

Mail Anti-Relaying Policy

Email relaying, which is the transmission of mail transparently between networked systems that run mail daemons, is a necessity in the cooperative world of the Internet. Such cooperation and interoperation are what allow mail of various origins to be delivered to arbitrary hosts that often consist of unknown hardware and software, and allow arbitrary mail readers to open and process the mail.

One flaw in mail relaying is that it can be misused for malicious, unsavory, unethical, or illegal purposes. The most common use today is delivery of unsolicited commercial email (UCE), frequently with the sender's address concealed, exploiting systems that allow unauthorized relaying of mail so that it can be delivered from Point A to Point B by way of the unsuspecting Point C.

Unfortunately, this exploitable setting is nearly always the default for software that controls the delivery of mail, and must be reconfigured by the system manager.

Policy for hosts attached to NYU-NET is that mail relaying for messages FROM non-NYU addresses TO non-NYU addresses must be blocked. In this way, machines outside NYU cannot use university resources as a conduit in the transmission of questionable mail, and NYU does not gain a reputation as a haven for unethical practices. (There is also a growing trend toward blacklisting network domains that tolerate relaying of UCE.)

Note: the addresses referred to are the envelope addresses, not any addresses on the mail headers in the message being sent which may well be forged or different from those on the envelope.

SAMPLE EXPLOIT TO BE BLOCKED:

joe@blob.org relays mail to mary@birds.org
by way of blackbox.nyu.edu:

From: joe@blob.org
[illicitly, via blackbox.nyu.edu]
To: mary@blackbox.nyu.edu@birds.org [or]
To: mary%blackbox.nyu.edu@birds.org

SAMPLE LEGAL ADDRESSING:

billy@yoyo.com sends mail to mary@birdbones.org:

From: billy@yoyo.com
[with correct transparent relay via smtp.yoyo.com]

To: mary@birds.org

Practical Considerations

Unix mail transport agents (MTAs) such as sendmail, postfix, qmail, and PMDF, have features that allow the system administrator to disallow relaying mail from an outside host to an outside host. Such MTAs must be upgraded and/or configured by the system administrator to disallow such relaying. **[See related links for details.]**

VMS MTAs have similar tunability and must be configured in the same way.

Netware MTAs, such as Mercury, have been revised to forbid unauthorized relaying.

The PMDF MTA for Windows NT or Windows 2000 Server offers control of mail relaying in the same way.

Other types of systems may have other types of MTAs that can be tuned to block unauthorized transmissions. In all cases, these configurations should be set to block unauthorized relaying. System administrators who have questions about how to do this should send mail to noc@nyu.edu for guidance or further assistance.

Considerations for Travelers

People who use portable machines may find themselves logging into Internet Service Providers (ISPs) that are not under the NYU-NET umbrella of services. In such cases, when mail software (such as Eudora) is configured to use your NYU account as its SMTP host, you will be unable to send mail to people outside NYU, because the NYU host will see you as a non-NYU network object and will block your transmission. The correct solution is that when you use your ISP for network connectivity, change your SMTP host to the hostname supplied by your ISP (e.g., smtp1.ibm.net for users of the IBM Global Network), and revert to your NYU SMTP host when using the NYU network.

Questions or comments? Send email to noc@nyu.edu.

All contents copyright

© New York University

All rights reserved

Page last revised: **December 1998**

Page last reviewed: August 22, 2006