E-Mail Server and Traffic Control Management in 2012

~ *Ph. D.* **Cosmin Catalin Olteanu** *(University of Bucharest, Faculty of Business and Administration, Romania)*

Abstract: *Emails represents one of the most used communication system in world wide web for more than 15 years and "spam" messages are one of the most annoying and disturbing phenomena. All of us are aware that online marketers are trying to transmit their advertising messages to as many addresses they can. For such "unwanted" messages, adaptive systems must be assembled to review and mark what is wright and what is bad. Always these systems must adapt to consumers preferences to mark only that messages that are not in his white list. Surveys for more than 3000000 messages showed me that some criteria can be defined by start.*

Key words: Email server services, spam adaptive systems, sender policy framework, anti-spam and antivirus email systems.

1. Introduction

The main purpose of the paper is to illustrate that emails represents one of the most used communication system in world wide web for more than 15 years and "spam" messages are one of the most annoying and disturbing phenomena. All of us are aware that online marketers are trying to transmit their advertising messages to as many addresses they can. For such "unwanted" messages, adaptive systems must be assembled to review and mark what is wright and what is bad. Always these systems must adapt to consumers preferences to mark only that messages that are not in his white list. Surveys for more than 300 students showed me that some criteria can be defined by start.

We can improve a public institution email servers services to adapt and fight to spam messages.

A web site should provide different design templates for every device that connects to your site.

The general idea is to decrease unwanted messages.

2. Email System Server Services.

Today is obvious that "spam" phenomena are one of most disturbing system of online marketers to send messages to consumers. For a few years, maybe 10 years ago, was one of the best online selling methods but todays is one that disturbs and annoys people.

For an email server administrator "spam" is always a battle that is running continuously. You should always find other ways for marking unwanted messages and fighting "bad" guys.

For start I have found that a colection of systems that are well running toghether can figth quite well. These systems are: Postfix, Spamassasin, Clam Assasin, Clam AV, Procmail, Dovecot and Roundcube.

Nowadays mail servers check a meesage on arival if is signed by domain keys or by sender policy framework (SPF). A SPF mark will check DNS settings if SPF is the designated one in name server.

For example:

```
faa.ro. IN  TXT "v=spf1 ip4:92.87.204.140 a mx ptr include:faa.ro a:faa.ro mx:faa.ro ~all"
```

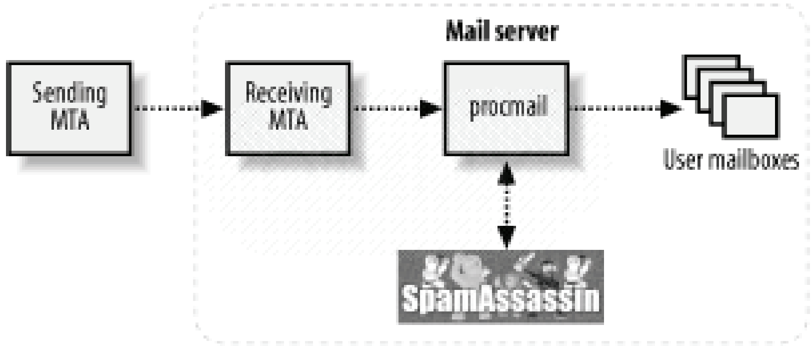
If we look at a survey for one day on a server running these services we can see how may messages were marked as spam or with virus signatures and on what hours were delivered:

```
Grand Totals
------------
messages

  1529   received
  1761   delivered
   121   forwarded
    28   deferred  (69  deferrals)
   231   bounced
  1379   rejected (43%)
     0   reject warnings
     0   held
     0   discarded (0%)

 63570k  bytes received
 78152k  bytes delivered
  1064   senders
   209   sending hosts/domains
   175   recipients
    25   recipient hosts/domains
```

```
Per-Hour Traffic Summary
------------------------
   time         received  delivered   deferred    bounced     rejected
   ------------------------------------------------------------------
   0000-0100        60        69          3          8          84
   0100-0200        66        72          4         11          73
   0200-0300        82        91          3         14          84
   0300-0400        50        60          4         12          65
   0400-0500        73        90          0          9          85
   0500-0600        55        63          6          0          54
   0600-0700        46        51          4          6          29
   0700-0800        52        59          4         11          48
   0800-0900        61        68          5         11          36
   0900-1000        53        59          0          4          48
   1000-1100        66        73          0          9          55
   1100-1200        81        93          5         13          57
   1200-1300        67        73          8         16          75
   1300-1400        92       104          7          7          62
   1400-1500        92       111          2          8          69
   1500-1600        91       106          3         13          69
   1600-1700        89       103          1         13          93
   1700-1800        71        74          0          9          48
   1800-1900        48        61          0          3          43
   1900-2000        49        63          0          8          35
   2000-2100        59        76          1         17          67
   2100-2200        46        47          0         14          43
   2200-2300        37        37          8          2           0
   2300-2400        43        58          1         13          57
```

Fig 1 Mail sever

(source http://commons.oreilly.com/wiki/images/b/bf/SpamAssassin_I_2_tt8.png)



For start we can set as a MTA service Postfix that is configured for authenticate on sending messages with SSL and not to be an open relay.

Than we can define in Postfix master.cf to open PROCMAIL to check the status of message.

```
mailbox_command = /usr/bin/procmail -f- -a "$USER"
```

This starst Procmail to look for config procmailrc:

```
PPRIVS=yes
LOGFILE=/var/log/procmail
VERBOSE=ON

:0fw
| /usr/local/bin/clamassassin

:0:
* ^X-Virus-Status: Yes
/home/$LOGNAME/mail/Trash

:0fw: spamassassin.lock
* < 300000
| spamassassin

# Mails with a score of 15 or higher are almost certainly spam (with 0.05%
# false positives according to rules/STATISTICS.txt). Let's put them in a
# different mbox. (This one is optional.)
:0:
* ^X-Spam-Level: \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*
/home/$LOGNAME/mail/Trash

# All mail tagged as spam (eg. with a score higher than the set threshold)
# is moved to "probably-spam".
:0:
* ^X-Spam-Status: Yes
/home/$LOGNAME/mail/Trash

# Work around procmail bug: any output on stderr will cause the "F" in "From"
# to be dropped. This will re-add it.
:0
* ^^rom[ ]
{
LOG="*** Dropped F off From_ header! Fixing up. "

:0 fhw
| sed -e '1s/^/F/'
}
```

That file is looking for Spamassasin and Clamassasin config to check for spam and virus signatures and if found send it to Trash/SPAM folder of web mail.

Spam assassin config file should look like:

```
required_hits 4.8
report_safe 1
rewrite_header Subject *****SPAM***** _SCORE(00)_ ***
#autolearn 1
use_bayes 1
bayes_auto_learn 1
skip_rbl_checks 0
use_razor2 1
#use_dcc 1
use_pyzor 0
#ok_languages en fr ro
#ok_locales ro
whitelist_from logwatch@faa.ro

## Optional Score Increases
score DCC_CHECK 4.000
score SPF_FAIL 10.000
score SPF_HELO_FAIL 10.000
score RAZOR2_CHECK 2.500
score BAYES_99 4.300
score BAYES_95 3.500
score BAYES_80 3.000
```

Clamassassin config file should look like:

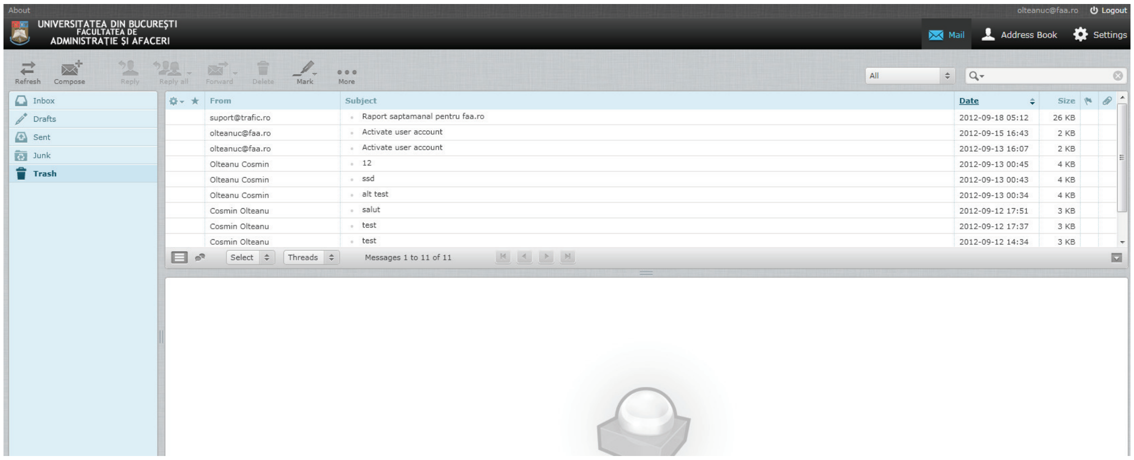
```
bail()
{
  ${RM} -f ${MSGTMP} ${LOGTMP}
  exit ${1}
}

# Routine to bail if error code is passed
bailiferr()
{
  if [ ${1} != 0 ]
  then
    bail ${1}
  fi
}

# Make a temporary file, or bailout if it fails
```

```
mktmp()
{
  MKTMPFILE=`${MKTEMP} -q ${TMPPATH}/${1}.XXXXXXXXXX`

  # The usual method of bailing out when mktemp fails would cause mail to
  # bounce, so instead we add extra logic to have it pass the message
  # unfiltered intead
  if [ $? != 0 ]
  then
    ${FORMAIL} -f -I “X-Virus-Status: Failed” -I \
        “X-Virus-Report: Internal error mktemp ${2} failed” \
        -I “X-Virus-Checker-Version: ${VERSION}”
    bail $?
  fi
}

# make temporary file for message
mktmp clamassassinmsg MSGTMP
MSGTMP=${MKTMPFILE}

# make temporary file for log
mktmp clamassassinlog LOGTMP
LOGTMP=${MKTMPFILE}

# Store the message in the message tempfile for later processing
${CAT} > ${MSGTMP}
bailiferr $?

# Set version header string
CLAMVERS=`${CLAMSCAN} -V --stdout`

if [ ${ADDSCANNERFLAG} != 0 ]
then
  SHORTCLAMSCAN=`${ECHO} ${CLAMSCAN} | ${SED} -e “s/.*\///”`
  CLAMVERS=”${SHORTCLAMSCAN} / ${CLAMVERS}”
fi

if [ ${SIGVERSFLAG} != 0 ]
then
  MAJOR=`${SIGTOOL} --stdout -i ${SIGLOC}/main.cvd \
    | ${SED} -e “/^Version: /!d” -e “s/.* //”`
  MINOR=`${SIGTOOL} --stdout -i ${SIGLOC}/daily.cvd \
    | ${SED} -e “/^Version: /!d” -e “s/.* //”`
  SIGVERS=”${MAJOR}.${MINOR}”
  VERSION=”clamassassin 1.2.4 with ${CLAMVERS} signatures ${SIGVERS}”
else
  VERSION=”clamassassin 1.2.4 with ${CLAMVERS}”
fi
```

```
# Have ClamAV check the message and save the simple results in the log
# temp file

${CLAMSCAN} ${CLAMSCANOPT} - < ${MSGTMP} > ${LOGTMP} \
  2> /dev/null
RESULT=$?

# If the message is clean, clamscan exits with status 0

if [ ${RESULT} = 0 ]
then
  # Spit out the message with a header indicating it is clean
  ${FORMAIL} -f -I “X-Virus-Status: No” -I “X-Virus-Report:” \
     -I “X-Virus-Checker-Version: ${VERSION}” < ${MSGTMP}
  bailiferr $?
else
  # If the result is 1, then a virus was detected
  if [ ${RESULT} = 1 ]
  then
    # Chop off the tempfile name off the virus message
    # This is a bit complex because there may be multiple status lines
    REASON=`${SED} -e ‘s/[^:]*: //’ -e ‘/ FOUND$/!d’ \
      -e ‘s/ FOUND$/ Gasit /’ < ${LOGTMP} | ${SED} -n -e ‘H;${x;s/\n//g;p;}’`
    # Extract the subject so it can be modified if SUBJECTHEAD is set
    # Note that some versions of formail will add a leading space to the
    # subject line, so we strip off one leading space if present.
    SUBJECT=`${FORMAIL} -c -x “Subject:” < ${MSGTMP} | ${SED} -e “s/^ //”`
    # Spit out the message with the headers showing it is infected and how
    ${FORMAIL} -f -I “Subject: ${SUBJECTHEAD}${REASON}*****${SUBJECT}” \
      -I “X-Virus-Status: Yes” -I “X-Virus-Report: ${REASON}” \
      -I “X-Virus-Checker-Version: ${VERSION}” < ${MSGTMP}
    bailiferr $?
  else
    # If the result was not 0 or 1 then some sort of error occured
    ${FORMAIL} -f -I “X-Virus-Status: Failed” -I \
      “X-Virus-Report: ${CLAMSCAN} error ${RESULT}” \
      -I “X-Virus-Checker-Version: ${VERSION}” < ${MSGTMP}
    bailiferr $?
  fi
fi

# Clean up the temp files
bail 0
```

An end user always see an webmail interface where all the mail are in inbox and unwanted messages on TRASH/Spam folder. For example Roundcube or Squirrelmail.

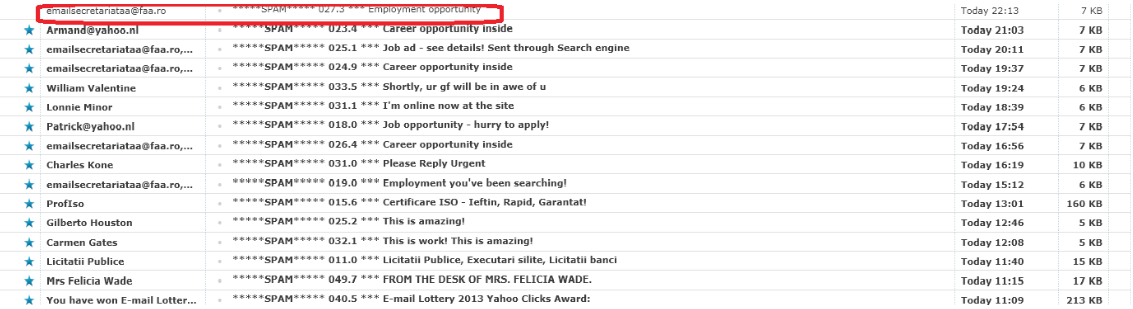
Fig. 2 Roundcube Webmail



From	Subject	Date	Size
suport@trafic.ro	Raport saptamanal pentru faa.ro	2012-09-18 05:12	26 KB
olteanuc@faa.ro	Activate user account	2012-09-15 16:43	2 KB
olteanuc@faa.ro	Activate user account	2012-09-13 16:07	2 KB
Olteanu Cosmin	12	2012-09-13 00:45	4 KB
Olteanu Cosmin	ssd	2012-09-13 00:43	4 KB
Olteanu Cosmin	alt test	2012-09-13 00:34	4 KB
Cosmin Olteanu	salut	2012-09-12 17:51	3 KB
Cosmin Olteanu	test	2012-09-12 17:37	3 KB
Cosmin Olteanu	test	2012-09-12 14:34	3 KB

Messages 1 to 11 of 11

Fig. 3 Spam messages with points analysis on SPAM



	emailsecretariataa@faa.ro	*****SPAM***** 027.3 *** Employment opportunity	Today 22:13	7 KB
★	Armand@yahoo.nl	*****SPAM***** 023.4 *** Career opportunity inside	Today 21:03	7 KB
★	emailsecretariataa@faa.ro,...	*****SPAM***** 025.1 *** Job ad - see details! Sent through Search engine	Today 20:11	7 KB
★	emailsecretariataa@faa.ro,...	*****SPAM***** 024.9 *** Career opportunity inside	Today 19:37	7 KB
★	William Valentine	*****SPAM***** 033.5 *** Shortly, ur gf will be in awe of u	Today 19:24	6 KB
★	Lonnie Minor	*****SPAM***** 031.1 *** I'm online now at the site	Today 18:39	6 KB
★	Patrick@yahoo.nl	*****SPAM***** 018.0 *** Job opportunity - hurry to apply!	Today 17:54	7 KB
★	emailsecretariataa@faa.ro,...	*****SPAM***** 026.4 *** Career opportunity inside	Today 16:56	7 KB
★	Charles Kone	*****SPAM***** 031.0 *** Please Reply Urgent	Today 16:19	10 KB
★	emailsecretariataa@faa.ro,...	*****SPAM***** 019.0 *** Employment you've been searching!	Today 15:12	6 KB
★	ProfIso	*****SPAM***** 015.6 *** Certificare ISO - Ieftin, Rapid, Garantat!	Today 13:01	160 KB
★	Gilberto Houston	*****SPAM***** 025.2 *** This is amazing!	Today 12:46	5 KB
★	Carmen Gates	*****SPAM***** 032.1 *** This is work! This is amazing!	Today 12:08	5 KB
★	Licitatii Publice	*****SPAM***** 011.0 *** Licitatii Publice, Executari silite, Licitatii banci	Today 11:40	15 KB
★	Mrs Felicia Wade	*****SPAM***** 049.7 *** FROM THE DESK OF MRS. FELICIA WADE.	Today 11:15	17 KB
★	You have won E-mail Lotter...	*****SPAM***** 040.5 *** E-mail Lottery 2013 Yahoo Clicks Award:	Today 11:09	213 KB

A detailed analysis on a SPAM messgae can be seen bellow.

```
Content analysis details:   (27.3 points, 4.8 required)

 pts rule name              description
---- ---------------------- --------------------------------------------------
 0.6 URIBL_PH_SURBL         Contains an URL listed in the PH SURBL blocklist
                            [URIs: europswork.com]
 1.6 URIBL_WS_SURBL         Contains an URL listed in the WS SURBL blocklist
                            [URIs: europswork.com]
 1.2 URIBL_JP_SURBL         Contains an URL listed in the JP SURBL blocklist
                            [URIs: europswork.com]
 0.0 URIBL_BLOCKED          ADMINISTRATOR NOTICE: The query to URIBL was blocked.
                            See
                            http://wiki.apache.org/spamassassin/DnsBlocklists#dnsbl-block
                             for more information.
                            [URIs: europswork.com]
 1.7 URIBL_DBL_SPAM         Contains an URL listed in the DBL blocklist
                            [URIs: europswork.com]
```

```
4.3 BAYES_99             BODY: Bayes spam probability is 99 to 100%
                   [score: 1.0000]
2.2 FSL_HELO_BARE_IP_2     FSL_HELO_BARE_IP_2
3.5 HELO_DYNAMIC_SPLIT_IP  Relay HELO'd using suspicious hostname (Split
                   IP)
0.0 TVD_RCVD_IP          TVD_RCVD_IP
0.4 RCVD_IN_XBL          RBL: Received via a relay in Spamhaus XBL
                   [190.186.31.73 listed in zen.spamhaus.org]
3.3 RCVD_IN_PBL          RBL: Received via a relay in Spamhaus PBL
0.0 FREEMAIL_FROM        Sender email is commonly abused enduser mail provider
                   (cutletscd2[at]yahoo.nl)
1.4 RCVD_IN_BRBL_LASTEXT   RBL: RCVD_IN_BRBL_LASTEXT
                   [190.186.31.73 listed in bb.barracudacentral.org]
0.0 RCVD_IN_SORBS_DUL      RBL: SORBS: sent directly from dynamic IP address
                   [190.186.31.73 listed in dnsbl.sorbs.net]
0.2 FREEMAIL_ENVFROM_END_DIGIT Envelope-from freemail username ends in
                   digit (cutletscd2[at]yahoo.nl)
0.5 TAB_IN_FROM          From starts with a tab
2.8 KB_DATE_CONTAINS_TAB   KB_DATE_CONTAINS_TAB
0.8 RDNS_NONE            Delivered to internal network by a host with no rDNS
2.7 KB_FAKED_THE_BAT       KB_FAKED_THE_BAT
```

As a conclusion , I can say that such a system managed on a public email server is a plus for confort of end users and safety of computers.

REFERENCES:

1. http://en.wikipedia.org/wiki/Spam_(electronic)
2. http://spamassassin.apache.org/
3. http://jameslick.com/clamassassin/
4. http://roundcube.net/