**E-mail spoofing and open SMTP server**

An **open mail relay** is an SMTP server configured in such a way that it allows anyone on the Internet to send e-mail through it, not just mail destined to or originating from known users. This used to be the default configuration in many mail servers; indeed, it was the way the Internet was initially set up, but open mail relays have become unpopular because of their exploitation by spammers and worms. Many relays were closed, or were placed on blacklists by other servers.

In the mid-1990s, with the rise of spamming, spammers resorted to re-routing their e-mail through third party e-mail servers to avoid detection and to exploit the additional resources of these open relay servers. Spammers would send one e-mail to the open relay and (effectively) include a large blind carbon copy list, and then the open relay would relay that spam to the entire list. While this greatly reduced the bandwidth requirements for spammers at a time when Internet connections were limited, it forced each spam to be an exact copy and thus easier to detect.

Since open mail relays make no effort to authenticate the sender of an e-mail, open mail relays are vulnerable to address spoofing.

**Email spoofing** is the creation of email messages with a forged sender address.

Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead the recipient about the origin of the message.

When an SMTP email is sent, the initial connection provides two pieces of address information:

* **MAIL FROM:** - generally presented to the recipient as the *Return-path:* header but not normally visible to the end user, and by default *no checks* are done that the sending system is authorized to send on behalf of that address.
* **RCPT TO:** - specifies which email address the email is delivered to, is not normally visible to the end user but *may* be present in the headers as part of the "Received:" header.

Together these are sometimes referred to as the "envelope" addressing, by analogy with a traditional paper envelope, and unless the receiving mail server signals that it has problems with either of these items, the sending system sends the "DATA" command, and typically sends several header items, including:

* **From:** Joe Q Doe <joeqdoe@example.com> - the address visible to the recipient; but again, by default no checks are done that the sending system is authorized to send on behalf of that address.
* **Reply-to:** Jane Roe <Jane.Roe@example.mil> - similarly not checked

and sometimes:

* **Sender:** Jin Jo <jin.jo@example.jp> - also not checked

The result is that the email recipient sees the email as having come from the address in the *From:* header; they may sometimes be able to find the *MAIL FROM* address; and if they reply to the email it will go to either the address presented in the *From:* or *Reply-to:* header - but none of these addresses are typically reliable, so automated bounce messages may generate backscatter.

Although email spoofing is effective in forging the email address, the IP address of the computer sending the mail can generally be identified from the "Received:" lines in the email header. In many cases this is likely to be an innocent third party infected by malware that is sending the email without the owner's knowledge.

*Source: https://en.wikipedia.org/wiki/Open\_mail\_relay; https://en.wikipedia.org/wiki/Email\_spoofing.*