Ukrainian Research and Academic Network

Elimination of SPAM in URAN's Mail System

Yevhenii Preobrazhenskyi
Volodymyr Galagan

Filtering of SPAM

Based on local processing:

- **Grey List Filtering**

Based on interoperation between mail servers:

- **SPF** (Sender Policy Framework)
- **DKIM** (Domain Keys Identified Mail)
- **DMARC** (Domain-based Message Authentication, Reporting & Conformance)

Grey List Filtering (1)

Processing three parameters (triple tag):

1 - field FROM, 2 - field TO, 3 - IP address.

Forming local databases: ***Whitelist*** and ***Graylist***.

- If new message tag is equal to the ***Whitelist*** – the message is received.
- If new message tag is equal to the ***Graylist*** – the message is received and tag moved from ***Graylist*** to ***Whitelist***. The time to live of tags in the ***Graylist*** is restricted to a certain time (~30min).
- If new message tag is not equal to anything – tag is inserted in ***Graylist***, message is ignored, receipt confirmation is not sent.

Grey List Filtering (2)

Sender (not SPAMer) repeats the message during 30min. Message reaches the recipient with a delay. Next messages will not be delayed.

The success of this method is based on the fact that:

SPAMers usually do not care about the receipt confirmations and do not repeat messages

SPF
(Sender Policy Framework)

Sender in its own DNS inserts the list of IP's used to send e-mail messages.

Receiver verifies IP's of the message source and receives only messages with valid addresses

Sender Policy Framework is defined in IETF publication

DKIM
(Domain Keys Identified Mail)

DKIM offers stronger security than does SPF since it implements a secure verification connection with the senders

The verification is based on keys signature of the messages

The public part of the key is written in the DNS of the sender and is used by the sender for signing the messages. Receiver read the public part of the key and verify the messages.

DKIM is described in RFC 6376

DMARC (Domain-based Message Authentication, Reporting & Conformance) (1)

DMARC expands on the two previous mechanisms, SPF and DKIM, coordinating their results on the alignment of the domain in the FROM header field, which is often visible to end users.

It allows specification of policies (the procedures for handling incoming mail based on the combined results) and provides for reporting of actions performed under those policies

DMARC (Domain-based Message Authentication, Reporting & Conformance) (2)

More than 60% of the world's email boxes are protected by DMARC, representing ~ 2 billion accounts

(http://dmarc.org/presentations/DMARC_anniversary_review_20140218.pdf)

Result of implementation of DMARC and Gray List filtering on URAN mail server:

Reduction of SPAM more than a 100 times

URAN proposal

- To implement DMARC for NRENs and for NRENs users.
- To develop a CBP document on the topic and disseminate it to NRENs.

Used software

- Postgrey: http://postgrey.schweikert.ch
- smf-spf: https://github.com/jcbf/smf-spf
- spfOpenDKIM: http://www.opendkim.org
- OpenDMARC: http://sourceforge.net/projects/opendmarc

Thanks for the attention

Yevhenii Preobrazhenskyi melkin@uran.ua
Volodymyr Galagan gal@uran.ua

www.uran.ua