TURKU AMK
TURKU UNIVERSITY OF
APPLIED SCIENCES

Instructions for email filtering

Turku University of Applied Sciences 13.9.2015

Sisältö

Instructions for email filtering

Introduction

The principles for transmitting emails are defined in the regulations concerning email-transmission. These instructions specify the way in which emails are filtered at TUAS. The filtering must always be done programmatically, and the actions taken must not violate the freedom of speech, protections provided for privacy or the confidentiality of email-messages to a greater extent than necessary. These instructions are public, and must be publicly accessible.

Since nuisance software and junk emails pose a threat to data security, and may even prevent communication, messages may be undelivered on a case-by-case basis. Messages may also be destroyed, removed, isolated in a separate, quarantined area for a specific period of time, after which they will be destroyed; or they may be transmitted to the recipient marked as junk mail. An attempt must always be made to remove nuisance software from messages to be transmitted. In terms of filtered messages, error messages to be sent to the sender or the transmitting mail-server and/or recipient, must in all instances adhere to the RFC 2821-standard. A user-friendly description of the error may also be attached to the error message, whenever possible.

Filtering Methods

1 Third party open relay-blocking, i.e. blockage of relay attacks via the Turku University of Applied Sciences (TUAS) computers

The Turku University of Applied Sciences does not externally transmit messages, which do not originate in the TUAS address-universe, and whose recipients have an email address other than that of TUAS. Additionally TUAS, through its firewall-operation, prevents SMPT-connections from the Internet to other than its primary mail-servers.

An example of an error message to be delivered to a transmitting mail-server: "550 Relaying denied".

2 Mail transmission from unknown domains or computers

The TUAS mail server does a name-service check-up in order to ascertain the existence of a sender domain or computer. In cases where the sending domain or computer does not clear the name-service check-up, delivery of the message is prevented temporarily, until the name-service records of the transmitting computer or domain get clearance.

An example of an error message to be delivered to an originating mail-server: "451 Sender domain must resolve".

3 Blacklists

The Turku University of Applied Sciences does not transmit mail from mail servers, which may be used for relay attacks (Item 1); TUAS may use international databases provided and maintained by well-known service providers as a check-up tool.

Blacklist service providers currently in use:

- ORDB (Open Relay DataBase)
- Blitzed Open Proxy Monitor List
- DSBL (Distributed Server Boycott List)
- SPAMHAUS (The Spamhaus Project)
- CBL (Composite Blocking List)
- SORBS (Spam and Open-Relay Blocking System)

An example of an error message to be delivered to the originating mail server: "550 Mail from XX rejected as spam.

In terms of Items 3 and 4, TUAS may utilise international databases provided and maintained by well-known service providers as a check-up tool. When using these types of databases, their appropriateness must be ascertained by for example, checking the principles applied in adding addresses to the database. The database service provider must be able to provide a

customer-friendly, easy-to-use mechanism to be used for requesting addresses to be removed from the database. Removal requests must be processed within a reasonable time from when they were received. When using databases, the check-up can either be done in real time, or TUAS may maintain its own copy of the databases; in the latter case, the copy must be updated periodically.

4 Server-specific access list

TUAS maintains and uses server-specific access lists to ward off nuisance emails on an as-needed basis. The list enables temporary or permanent closing of separate domains, senders, recipients, individual network addresses, or entire sub-networks, in cases where it is necessary in order to keep other transmissions secure, or to protect an individual from harassment.

An example of an error message to be sent to an originating mail-server: "550 Mail from XX rejected as spam", or "550 Access denied".

5 Filtering based on traffic volume

In traffic-analysis filtering, deviations from regular mail service can be detected by real-time observance of the email-service log. These types of variations may be related to junk mail and may include unusually long connection times to the mail-server, an exceptionally large amount of messages from the same host, or a large quantity of recipients of the same message. Traffic volume may be controlled proactively as well, by for example, slowing down connection speed, or limiting the duration of the connection. Restrictions must, however, always be used carefully in order to prevent disturbances in the functioning of email-lists, for example.

6 Message size and attachment volume

TUAS has the right to limit the size of the messages it delivers, as well as the volume of attachments they may contain. Information on message size and the restrictions placed on the volume of attachments must be publicly available.

7 Removal of nuisance software

The University removes, whenever possible, nuisance software from the messages it delivers, or destroys the entire message containing nuisance software, when necessary.

8 Attachment file types

The Turku University of Applied Sciences reserves the right to not retrieve/relay messages containing risk-prone file types typically used for transporting nuisance software.

BLOCKED FILE TYPES

Double-ended file types, for example:

- File.txt.(exe|vbs|pif|scr|bat|cmd|com|dll)

Additional examples of types of files:

*.ade, *.adp, *.bas, *.bat, *.chm, *.cmd, *.com, *.cpl, *.crt, *.dll, *.docm, *.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 file types, which the TUAS mail-server does not retrieve/relay, must be publicly available at all times.

9 Delaying

The University has the right, when necessary, to delay the delivery of messages for a reasonable period of time in order to identify nuisance software that may accompany regular traffic.

TUAS utilises the greylisting-feature to block messages before they leave the sender's computer. Software operating in front of the mail-server checks the sender's email and ip-addresses, and the recipient's email-address in the greylisting-server database prior to retrieving the message. If one of these three is unknown, the message is refused, and a request is sent to the transmitting server to try again after a short while.

Email servers operating correctly line up the message to be sent in its own queue and retry after a few minutes. For a regular mail-server, this does not present a problem, but for junkmail-senders maintaining a massive queue of messages to be sent it is a problem, due to the limited time available for sending messages.

10 Additional information

TUAS must in its firewall-configuration or otherwise, block transmission of emails to other domains whenever possible, except when using its official mail-servers.

TUAS must see to it that the email-addresses related to the email-domain do exist, and that they are directed to the correct party. These addresses include, among others, postmaster (at) turkuamk.fi and abuse (at) turkuamk.fi.

Information on the filtering methods TUAS uses must be available to the public at all times. Further information is available at postmaster (at) turkuamk.fi.