E-Mail filtering

E-mail processing rules define the policy for relaying e-mail. These instructions specify the methods of filtering e-mail messages at University. Filtering must always be performed by software, upholding the secrecy of communications.

These instructions are public, and they must be publicly available.

Since malware and spam endanger information security and may in some cases even prevent communications, filtered messages can be processed in various ways. From case to case, possible actions are: to leave the e-mail message unrelayed; to delete the e-mail message or its attachment; to isolate the message to a specific quarantine zone for a specified period of time, after which it will be deleted; or to relay the message marked as spam to the recipient. Malware should always be removed from the relayed messages. The error messages sent to the original sender or the originating e-mail server and/or the recipient must be in accordance to the RFC 2821 standard. The error message may also contain a user friendly explanation of the error, when possible.

Filtering methods

Blocking Third Party Open Relaying Through University Hosts
University shall not relay to external networks messages that are not originated from the address space of the University, and are not addressed to a recipient who has an e mail account at the University. In addition, University shall have a firewall policy to allow SMTP connections only to its own main mail servers. An example of the error message sent to the originating mail server: -550 Relaying denied-

Relaying E-Mail from Unknown Domains or Hosts
University mail server shall check the DNS records (i.e. Domain Name System records) to confirm the existence of the originating domain or host. If the originating domain or host can not be identified by the means of DNS lookup, relaying can be halted temporarily, until the DNS records of the originating host or domain are in order. An example of the error message sent to the originating mail server: -451 Sender domain must resolve-

Blacklists
University shall not relay e-mail from mail servers that can be used for open relay attacks (see item 1). University may use international databases from well-known service providers for blacklist checks. Examples:

- MAPS (Mail Abuse Prevention System)
- ORDB (Open Relay DataBase)
- DSBL (Distributed Server Boycott List)
- SPAMHAUS (The Spamhouse Project)

An example of the error message sent to the originating mail server: -550 Mail from rejected as spam; see http://www.blacklist_used.domain-

Relaying E-Mail from Mail Servers Known to Be Used for Sending Spam
University shall not relay mail from hosts that are known to be used in sending spam, or hosts that are administrated by organizations that are known to support spammers. For this, University may use international databases from

well-known service providers, e.g. the NJABL database (Not Just Another Bogus List). An example of the error message sent to the originating mail server: -550 Mail from rejected as spam; see http://www.njabl.org-

Relaying E-Mail from Hosts with a Dynamic Network Address
University has the right to decline from relaying e-mail from hosts whose network address is within a dynamically assigned address space. For this, University may use international databases from well-known service providers, e.g. NJABL Dynablock.

An example of the error message sent to the originating mail server: -550 Mail from rejected as spam; see http://www.njabl.org/dynablock.html-

University may apply international databases from well-known service providers in the checks. When using these databases, University must confirm their pertinence, for instance, by checking the service provider's policy for adding addresses into the database. The service provider administering the databases must offer an easy-to-use mechanism to request for removal of an address from the database. The removal requests must be processed within a reasonable timeframe. Database checks can either be performed in real-time, or University may have a local copy of the database, which must be updated at reasonable intervals.

Server-Specific Access Control List
If necessary, University shall use its own server-specific access control lists for spam and malware control. Lists may be used to block temporarily or permanently separate domains, senders, recipients, single network addresses or complete subnets, when it is necessary in order to secure other traffic or to provide protection from intrusion for a single user. An example of the error message sent to the originating mail server: -550 Mail from rejected as spam- or -550 Access Denied-

Filtering Based on Traffic Volume
In traffic analysis filtering, it is possible to notice exceptions in the normal mail traffic, e.g. by monitoring mail server logs in real-time. Such exceptions, suggesting spamming, can be e.g. abnormally long connection duration to a mail server, an abnormally large amount of messages from the same host, or a large amount of recipients in a single message. Traffic can also be controlled proactively, e.g. by bandwidth throttling or by limiting connection duration. Restrictions should, however, always be carefully considered in order not to hinder normal operations, e.g. mailing list operations.

Size of Messages and Number of Attachments
University has the right to restrict the size of the relayed messages, and the number of allowed attachments. Information on the restrictions in the message size and the number of attachments must be publicly available.

Removal of Malware
University shall, within its possibilities, remove malware from the relayed messages, or, when necessary, delete a message containing malware completely.

File Types of Attachments
University has the right to not accept or relay messages containing hazardous file types commonly used in spreading malware.

Examples of the file extensions that can contain malicious code: .ade, .adp, .bas, .bat, .chm, .com, .cpl, .crt, .dll, .exe, .hlp, .hta, .inf, .ins, .isp, .js, .jse, .lnk, .mdb, .mde, .msc, .msi, .msp, .mst, .ocx, .pcd, .pif, .reg, .scr, .sct, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh

An up-to-date list of the file types that University mail server will not accept/relay, shall always be publicly available. Unrelayed files may be isolated to a specific quarantine zone for a specified amount of time, in which case the recipient or the sender shall be informed of their existence before deletion. In such cases, the file may be relayed to the recipient per request, presumed the file does not contain code determined as malicious.

Filtering Based on Message Content
University may filter spam with the help of automated content analysis, e.g. by the means of filtering software performing spam scoring (e.g. Spam Assassin, IMF).

In content analysis, message classified as spam shall always be marked as spam and be delivered to the recipient's mail account, filtered to a specific quarantine zone where the recipient can read it, or otherwise be brought to the recipient's attention within a reasonable timeframe.

Delaying
When necessary, University has the right to delay relaying a message for a reasonable time in order to recognize possible malware in e-mail traffic.

Miscellaneous
University shall within its possibilities, either in its firewall configuration or by other means, prevent sending e-mails addressed to other domains through other servers than its official mail servers.

E-mail filtering may be performed by an add-on program installed to e-mail software, by a central filtering server or by a gateway. Items 1 through 8 in these instructions are recommended to be performed in an e-mail gateway; item 9 in a central filtering server and on user's workstation; item 10 in a central filtering server; and item 11 in a central filtering server and/or user's workstation.

At the time of the compilation of these instructions, filtering methods that significantly restrict the openness typical to e-mail service were considered as non-recommendable. Such methods include challenge/response, graylisting and methods that are in experimental phase, e.g. RMX, SPF, DMP. Use of the previously mentioned methods is acceptable for evaluation purposes, but they should not be used as primary filtering methods.

University shall see to it that the e-mail addresses used in the administration of an e mail domain (e.g. postmaster@tut.fi and abuse@tut.fi) exist and the messages sent to them are delivered to the correct recipients.
Information on the filtering methods used by University shall always be publicly available.

More information can be obtained from address postmaster@tut.fi.