Possible protection methods against DHA attacks by the attackers recognition and centralized ban

Introduction:

In result of growing number of uninvited mails,viruses spreading in mails and other malwares people tend to think it twice who they give their e-mails to. They have another think whether they should take the risk to use their e-mail on an online forum, or even to leave it on their own web page or calling card. Cause of the reasons above, the users usually keep an other one-time e-mail address, often at some free service provider, which in case of flooding of uninvited mails, it can be leaved to its own devices.

The root of the problem in DHA is in the SMTP protocoll itself: the e-mail servers, if they got the mail to a proper address, would not respond, simply accept it.

If the server got a mail to a non-existent address, then it would give a response either immediately or later whether the post office box exists or not. This process gives information about the e-mail addresses which are upkept by the server. The attackers use this information, sending huge amount of messages to the e-mail server. The addresses from which do not arrive response (so the server accepts the e-mail without negative signal) are gathered to a list. These addresses should belong to valid user accounts, so it is worthy to send uninvited mails to it.

Beside of getting out of our address, the other problem may the DoS like attack of the mail server. For the sake of gathering the e-mails, the attacker (or even more than one) sends huge amount of misaddressed e-mails, which can result in the overloading of computing and network capacity of the server.

There are two main types of DHA attack: the first one is a “brute force” like method, when all the possible character combinations are tried out as e-mail address; the second, a much more sophisticated: typical occurent e-mail addresses are generated from first, second, and nick names, offten occurent words, and well-known e-mail IDs.

One way of the protection against DHA attacks can be the simply complicated-choosen e-mail addresses. Although our collegues may be hardly able to remember it, and the other side of the coin is that this method can do nothing against brute force like attacks.

Other solution can be if we configure the server to accept every e-mails and do not feedback to anyone, and so the misaddressed e-mails are simply ignored. This solution has several backdraws: the mail senders does not know that an address does not exist, so the server may be flooded by uninvited mails. It is also important, that even the legitim user is not informed about misaddressed e-mails. So because of all of these reasons, the ban of feedback is not suggested.

The most applicable would be the refinement of SMTP protocoll, but what can we do by the time this not happens?

Our suggested solution:

We suggest a system built up by components, which infiltrates besides our current system and halts these types of attacks. This system consists of a syslog analyzator, a spam detector, and a virus searching portion. The results are summerised in a centralized registration list, so we keep the list of those computers which are involved in the DHA attack. With the help of the centralized registration list, all member of the system using our components gain information even from each others problems, so the attacker can be banned not only from one place but it can not do any harm for the others as well.

The syslog analyzing system looks up in the e-mail server notifications that where the misadressed e-mails are coming from (which IP address), and makes a detailed report to the central database. In favour of the low number of misaddressed mails, we introduce a method that the discrete missaddressed e-mails can be divided from the real attackers.

Our system can be connected to spam-recognizing softwares. The solution makes it possible to save resources by not analysing the e-mails coming from known DHA attacking servers with other resource-intensive content filtering methods but we ban them. Our system even raises these softwares efficiency combined with them.