E-mail Sender Address Forgery Mitigation

In the last years there was a rise in abusive-e-mail carrying fake sender e-mail addresses.

One of the most common e-mail abuses, spam, is often distributed using spoofed e-mail addresses by forging the e-mails' "Mail From" in the message body or the "From" in the header. Today most spammers will not use a real return address because they would have their account blocked very quickly. A side-effect of the use of forged or spoofed e-mail addresses is a "backscatter" i.e. you receive a bounce message with a Non Delivery Report (NDR) for an e-mail that you had never sent. They also use lists of valid e-mail addresses (such as your own) just for the purpose of diverting bounced messages. If a message bounces, spammers don't want it coming back to their mailbox.

Other types of e-mail abuse where the sender address is forged is done by

- Fraudsters, who want to cover their tracks and remain anonymous;
- Computer worms;
- Last and most importantly, for *phishing* and *spear-phishing attacks*. Phishers want to impersonate well-known, trusted identities in order to steal passwords or other personal data from users.

This last type of attacks are performed forging the from (header sender address) with the intent that users can be duped into disclosing information in response to an email purportedly sent by a trusted organization.

To mitigate this risk a framework under the name *Sender Policy Framework* was created. SPF is an e-mail validation system-framework designed to prevent e-mail spam, detecting e-mail spoofing, by verifying sender IP addresses.

Sender Policy Framework (SPF)[1] is an open standard specifying a technical method for e-mail validation. Mail exchangers (MX) use the DNS to check if an e-mail from a given domain is being sent by a host who has the permission to do so. They can check if the sending MTA's IP address is allowed to send messages on behalf of the given domain by analysing the message's address from the MAIL FROM command and querying the domain's DNS record for permitted MTA IP addresses.

SPFv1 protects the envelope sender address or return-path that is used during the transport of the message from mail server to mail server and not the header sender address contained in the "From" or Sender header.

[1] Sender Policy Framework is defined in IETF publication RFC 4408.

SPFv1 allows the owner of a domain to specify their mail sending policy, i.e. which mail servers they use, to send mail from their domain. This is achieved in two steps

- The domain owner publishes this information in an SPF record in the domain's DNS zone;
- When someone else's mail server receives a message claiming to come from that domain, the receiving server checks whether the message complies with the domains stated policy, i.e. what to do with an e-mail coming from an unknown server.

Once you are confident about the authenticity of the sender address, you can accept it and attach reputation to it. While IP-address-based reputation systems have prevailed so far, reputation will increasingly be based on domains and even individual e-mail addresses in the future, too.

HOW TO Publish an SPF record

There are some very good resources on how to publish and check your SPF record:

OPENSPF Project

http://www.openspf.org/

Validate your SPF record

http://www.kitterman.com/spf/validate.html

Create an SPF record:

For Microsoft SenderID Framework
http://www.microsoft.com/mscorp/safety/content/technologies/senderid/wizard/

Other free SPF wizards

http://spfwizard.com/

http://www.mailradar.com/spf/

Enable SPF Check on sender/receiver side

The domain sender policies alone are not worth much, it is the receiving mail servers that need to enforce them. Most mail servers support *SPF* checking either natively or through extensions. A reference in SPF implementations can be found in

http://www.openspf.org/Implementations

In Microsoft Exchange product family SPF is not supported natively, instead they have implemented SenderID [2]. SenderID is a Microsoft protocol derived from SPF with identical syntax, which validates one of the message's address header fields defined by IETF RFC

[2] SenderID is defined in IETF RFC 4406

2822. Which one it validates is selected according to an algorithm called PRA[3] (Purported Responsible Address). The algorithm aims to select the header field with the e-mail address "responsible" for sending the message.

Sender ID can also validate the MAIL FROM. But it defines the new PRA identity to validate, and defines new sender policy record tags that specify whether a policy covers MAIL FROM (called MFROM by Sender ID), PRA, or both.

EXCHANGE 2003 SP2 and later Exchange versions

In Exchange server, SPF is used with SenderID filtering so to use SPF, you have to enable SenderID. To enable it, if you have Exchange 2003 SP2, the Sender ID options can be found by selecting *Properties* of the *Message Delivery object* under *Global Settings* in *the Exchange System Manager* console.

You also need to enable it on the *SMTP virtual server -> ESM -> Servers ->* <your server> *-> Protocols -> SMTP*. Right click on *the Default SMTP Virtual Server* and choose *Properties*. Click on the *Advanced button*, then *edit*. Enable the filter. *Apply/OK* and restart the *SMTP virtual server*.

For more details see the following link

http://www.msexchange.org/articles-tutorials/exchange-server-2003/security-message-hygiene/Configuring-enabling-Sender-ID-filtering-Exchange-2003-SP2.html

EXCHANGE 2010

Open the Exchange Management Console (EMC) on the Edge Transport server. In the console, click **Edge/Hub Transport**. In the work pane, click the **Anti-spam** tab, and then select **Sender ID**. In the action pane, click **Enable** or **Disable** as appropriate and choose an appropriate action.

SenderID how to from Microsoft

http://www.microsoft.com/en-us/download/details.aspx?id=5546

http://www.microsoft.com/en-us/download/details.aspx?id=11163

Once implemented and configured you can see that SPF checking is implemented by seeing the headers of a received e-mail message and consulting the antispam stamps.

Antispam Stamps

In Microsoft Exchange Server 2007/10, anti-spam stamps help you diagnose spam-related problems by applying diagnostic metadata, or "stamps," such as sender-specific information, puzzle validation results, and content filtering results, to messages as they pass through the anti-spam features that filter inbound messages from the Internet, you can consult them at:

[3] Purported Responsible Address, IETF RFC 4407

http://technet.microsoft.com/en-us/library/aa996878(v=EXCHG.80).aspx

EXAMPLE on how to read E-Mail Headers

Domain with an SPF record

<……..>

Message-ID: <5112284C.5080801@cert.europa.eu>

Date: Wed, 6 Feb 2013 10:54:20 +0100

From: Christos Kxxxxxx <chriskxxx@xxx.europa.eu>

User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:15.0) Gecko/20120907 Thunderbird/15.0.1

MIME-Version: 1.0

To: <christos.kxxxxx@xxx.europa.eu>

Subject: test

X-Enigmail-Version: 1.4.4

Content-Type: text/plain; charset="ISO-8859-1"

Content-Transfer-Encoding: 7bit

Return-Path: chriskxxxx@xxx.europa.eu

X-MS-Exchange-Organization-PRD: xxx.europa.eu

Received-SPF: Pass (xxxxxxxxxxxx: domain of

chriskxxx@xxx.europa.eu designates nnn.nnn.nnn.nnn as permitted sender)

receiver=xxxxx(FQDN); client-ip= nnn.nnn.nnn.nnn;

helo=mail.xxx.europa.eu;

X-MS-Exchange-Organization-AVStamp-Mailbox: MSFTFF;1;0;0 0 0

X-MS-Exchange-Organization-SCL: -1

X-MS-Exchange-Organization-SenderIdResult: PASS (1)

X-MS-Exchange-Organization-Antispam-Report: xxxxxxxxxxxxxxxxxxxxxx

X-MS-Exchange-Organization-AuthSource: xxxxxxxxxxxxxxxxxxxxxx

X-MS-Exchange-Organization-AuthAs: Anonymous

<……>

Result on SPF check is in Green , SenderID judgment in Red

The Sender ID (SID) stamp is based on the sender policy framework (SPF) that authorizes the use of domains in e-mail. The SPF is displayed in the message envelope as Received-SPF. The Sender ID evaluation process generates a Sender ID status for the message. This status is: (1) PASS meaning: The IP Address and Purported Responsible Domain pair passed the Sender ID verification check

Domain without an SPF record

<.....>
Accept-Language: en-GB, fr-LU, en-US
Content-Language: en-US
X-MS-Has-Attach:
X-MS-TNEF-Correlator:
x-originating-ip: [nnn.nnn.nnn.nnn]
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable
Return-Path: Christos.KOUxxxxx@xxx.europa.eu
X-MS-Exchange-Organization-AuthSource: XCHSVR1.xxx.europa.eu
X-MS-Exchange-Organization-AuthAs: Anonymous
X-MS-Exchange-Organization-PRD: xxx.europa.eu
X-MS-Exchange-Organization-SenderIdResult: None
Received-SPF: None (XCHSVR1.xxx.europa.eu:
Christos.KOUxxxxx@xxx.europa.eu does not designate permitted sender
hosts)
X-MS-Exchange-Organization-SCL: -1
<……..>

The Sender ID (SID) stamp is based on the sender policy framework (SPF) that authorizes the use of domains in e-mail. The SPF is displayed in the message envelope as Received-SPF. The Sender ID evaluation process generates a Sender ID status for the message. This status is NONE meaning: No published SPF data exists in the sender's Domain Name System (DNS).