To Acknowledge new message
9	+CMSS	To send message from memory

5. Proposed System

In proposed system network devices transmit warnings and messages to the network administrator using IMAP protocol. Network administrator receives warnings and messages, he sends email by applying a command to a specific device on the network. The network administrator logs the status of any individual device by email[5].

Upon a successful connection to a remote IMAP server, client might choose to authenticate itself if the server has not already pre-authenticated it automatically under a particular user account. After that or in case the authentication is not required, the connection enters the authenticated state. In this phase, no mailbox is selected and only a subset of commands is valid. Clients can, for example, ask for listings of the mailbox tree, get quick information about number of mails in a particular mailbox or otherwise manage mailboxes as a whole. They have to, however, select a mailbox in order to do anything else, like retrieving mails or marking them as read. A mailbox can be opened as read-only or for both reading and writing, provided the authenticated user has sufficient privileges. Retrieving messages can be done in both modes, but write operations (like storing a new message to the mailbox or manipulating the message flags) require read write access. Changes to the number of messages in the mailbox are communicated mainly by two kinds of untagged replies, EXISTS and EXPUNGE. EXISTS reply is used to inform the client that new message was delivered, The EXPUNGE reply contains a sequence number of the message that has been permanently removed from the mailbox.

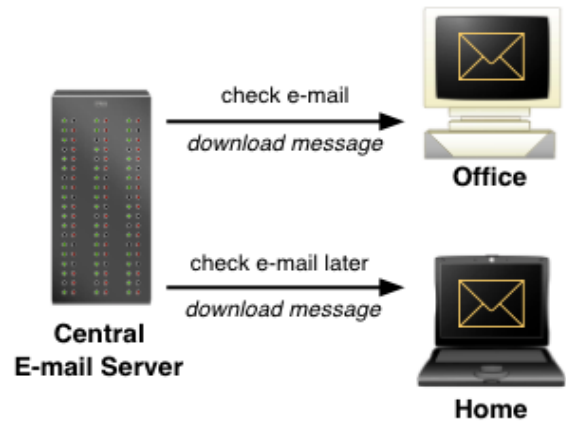


Figure 1: flow of data

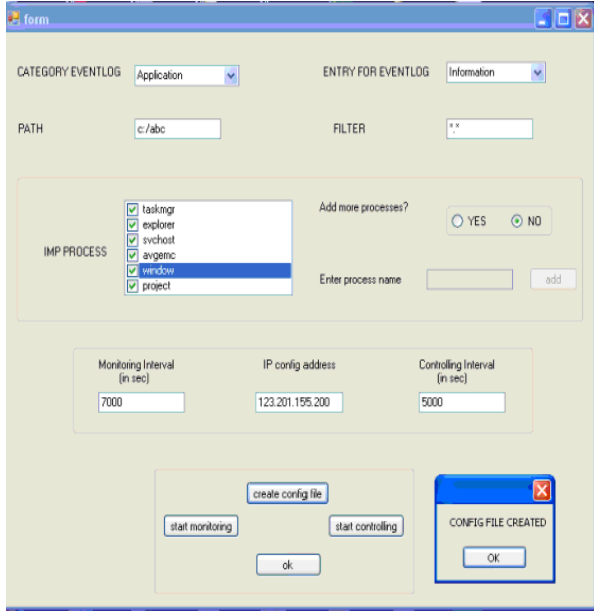
Figure 1 shows how the communication is done between the user and server using IMAP. An application which runs on the user system sends mail to the server. From here the data is sent to administrator. Administrator checks the data and sends response to the user, if there are any errors he corrects it by sending commands.

In this it consists of mainly three modules they are:

- A) Admin
- B) Monitoring
- C) controlling

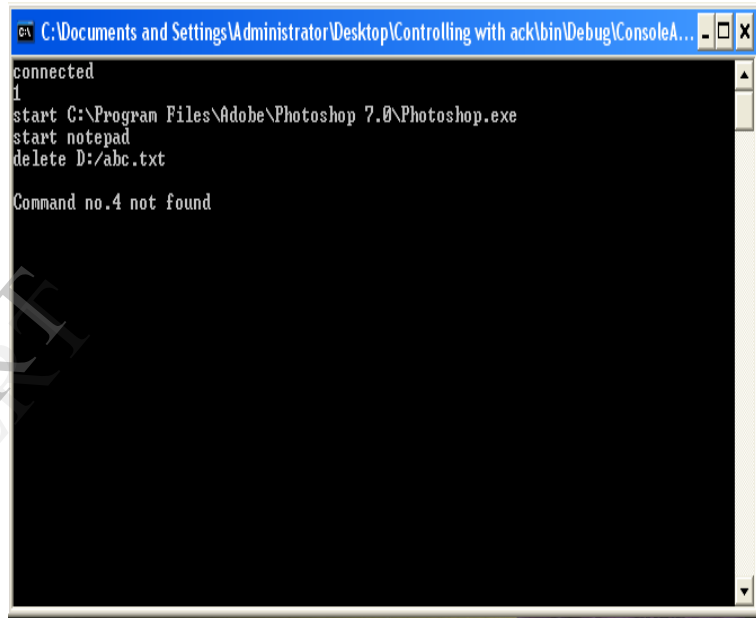
A . Admin :

In this administrator sets path, eventlog ,time, which process it has to provide security etc. create config file is used to create a config file, start monitoring is used to monitor the data if he wants to monitor then by simply clicking start monitor it monitors the data in the same way for controlling click on start controlling. In this it provides hole data that are to be fetched ,based on this data a log file is created which is used for monitoring.



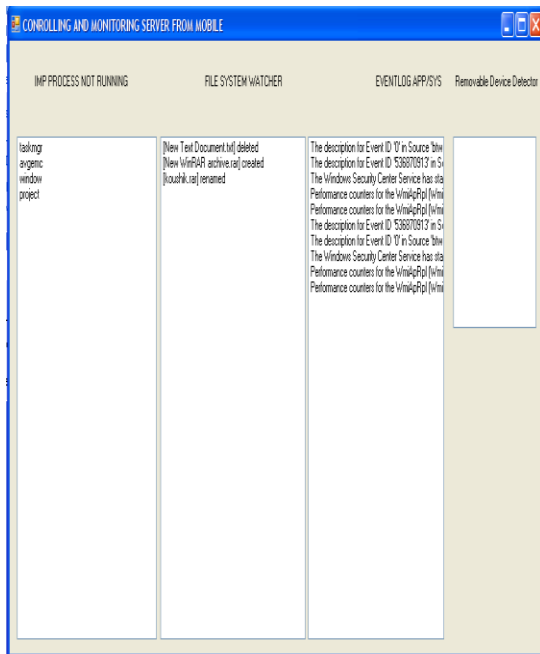
C . Controlling:

After clicking start controlling the following screen is displayed. It is used for controlling the data. This module fetches the mail from administrator, extracts the body part and stores it in a file. Then that command is executed after parsing the file. Administrator will send command as mail. This module will fetch the mail, and then execute the body part of the mail, if any syntax error in the command it will inform that command given is wrong.



B. Monitoring:

After clicking start monitoring the following screen is displayed. In this it gives information to the administrator that which process are not running, which files are modified, where an eventlog information is provided in order to detect errors.



6. Security Aspects Of Proposed System

The security aspects provided by the proposed system are:

- 1) *Confidentiality*: Prevention of database from unauthorized access is done by utilization of information hiding methods.
- 2) *Authentication*. The process of verifying that users are who they claim to be when logging onto a system. Generally, the use of user names and passwords accomplishes this.
- 3) *Access Level Security*: These days large scale networks can not be managed by one person and thus

each administrator has a limited domain of network control. The application program is capable of granting access right to each individual for only a specific domain of network. This provision of security grantee unauthorized access to different section of network is prohibited. The access right of network administrators can be redefined at any time if is required. The report generating capability of the application allows monitoring each administrator actions. For example it can be observed that what has been the response of an administrator to an event of network failure and what action has been taken on his part. To ensure the accuracy of reports, the events are time stamped and all messages are recorded in database.

4) *Availability*. The prevention of unauthorized withholding of information or resources. This does not apply just to personnel withholding information. Information should be as freely available as possible to authorized users.

7. Conclusion

In proposed system Authentication and Curbing Based On Exaction by IMAP, the main advantage is it allows message access and management from more than one computer and support concurrent access to shared mailboxes and provides strong security. In this work we have taken mail and integrated with advantages of IMAP protocol by creating a middleware, referred to it as application program. This system is capable of generating appropriate report on network status and transmits to the network administrators by mail. It is also able to apply any necessary command ,remotely by mobile phone, using mail to control and to take corrective action on any device within the network of under administration.

8. References

- [1] M.S.Crisipin “version2 of the protocol operations for the internet message access protocol(IMAP)”,RFC3501.
- [2] “AT COMMAND REFERENCE”,Gtran wirelessInc,Avalable
- [3] CryptoNET: Integrated Secure Workstation, Abdul Ghafoor Abbasi and Sead Muftic.
- [4] Traffic Analysis of a Short Message Service Network, Vikrant Tomar, Himanshu Asnani.J. Wang, “Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication),” *IEEE J. Quantum Electron.*, submitted for publication.
- [5] S.vogioukas, m.roumeliotis,”A system for basic level network fault management based on the GSMshort message service,IEEE international conference on communication,2001.
- [6] Abdul ghafoor abbasifor for “secure workstation”.
- [7] Rio de janeiro and Brazil,”A study of the short message service of a nationwide cellular network”,2006. crispin”message staff information of IMAP”,RFC1708.
- [8] crispin”message staff information of IMAP”,RFC1708.
- [9] Mobile control and management of computer networks using SMS services