Spam Filter based on Dynamic Sender Policy Framework

Tuan-Anh Nguyen, Quang-Anh Tran, Xuan-Thang Nguyen
Faculty of Information Technology, Hanoi University, Hanoi, Vietnam

E-Mails: tuananh,anhtq,nxthang@hanu.edu.vn

Abstract: The Sender Policy Framework (SPF) [1] is an open standard specifying a technical method to prevent sender address forgery. This technique requires network administrators to create SPF records for their domains. A philosophic issue, which may limit the deployment of SPF, is that in order to use SPF, a network administrator needs to configure local DNS; but others, not himself, will take benefits from that configuration. Therefore, we proposed the Dynamic Sender Policy Framework (DSPF) approach, in which, the legal IP addresses of servers which send emails are collected and provided by a third-party. The database of SPF records can be updated automatically and can also be used among other email servers and email gateways. Using DSPF, clients may check the SPF records without any extra configuration of their DNS. Results showed that the system is able to filter 98% spam and 100% phishing. Collecting and updating processes of the database are described. Factors that influence database’s performance are discussed.

Keywords: Spam; Phishing; Dynamic Sender Policy Framework; DSPF;

1. Introduction

The amount of unsolicited commercial email (spam), and more importantly, the fraction of email which is spam, has risen dramatically in the last few years. Recently, a study has shown that 52% of email users say spam has made them less trusting of email, and 25% say that the volume of spam has reduced their usage of email [5]. A calculation about Hanoi University (HANU)’s case shows that the email server in HANU has to handle 15000 emails per day, 80% of which, i.e. 12000 emails, are spam. If a user needs 15 seconds to process an email, including download, read and delete, HANU staff have to spend 50 hours per day to process spam. It results in 1.500.000 VND in economic loss each day.

This crisis has prompted proposals for a broad spectrum of potential solutions, ranging from the design of more efficient anti-spam software tools to calls for anti-spam laws. Over the past
few years, many have proposed new standards or bolt-ons to the SMTP protocol. SMTP stands for Simple Mail Transfer Protocol and is the way mail servers communicate with each other. Spammers have taken advantage of this aspect of email servers to send spam anonymously. Many fixes have been proposed, ranging from simple add-ons to complete rewrites of the protocol. One of the more recent proposals for fighting spam is called Sender Policy Framework (SPF), proposed by an organization called the Anti-Spam Research Group (ASRG). DomainKeys (Yahoo!) and CallerID (Microsoft) [2], [3] are also the techniques in this category.

The Sender Policy Framework (SPF) [1] is an open standard specifying a technical method to prevent sender address forgery. That technique is an essential front-line defense against sender address forgery when deploying protection for the header fields and body. Although this is a great idea not many organizations deployed SPF. The case in Vietnam is even worse. At the time this paper is written, the authors have checked some main email servers in Vietnam such as vnn.vn and netnam.vn but no SPF record is found. A philosophic issue, which may limit the deployment of SPF, is that in order to use SPF, a network administrator needs to configure local DNS; but others, not himself, will take benefits from that configuration. Therefore, we proposed the Dynamic Sender Policy Framework (DSPF) approach, in which, the legal IP addresses of servers which send emails are collected and provided by a third-party. The database of DSPF records is generated and updated automatically by using our DSPF method. Having DSPF, user can query for SPF record without any extra configuration.

This paper discusses technical issues in DSPF approach as well as generating DSPF database and it is structured as follows: Section 2 presents a short description of SPF. Section 3 analyzes in detail the model for the DSPF database and our procedures for generating and updating this database, including some factors that may influence the performance of the database. That influence is discussed in the next section: experiments. A short description of DSPF in progress will be presented in Section 5. Finally, we conclude and provide directions for future research.

2. Methods Sender Policy Framework

Sender Policy Framework (SPF), proposed by an organization called the Anti-Spam Research Group (ASRG). SPF is one of those brain-dead simple ideas that make people wonder why no one thought of it before. It defines which machines on a network are allowed to send mail.

SPF functions as a bolt-on to the SMTP protocol that takes advantage of text records in DNS (records that exist for adding comments and extra information to Internet name records) and allows ISPs to identify “reverse MX records,” which are mail servers on their network that are permitted to send mail. Any host that is sending mail but is not in the permitted-from list can then be identified and either discarded, quarantined, or evaluated with additional scrutiny by a
spam filter. SPF is presently in use at AOL, and many other large providers are beginning to follow suit. An SPF record is one line in DNS and looks like this:

```
aol.com IN TXT "v=spf1 mx -all"
```

The goal of SPF is not to prevent spam but to prevent forgery. In coming years, as SPF grows more popular, sending forged mail “from” a domain that is using SPF will become more difficult. Many believe that pushing the means of identifying spammers out to the domain level instead of the host level will make it easier to find and prosecute spammers (making it more difficult for spammers to operate), as they will have to register and use real domains. With new products like prepaid credit cards, it is relatively easy to register a domain while maintaining your anonymity, however. Still, it is much more difficult to move an entire domain every day than it is to just jump on a newly stolen dialup account. The following example explains more detail how SPF works.

Suppose a spammer forges an aol.com address and tries to spam you. He connects from an IP address somewhere. When he declares MAIL FROM: <forged_address@aol.com>, you don't have to believe him. You can ask AOL if the IP address comes from their network. In this example, AOL publishes an SPF record. That record tells you (your computer) how to find out if the sending IP address belongs to them: aol.com IN TXT "v=spf1 ptr -all"

You execute the "ptr" mechanism, which means: find out the hostname of the sending IP; if it ends in aol.com, it's legit. If the message fails SPF tests, it's a forgery. That's how you can tell it's probably a spammer. By rejecting envelope forgeries early, not only network traffic can be saved but also computing power for further protection measures, thus making the entire process more efficient [1]. By applying SPF, email’s content is not necessary. Therefore legal issues are avoided and the filters do not have to deal with different languages problem; A philosophic issue, which may limit the deployment of SPF, is that in order to use SPF, a network administrator needs to configure local DNS; but others, not himself, will take benefits from that configuration.

We proposed the Dynamic Sender Policy Framework (DSPF) approach, in which, the legal IP addresses of servers which send emails are collected and provided by a third-party. The database of DSPF records is generated and updated automatically by using our DSPF method. We will discuss the procedure for generating DSPF database in following sections.

3. Results Dynamic Sender Policy Framework – DSPF

3.1. DSPF Model

The nature of spam problem is very similar to the nature of DDOS problem where spam uses email forgery while DDOS uses IP spoof. An attractive idea to defense against DDOS was proposed by Kim [5], in which TTL of a packet is compared to the statistical value of TTL in packets which were sent from the same IP address in order to estimate the reliability of that IP. Compared to the spam problem, TTL acts as the IP address of server which sends emails.
Based on the idea for DDOS problem, we maintain the IP addresses of servers which send emails in order to estimate the reliability of an email address. We call this approach “Dynamic SPF”. A model to generate and maintain the DSPF database is proposed as shown in “Fig. 1”

In “Fig. 1”, email database contains up-to-date emails. The emails come from some other ways, including HANU anti-spam service and HANU Mail Service which receive both so many ham emails and spam emails from variety mail servers all over the world. As only domain name and its legal IP addresses are needed, using email header is enough; the content of email is not necessary. We developed a dynamic method to generate DSPF database automatically based on the email database. Since email database is up-to-date every day, the DSPF database always catches up with changes in IP addresses of a domain name of email servers. Even more, DSPF database is provided through a service which automatically provides DSPF database for email gateways and servers. Those users all around the world authenticate senders by conveniently using DSPF service in order to filter spam emails.

Other anti-spam approaches, such as Content-based techniques (SpamAssassin, Bayesian), require a set of ham emails and another set of spam emails independently as sample sets for teaching spam filters to identify the words, headers and other text (characteristics) that stick out the most. As the filters analyze more message text, it’s also able to identify particular characteristics belonging to spam email, or ham email. In our model, generating DSPF database is the key process. This database is updated from a set of emails, without the spam and ham information.

3.2. Generating DSPF database

DSPF database stores the information about a domain name and its legal IP addresses. Each DSPF record contains two data fields, the first field is domain name and the second one keeps a
list of IP addresses belong to the domain name. Herein, we give some examples of DSPF records in Table 1.

**Table 1. Some examples of DSPF records**

<table>
<thead>
<tr>
<th>Domain name</th>
<th>Its IP addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>hanu.edu.vn</td>
<td>202.151.161.163</td>
</tr>
<tr>
<td>netnam.vn</td>
<td>202.151.160.20, 202.151.160.23</td>
</tr>
<tr>
<td>gmail.com</td>
<td>38.98.127.148, 74.125.46.29, 74.125.46.30, 74.125.46.31, 74.125.46.152, 74.125.46.156, 74.125.46.158, 202.151.160.20,…</td>
</tr>
</tbody>
</table>

The easiest way to build up database is to contact with domain names owners, asking for the IP addresses of each domain name but this way seems to be an impossible mission.

Another way is we built the database based on the information extracted from email header. As explained, the Active Duration of all pairs of domain-IP address is considered in generating DSPF database process. We implemented a script to extract needed information in email header from emails database. Based on our spam/ham set, statistical figures show that 99% of spam servers use one domain name to send spam in the period of less than 5 days. For example, Table 3 provides the active duration of some pairs of domain name gmail.com while Table 4 shows general information about the active duration of all pairs of gmail.com

**Table 2. Active duration of some pairs of gmail.com**

<table>
<thead>
<tr>
<th>Domain name</th>
<th>IP Address</th>
<th>Active duration (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmail.com</td>
<td>72.14.246.241</td>
<td>1</td>
</tr>
<tr>
<td>gmail.com</td>
<td>74.125.46.29</td>
<td>12</td>
</tr>
<tr>
<td>gmail.com</td>
<td>202.151.160.20</td>
<td>22</td>
</tr>
<tr>
<td>gmail.com</td>
<td>202.151.160.25</td>
<td>18</td>
</tr>
<tr>
<td>gmail.com</td>
<td>194.44.120.190</td>
<td>less than 1</td>
</tr>
</tbody>
</table>

**Table 3. Active duration of all pairs of gmail.com**

<table>
<thead>
<tr>
<th>Domain name</th>
<th>IP Addresses</th>
<th>Active duration (days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>gmail.com</td>
<td>38.98.127.148, 74.125.46.29, 74.125.46.30, 74.125.46.31, 209.85.142.188, 209.85.142.189,…</td>
<td>&gt;=3</td>
</tr>
<tr>
<td>gmail.com</td>
<td>72.14.220.156</td>
<td>2</td>
</tr>
<tr>
<td>gmail.com</td>
<td>219.148.11.192, 219.148.11.176, 219.148.11.184, 219.148.11.163, 64.233.184.236, 74.125.44.29,…</td>
<td>Less than 1</td>
</tr>
</tbody>
</table>

This valuable information can be used to authenticate one sender, and generate DSPF database. Based on email database, we extracted information about active duration of all pairs of domain-IP address. The active duration (in days) of one pair is indicated from the first time to the last time sending mail event occurs.
4. Experiments

4.1. Dataset

The email set used in this research was collected from HANU’s email server in 1 month from 2008 June 1st to 2008 June 30th. The data set includes 7855 ham emails, 38955 spam emails, and 53 phishing emails to evaluate not only the performance results but also the accuracy of active duration of pairs domain-IP address.

4.2. Accuracy of active duration of a pair domain-IP

We calculated the number of pair domain-IP for each particular active duration value ranging from 1 day to 26 days. The result is shown in Fig. 2. As can be seen from “Fig. 2”, based on our spam/ham dataset, almost all pairs of spam servers have the active duration is less than 3 days and very few have the active duration is more than 3 days, this number decreases when the time increases. Meanwhile, almost all pairs of legal servers have the active duration is more than 3 days. As a result, it is reasonable to choose 3 days as the threshold to distinguish between pairs of spam servers and pairs of legal servers.

![Figure 2. Active duration of legal domains and spam domains](image)

4.3. Performance

About the evaluation criterion, we used four common parameters to evaluate our filter, FN (False-Negative) is the number of spam messages marked as ham; FP (False-Positive) is the number of ham marked as spam; TN (TrueNegative) is the number of ham marked as legitimate; TP (True Positive) is the number of spam messages marked as spam; SR (Spam recall); and HE (Ham Error). With:

\[
SR = \frac{TP}{TP + FN} \quad HE = \frac{FP}{TP + FP}
\]
As proposed in Section 3, active duration is very important factor that influences the performance result of DSPF database or the filter. Experiment results with different values of the active duration threshold are as follows:

Table 4. Active duration of all pairs of gmail.com

<table>
<thead>
<tr>
<th>Active duration threshold (days)</th>
<th>Amount of FP</th>
<th>Amount of FN</th>
<th>FP (%)</th>
<th>FN (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2</td>
<td>1381</td>
<td>0.03</td>
<td>3.55</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>1063</td>
<td>0.08</td>
<td>2.73</td>
</tr>
<tr>
<td>3</td>
<td>11</td>
<td>866</td>
<td>0.14</td>
<td>2.22</td>
</tr>
<tr>
<td>4</td>
<td>51</td>
<td>809</td>
<td>0.65</td>
<td>2.08</td>
</tr>
<tr>
<td>5</td>
<td>103</td>
<td>760</td>
<td>1.31</td>
<td>1.95</td>
</tr>
<tr>
<td>6</td>
<td>140</td>
<td>731</td>
<td>1.78</td>
<td>1.88</td>
</tr>
<tr>
<td>7</td>
<td>189</td>
<td>708</td>
<td>2.41</td>
<td>1.82</td>
</tr>
</tbody>
</table>

“Fig. 3” shows a spectacular result. The Spam Recall of the filter based on DSPF database is about 98% and the Ham Error is about 0.1% with the active duration threshold is 3-day. That means 3-day threshold is the best choice for the DSPF-based filter.

![Graph showing FP and FN percentages](image)

**Figure 3.** Performance with different active duration thresholds

5. DSPF in progress

As the results from experiments above, we implemented and deployed a DSPF Plug-in for SpamAssassin to verify email server addresses by querying the DSPF service (http://fit.hanu.vn/~anhtq/dspf). It can be easily installed in SpamAssassin. When SpamAssassin processes an email, the DSPF Plug-in (http://fit.hanu.vn/~anhtq/dspfplugin.html) extracts the domain and the IP which sent email from the email and forms a DNS query. DSPF Plug-in then queries the DSPF service to verify the IP is allowed to send email from the domain. The test results in a SpamAssassin rule. You may change the point of the rule to make it work well together with another rules in SpamAssassin.

We also provide an Anti-spam POP3 Proxy (http://fit.hanu.vn/~anhtq/p3sa.html) with SpamAssassin and DSPF Plug-in integrated. If a user uses this Anti-spam POP3 Proxy to receive
emails from a POP3 servers. His/her emails will go through the POP3 Proxy, in which they are examined by SpamAssassin before they come to the user's PC.

6. Conclusion

We proposed a dynamic method to generate automatically SPF records. With this method, the legal IP addresses of servers which send emails are collected and provided by a third-party. The database of SPF records can be updated automatically and can also be used among other email servers and email gateways. Using DSPF service, clients may check the SPF records without any extra configuration of their DNS. Spectacular results showed that the system is able to filter 98% spam and 100% phishing. For the case of DSPF, we have an experience that active duration of pairs domain-IP address is very important factor that influences the performance result of DSPF database and 3-day threshold can maintain the best database.

In other words, maintaining DSPF database is the most important process. In this research, we just used active duration as the key factor for maintaining. Besides, Email Networks is a very interesting approach for anti-spam issue. With a provided history log of an email server, an email network (a graph) whose nodes are email addresses and edges are links on couples of send-receive nodes can be constructed. P.O.Boykin and V. Roychowdhury's research [5] has a remarkable result in using an email network for determining spammers at the client side. This approach can be applied efficiently for maintaining DSPF. Another interesting thing is this method is developed based on a hypothesis that all the email addresses are reliable; however, email address can be forged easily. Applying DSPF could be able to solve the problems. This issue will be focused on in our near future researches.

Acknowledgements

This research was supported by the Ministry of Education and Training of Vietnam, Research Project No. B 2008-26-10. We also would like to express our gratitude to IT Center - Hanoi University for providing the opportunity and supplying data for this research.

References


© 2010 by the authors; licensee Asia Pacific Advanced Network. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/3.0/).