Sender Policy Framework - overview

Written by Marc Grote - mailto:grotem@it-training-grote.de

Abstract

In this article I will give you some information about SPF – Sender Policy Framework and it's implementation.

Some statistics stated that nearly 75% of all e-mail traffic is Spam, sometimes called UCE.

To help against this thread, several vendors are developing solutions against Spam. One solution is SPF.

What ist SPF? SPF is a solution to fight against email address forgery. SPF makes it easier to identify spam mails, viruses and worms.

Let's begin

What is the problem with e-mail and SMTP

SMTP was developed at a time where only a few clients and servers exist. SMTP has so few security features. Originally, any SMTP server would accept mail from anyone, for anyone - known as an open relay. This wasn't a problem in the early days of the Internet, but until some time ago it was a real threat. Today open relay is no longer an issue for the majority of companies because the Admins had done their work and closed open relays. If there are any open relays they will be relative fast listed on Open Relay blocklists like http://ordb.org and many more.
The biggest problem today is mail that's correctly addressed to a valid mail address, but comes from a dubious source (Spammer).

What is SPF

Sender Policy Framework (SPF), formerly Sender Permitted From, is an extension to the SMTP standard. SPF makes it easy to counter most forged "From" addresses in email, and thus helps to counter e-mail spam. The combination is also called SMTP+SPF.

You can see SPF protected domains on the basis of the following logo:

Figure 1: SPF logo

SPF was originally designed by Meng Weng of POBOX. You can read more about POBOX here.

POBOX and Microsoft has combined SPF and the Microsoft Implementation called Sender ID and a third specification called the Submitter Optimization to Sender ID Framework.

SIDF reflects the merger of multiple standards and input from the internet and messaging communities…
?

- ? SPF, by Meng Wong of pobox.com
- ? Microsoft Caller ID for Email

How does SPF work?

SPF is easy to understand. The „Internet“ uses DNS (Domain Name System) to resolve Domain Names (as an example www.msexchange.org) into IP addresses. DNS is also used to direct requests for different services like e-mail and Web Servers. For every Domain around the world an MX (Mail Exchanger) record must exist. An MX record tells the e-mail sender where the target server for receiving mail is located.
SPF is publishing „reverse MX“ records in DNS which tells the mail sender what machines send mail from the domain.
The recipient of the e-mail can now check these records to ensure that e-mail is coming from a „trusted“ sender of this domain.
These „reverse MX“ records can be easily published in DNS. It takes only one line in DNS to fullfil all requirements. I will give you an example later in this article.

SPF operates at the level of the SMTP transaction, and requires at most three pieces of information:

- ? The MAIL FROM: parameter of the incoming mail
- ? The HELO or EHLO parameter of the sending SMTP server (used for Mailer-Deamon bounces which send a blank MAIL FROM)
- ? The IP address of the sending SMTP server

Benefits from SPF

SMTP without SPF allows any computer to send email claiming to be from anyone so it is easy for spammers to send email from forged addresses.
This makes it very difficult to trace back from which system Spam comes from. On the other hand it is very easy for Spammers to fake their sender address so that the receiver trusts this e-mails.

Now it is time for SPF. SPF allows an Administrator of an Internet Domain to specify which machines are authorized to transmit e-mail fort hat domain.

SPF makes it more difficult for spammers to send spam, because if they simply forge a "From" address from an address that implements SPF, receivers that implement SPF will ignore the e-mail.

SPF prevents that spammers forging the domain names given in the „From“-addresses of an e-mail. If a spammer legitimately has an account in that domain, or he ist he owner of the domain, they can still send e-mail.
This is a real problem so that some experts except a massive grow in the registration of one-way domains for spammers to go around SPF and other techniques.

SPF in DNS

It is so easy to implement SPF records in DNS.

An SPF record is a single TXT entry in the DNS database for each domain. TXT entries are standard record types in DNS since DNS was developed.
SPF has a number of mechanisms defined in the SPF draft standard, but SPF is so flexible and extensible that new mechanisms can be implemented without having to rewrite the standard.

The most widely used mechanism for determining the e-mail server for a specified domain will be the 'MX' (Mail Exchanger) record, which states which server is designated to accept e-mails for your domain.

The 'PTR' (Pointer) record instructs the receiver to check the domain name of the sending host through DNS, and to look if this record corresponds with the domain name being checked. If there is a match, the e-mail is from an accepted source, but if they don't it's a forgery. 'PTR' records are used in Reverse Lookup zones.

The 'A' (Host) record allows you to specify that any machine with an address entry in the DNS database which matches your domain is allowed to send e-mail. The 'A' records doesn’t require a PTR DNS record, but instead performs an
This is slightly different to the PTR mechanism because it doesn't require a special PTR DNS record, but instead performs exhaustive searches.

Thus, the key issue in SPF is the specification for the new DNS information that domains set and receivers use. The exact specifications may change (the following specification is from 04/25/2004) but here is one example:

```
; zone file fragment for msexchange.org
                        IN  MX 10 mail.msexchange.org.
.......

mail            IN  A     192.168.1.2
; SPF enries
; domain SPF
Msexchange.org.  IN  TXT   "v=spf1 mx -all"
; mail host SPF
mail            IN  TXT   "v=spf1 a -all"
```

Figure 2: SPF entries in DNS

msexchange.org IN TXT "v=spf1 mx -all"

"v=" = defines the version of SPF used – this attribut is mandatory (SPF1)
„mx“ = Defines the MX record
„ptr“ = PTR ist he record fort he reverse lookup zone

"-all" = Specifies that, if the previous methods did not match, reject the message as a forgery.

The following methods are defined:

A - If the domain name has an A record corresponding to the sender's address, it will match.
MX - If the domain name has an MX record resolving to the sender's address, it will match.
PTR - If the sender reverse-resolves to a domain ending in the domain name, match.
IP4 - If the sender is in a given IPv4 range, match.
IP6 - If the sender is in a given IPv6 range, match.
EXISTS - If the given domain resolves, match.

For more information about SPF DNS configuration, have a look at the following article.

SPF records distribution in DNS

SPF uses the functionality of DNS to distribute SPF records across the DNS hierarchies. SPF records will be cached by several ISPs. This reduces the amount of bandwith required for SPF queries in DNS.

How to publish a SPF record

Publishing records is the first step to using SPF. There are more than 8.000 domains registered today.

How to register depends on the size of your organization. POBOX recommends the following:

If your organization:
- sends mail from under 5 servers,
- hasn't a large technical staff, or
- isn't email-mission-critical,

Self-publishing is your best option, with the quick and easy wizard. In the following picture i will give you an example of the wizard:

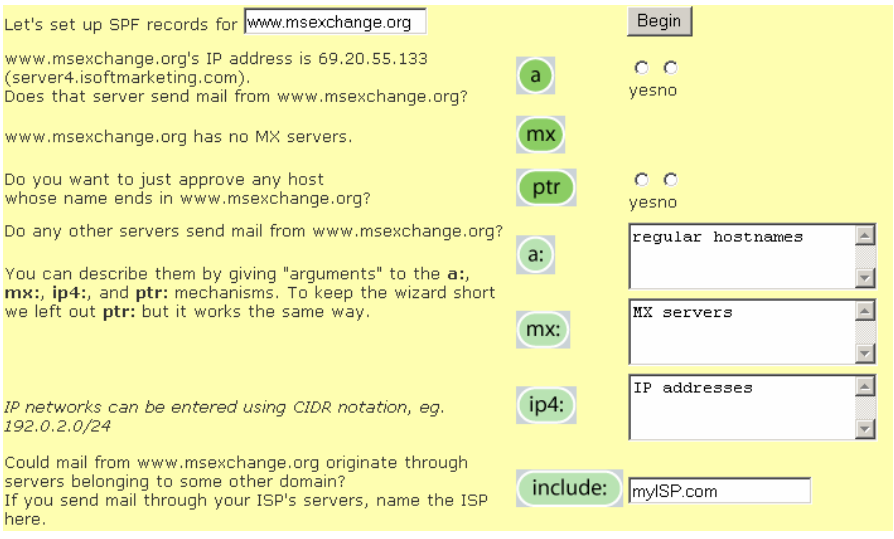

Figure 3: SPF Wizard

If your organization:
- has complex sending needs,
- sends a lot of mail, or
- is a Fortune 1000 company,
You may benefit from SPF certification or consulting. For more information goto the POBOX website at http://spf.pobox.com.

Mail Flows

The following picture shows the Mail Flow in an SPF environment

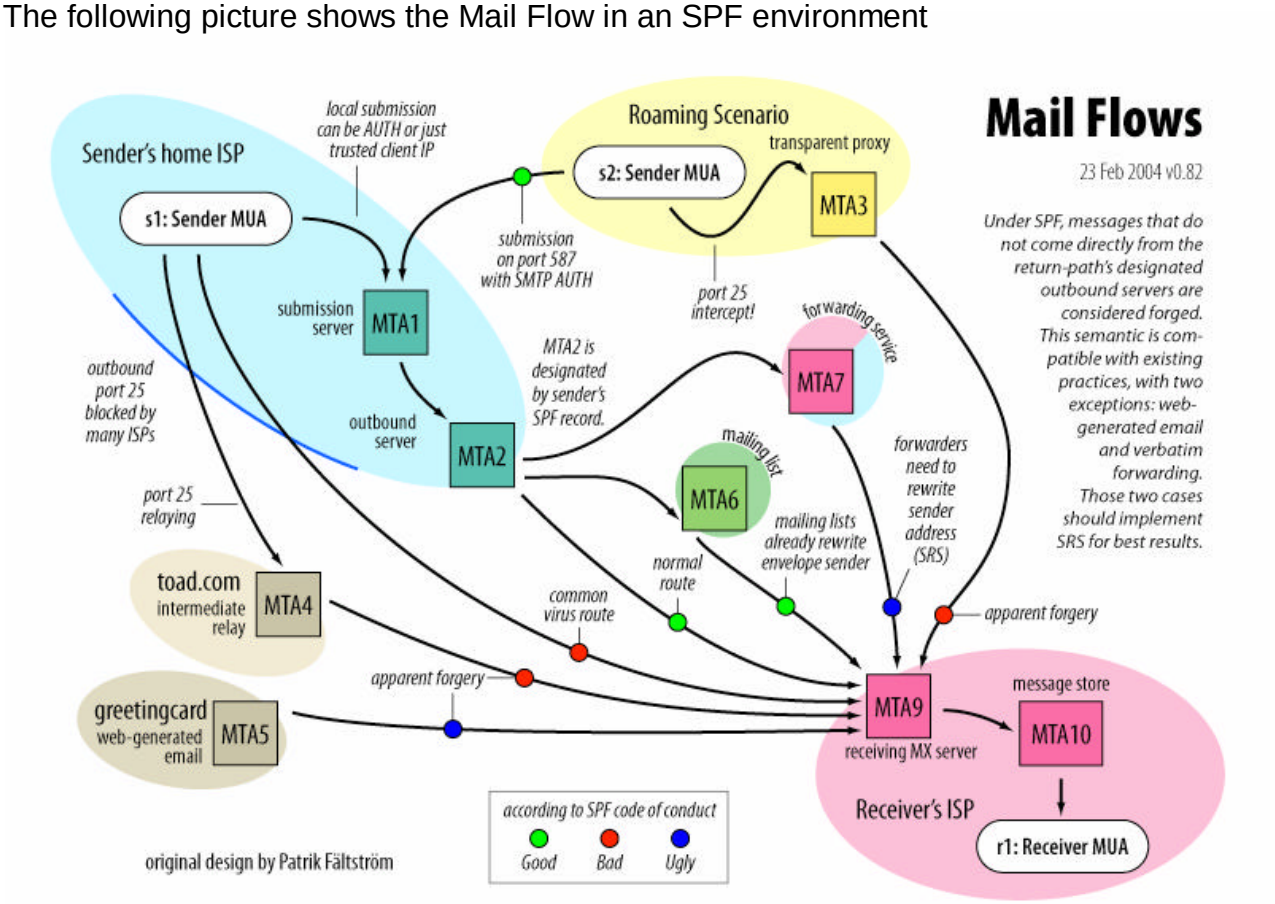

Figure 4: Mail Flow with SPF enabled – with friendly permission from http://spf.pobox.com

What to do with unsupported messaging systems?

As i wrote this article, messaging systems like Microsoft Exchange and Lotus Notes doesn't support SPF.
Until vendors like IBM and Microsoft doesn't support SPF it is possible to place an SPF enabled MTA in front of your unsupported systems. The only thing to do is to change the

mail flow that all incoming mails will be send to the SPF aware MTA. This MTA checks the e-mail and will forward it to the internal mail-system.

SPF problems

SPF breaks SMTP forwarding where an MTA forwards e-mail to someone else without changing the "from" address. One solution fort his problem is a technique called Sender Rewriting Scheme (SRS). SRS is a mechanism for rewriting sender addresses when a mail is forwarded in that way when mail forwarding continues to work within an SPF implementation. Learn more about SRS here.

If a spammer legitimately has an account in that domain, or owns the domain, they can still send email. This is a real problem so that some experts except a massive grow in the registration of one-way domains for spammers to go around SPF and other techniques. But this is not a problem of the SPF implementation – it is a problem in general.

Standardization Status

As i wrote this article, SPF is not an IETF standard but it is one solution with the highest chance to become a standard. There are some other implementations like Microsoft Sender ID, Yahoo DomainKeys and RMX. Another hopeful solution was MARID, but at 09/23/2004, the MARID working group has stopped working because of some differences which technique and record types will make the race.

SPF-aware MTAs

Plugins to MTAs can be found here. There are many MTA Plugins for well known Mail Servers like EXIM, Postfix, Windows 2000 SMTP.

Antispam and MTA vendors that support SPF

There are several Antispam and MTA vendors that support SPF. Some of them are: Brightmail, Ciphertrust, Communigate Pro, Declude, IronPort, MailArmory, MailFrontier, Penguin Software, Sophos and Symantec.

Some well-known names protected by SPF

As i wrote this article the following „Big Player“ were protected by SPF:

AOL.com, Altavista.com, DynDNS.org, eOnline.com, Google.com, GNU.org, LiveJournal.com, OReilly.com, SAP.com, Spamhaus.org, Symantec.com, Ticketmaster.com and w3.org

As you can see in the following picture, the number of SPF protected domains is growing.

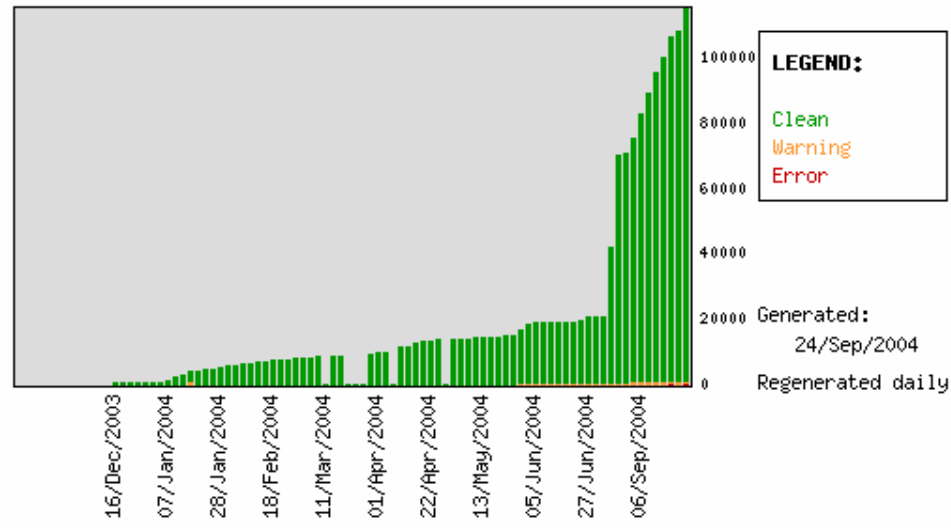

Figure 5: Growing SPF protected domains

Conclusion

SPF has a good chance to become an IETF Standard. SPF will not totally reduce Spam but is a powerful solution to fight against Spam.

Related Links

SPF in general
http://spf.pobox.com
SPF records in DNS
http://www.zytrax.com/books/dns/ch9/spf.html
Free SPF Filter for Windows – bought by GFI
http://www.michaelbrumm.com/smtpspffilter.html
SPF Event Sink for Windows 2000
http://sourceforge.net/projects/spf-event-sink/
How Do SPF and SenderID Work?
http://spf.pobox.com/howworks.html
Informations about SRS
http://www.libsrs2.org/srs/srs.pdf