(UPDATED) DECEMBER 2012

Mitigating spoofed emails – Sender Policy Framework explained

1. Australian Government agencies are commonly targeted by cyber 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 attackers to gain the trust of the target and increase the likelihood of a successful attack. These emails often contain malicious links or attachments which, when opened, can compromise networks.

2. Agencies 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 your email gateway environment.

What is SPF?

3. 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.

4. SPF allows an agency 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.

5. 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.

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

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

Why should SPF be implemented?

8. SPF is highly ranked in DSD's *Strategies to Mitigate Targeted Cyber Intrusions* and its overall security effectiveness is rated as *excellent*.

9. 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 agency.gov.au than from badguy.com.au.

SPF in the ISM

10. The *Australian Government Information Security Manual* (ISM) states:

    a. Agencies must specify their mail servers using SPF;

    b. Agencies should use SPF to verify the authenticity of incoming emails; and,

    c. Agencies should block, or mark as spam, incoming emails that fail SPF checks.

11. The ISM also advises that without a centralised gateway it is very difficult to deploy SPF. Attackers will often send malicious emails using the recipient's backup or secondary email server since it may be less secure. To prevent this, the ISM states where backup or alternative email gateways are in place, they should be maintained at the same standard as the primary email gateway.

How to implement SPF

12. SPF is implemented in two parts - checking and publishing:

    a. SPF *checking* enables your agency to determine whether incoming email was sent from an authorised source.

    b. SPF *publishing* enables you to advertise which email servers are authorised to send email from your agency.

    Steps required for SPF checking:

    a. Identify SPF software compatible for your email server. A list of software can be found at:

        http://www.openspf.org/Implementations

    b. 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 agency uses that the system users are aware of the procedure.

    c. 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.

    d. 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:

a. **Define your outgoing mail servers.** Identify your agency'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 the agency's mail server. Also identify other entities who send email for the domain, for example, advertising or recruitment firms.

b. **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.

c. **Construct your SPF record.** SPF records are usually laid out in typical DNS syntax as follows:

i. agency.gov.au. `IN TXT v=spf1 a mx a:domain1.gov.au a:domain2.gov.au ipaddress1 ipaddress2 –all`

ii. where:

- *agency.gov.au* is your agency (note the `.` after au to qualify your domain)
- `v=spf1` defines the version of SPF being used
- `a` and `mx` specify your agency's authorised email servers
- `a:domain1.gov.au a:domain2.gov.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.

d. **Domains that don't send email.** Agencies 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.

e. **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.

i. Users are a critical part of an agency'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.

ii. 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.

f. **Test your SPF record.** Testing will ensure that the emails are dealt with correctly.

g. **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.

h. **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.

i. **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 agency's configuration change control process.

What SPF cannot do

13. 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

14. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

15. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:
http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

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

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.