Internet Mail Transfer and Check System Based on Intelligence Mobile Agents

LI Cheng
Network and Information Center of Shanghai Jiaotong University,
Huashan Road No. 1954, Shanghai China, 200030.
Tel: 86-021-62932919, Email: licheng@sjtu.edu.cn

WANG Weinong
Network and Information Center of Shanghai Jiaotong University,
Huashan Road No. 1954, Shanghai China, 200030.
Tel: 86-021-62932919, Email: wnwang@mail.sjtu.edu.cn

Abstract
The Simple Mail Transfer Protocol (SMTP) based E-mail system is the most popular application in today's Internet world, but there are many dark clouds at the edge of the sunny sky. The most well known two threats are the “mail SPAM” and the “mail flooding attack.” Mobile agents (MAs) are software agents that can transport themselves from a client computer to various servers for remote execution. Their mobility, autonomy and distributed intelligence are very friendly to today and tomorrow's Internet computation. In this paper, we introduce a prototype of the Internet mail transfer and check system based on intelligence mobile agents. This new system model can improve the current simple mail transfer protocol model to defend the mail SPAM and the mail flooding attack. Compatible with the traditionary SMTP is the most important feature of our new model. Finally, we summarize some difficulties for turning this prototype model into practical software.

Key words: Mobile Agents, SPAM, Mail Flooding

1: Introduction

Mobile agents (MAs) are software agents that can transport themselves from a client computer to various servers for remote execution. In contrast to remote procedure calls (RPCs), which are limited to communicating data to a procedure to be executed on a remote server, MAs transport both the data and programs. Dispatching a program for execution on a server has been around since the early 1960s. At that time, the motivation was due to the limitation of computing power of desktop CPUs.

This paper is divided into four sections. The following second part describes the working model and its familiar vulnerability of current E-mail system; The third part introduces the theory of our new model; The fourth part discusses some difficulties for take this model into practice.

2: Current Internet Mail System

Though the most popular mail system today is based on the SMTP (Simple Mail Transfer Protocol), there are some security problems about its working model. The most well-known two threats are the “mail SPAM” and the “mail flooding attack.”

3: Internet Mail Transfer and Check System Based on Intelligence Mobile Agents
The basic working protocol of our system is still the SMTP. We only do some modify at the MTAs and the working process as show in figure 1. The modify include the follow points:

- The SMTP-sender should provide a running environment for the MAs;
- The SMTP-receiver should prepare one or more lightweight MAs, and each of these agents should have different “Intelligence” or user-specified policy;
- Define a new SMTP verb “AGENT” that indicate the SMTP-receiver want to send an agent to the SMTP-sender.

![Figure 1: Mail System Model Based on Mobile Agent](image)

Each time when a MTA has some mails to transfer, it first setups a transmission channel between the target MTA and itself, just as same as the current mail system. Once the transmission channel has been established, the SMTP-sender sends a MAIL command indicating the sender of the mail. Now, the path will deviate. In our model, if the SMTP-receiver can accept mail it responds with an AGENT reply instead of an OK reply [2] and sends a mobile agent to the SMTP-sender. This agent will run to audit and filter all the mails, forwarding the “good” one to the SMTP-receiver and refusing the “bad” one.

It is very clear that the working model of our architecture is under the control of the MAs, actually the SMTP-receiver. The power of this model lies on that we can apply all the researching fruits of software engineer and artificial intelligence into the agent. Moreover, the agent can access all the content in the mails, checking, analyzing and filtering them before we get it. On the contrary, the traditional MTAs have little information about the mails until they actual receive the messages, which at the same time, the bandwidth and the money have already been spent.

In the above working procedure, if the SMTP-receiver replies the MAIL command with an OK, the system will work under the traditional procedure, so it is backward compatible.

4: Difficulties and Challenges

Though our new architecture seems better, we will encounter some difficulties to take this model into practice. The most famous two challenges are:

- Security: how can we protect the mobile agents and the host [4-7];
- Accounting method: how to bill the mobile agents for they running on other ISPs’ hosts.

5: Reference