Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Mitigating Spoofed Emails Using Sender Policy Framework

DECEMBER 2012

Introduction

Organisations are commonly targeted by adversaries using socially engineered emails. Some of these emails are spoofed, that is, the sender's address and other parts of the email header are altered to appear as though the email originated from a different source. It is a common method used by adversaries to gain the trust of a target and increase the likelihood of a successful cyber intrusion. These emails often contain malicious links or attachments which, when opened, can compromise networks.

Organisations can minimise their vulnerability to spoofed emails by implementing a Sender Policy Framework (SPF). This document provides high level guidance on how to implement this framework effectively in an email gateway environment.

What is SPF?

SPF is an email validation system designed to detect and block forged or spoofed emails. This is done by verifying the sender's email server before delivering all legitimate email to a recipient's inbox.

SPF allows an organisation to specify which servers are allowed to send emails for their domain and makes this information available for recipients to check. This is achieved when the network owner creates an SPF entry in the Domain Name System (DNS) record for their domain. The SPF entry will contain a list of domains or valid IP addresses authorised to send emails for their domain.

When an email is sent to a network with SPF checking enabled, the recipient email server validates the sender's domain against the published SPF record. That is, it confirms that the IP address of the sending server is on the allowed list for the domain; if it does not match, SPF verification will fail.

To obtain the best security outcome, validation failure alerts should be acted upon. The network owner can decide whether to block, quarantine or tag emails as suspicious after failing SPF verification.

The Microsoft Exchange email server software implements a variant of SPF called 'Sender ID'.

Why should SPF be implemented?

When implemented and monitored appropriately, SPF can lower the chance of malicious content reaching a network by providing protection against spoofed emails. An adversary uses spoofed email to exploit the trust a user has in the sending domain. The user is much more likely to open a malicious attachment from yourorganisation.com.au than from badguy.com.au.

How to implement SPF

SPF is implemented in two parts – checking and publishing:

- SPF checking enables an organisation to determine whether incoming emails were sent from an authorised source.
- SPF publishing enables an organisation to advertise which email servers are authorised to send emails from their organisation.

Steps required for SPF checking:

- Identify SPF software compatibility for your email server[1].
- Determine your organisation's SPF handling procedure, preferably hard fail (blocking the messages at the gateway) instead of soft fail (tagging the messages as spam but accepting them), but ensure that whichever your organisation uses, users are aware of the procedure.
- In a test environment, configure and test the SPF software compatible with your email server. Ensure the SPF software is tested thoroughly before deployment to your production environment.
- Monitor SPF log messages. If reject messages are being logged, but are thought to be legitimate, consider notifying the administrator of the sender domain so they can check the accuracy of their published SPF record.

Steps required for SPF publishing:

- **Define your outgoing mail servers.** Identify your organisation's authorised mail servers, including your primary and backup outgoing email servers, and possibly your web servers if they send email directly. If users send email while travelling they should do this via an encrypted authenticated path back to your organisation's mail server. Also identify other entities who send email for the domain, for example, advertising or recruitment firms.
- **Ensure HELO/EHLO is sending a valid hostname and that you have an SPF entry for this hostname.** HELO and EHLO (Extended HELO) are basic handshake identification mechanisms relying on DNS hostnames in the Simple Mail Transfer Protocol (SMTP) process. Ensure your outgoing email server is saying EHLO using a valid hostname that can be resolved via DNS, and that you have an SPF entry for this hostname.
- **Construct your SPF record.** SPF records are usually laid out in typical DNS syntax as follows: *organisation.com.au. IN TXT v=spf1 a mx a:domain1.com.au a:domain2.com.au ipaddress1 ipaddress2 -all* where:
  - *organisation.com.au* is your organisation (note the '.' after au to qualify your domain)
  - *v=spf1* defines the version of SPF being used
  - *a* and *mx* specify your organisation's authorised email servers
  - *a:domain1.com.au a:domain2.com.au ipaddress1 ipaddress2* are examples of listing everything that can send emails on behalf of your domain
  - *-all* specifies a hard fail, directing receivers to drop email sent from your domain if the sending server is not authorised
- **Domains that don't send email.** Organisations can specify *v=spf1 -all* in their records, which effectively advises receivers to drop all emails sent from that domain as they will not be legitimate.
- **Warn your users.** Ensure users are warned about the new email policy using SPF. If users are aware of the new process, they will be able to report any implementation issues which may arise:

[1] http://www.openspf.org/Implementations

  - Users are a critical part of an organisation's security posture. Hard fail is the preferable option for SPF. However, if the policy chosen is to tag suspect emails but deliver them to the intended recipient, this is done via *~all* instead of *-all*. This should be done in a manner which delivers the email but alerts the recipient that it is suspect. This can help foster good user behaviour and reduce potential risks to the network.
  - With SPF implemented, emails sent from non-authorised servers, such as outside the corporate network, may no longer reach their intended destinations. If users are required to send emails while away from the corporate network environment, then provisions for (authenticated) remote access to a corporate email server specified in the SPF entry should be made.

- **Test your SPF record.** Testing will ensure that the emails are dealt with correctly.
- **Deploy your SPF record.** When you have a DNS record you intend to deploy, ensure the Time to Live (TTL) of the DNS record is very low (begin with approximately 5 minutes). This will reduce the time required to propagate changes to your authorised email server list across the Internet.
- **Monitor the success of the SPF record you just deployed.** After it has been added, watch your mail logs closely for approximately 20 minutes. Recipients that are not handling your SPF record will typically reject the message at connection time so the sending server will see this effect immediately if SPF is misconfigured.
- **Incorporate accounting for SPF into change controls.** SPF records will have to be updated when new email sending servers are deployed, or when DNS entries or IP addresses change. Make sure your procedures account for these necessary changes as part of your organisation's change management process.

What SPF cannot do

While useful for blocking spoofed emails and spam from an external domain, SPF cannot detect cross-user forgery, that is, where users within a given domain forge the email addresses of others.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

Further information on SPF can be found at http://openspf.org.

Contact details

Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).