Potential of Multilevel SPAM Protection in the Light of Current SPAM Trends

Tomáš Sochor, Alžběta Davidová
University of Ostrava
Czech Republic

International Conference on Networking, Sensing and Control
Evry April 2013
SPAM trends global & local

Global
OSU
UKF
Motivation of the Study

- SPAM amount is still increasing
  - the percentage increased approx. stopped
    - in 2010 (at >90%)
    - since it varies between 75 and 85%
    - but the absolute figures still rise!

- Greylisting
  - our long-term efficiency study since 2007
  - known limitations
    - Automatic White List
ICNSC 2013 Evry

anti-SPAM means should be applied HERE

- Server under control
- Before distribution to users
Typical SPAM control system

Internet → SMTP server Input Filtering → Greylisting → Virus Scanner

SMTP server

Mailboxes

ICNSC 2013 Evry
Greylisting

- Efficient tool to stop SPAM
  - filtering SPAM before delivery
    - saves server disk space and other resources
- Greylisting origin
  - 2003 in the world (E. Harris)
  - 2006 – University of Ostrava
Greylisting principle

- simple idea:
  - operates BEFORE message delivery
  - inserting short delay in message delivery
  - approx. 5 minutes
  - SPAMmer does not repeat the attempt
  - in practice only applied to unknown sources
"450 Greylisted" answered here

ICNC 2013 Evry
Scope of the Study

- refused message ratio at Postgrey
  - it is almost 100% SPAM
  - confirmed by previous studies
- measurement at 2 independent universities
  - 20,000 – 50,000 attempts/day avg.
    - i.e. 2,000 – 5,000 legal messages
- other smaller SMTP server has been studied for shorter period
SPAM percentage long-term

The chart shows the percentage change in SPAM from October 2007 to August 2012. The percentage fluctuates over time, with a general trend of decrease after a peak in mid-2008.
Greylisting weakness

- It is easy to adapt to greylisted server
  - so far it seems not efficient for SPAMmers
- SPAMmer can gets into AWL:
  - After several successful deliveries through greylisting it is considered to be a legal source
    - and not checked any more
  - this behaviour can be eliminated by connection with SPAM scanner
    - DNSB
SPAM Elimination Efficiency

![Bar chart showing spam elimination efficiency over time. The x-axis represents months from April 2010 to August 2012, and the y-axis is scaled in logarithmic units (x10^5). The chart illustrates the number of spam messages blocked by scanners and greylists.](chart.png)
SPAM search+greylisting linkage potential

- Thousands

- Blocked by scanner
- Potentially blocked by greylisting
Conclusions

- Main result: greylisting efficiency is stable in long-term;
- Combination of greylisting and SPAM scanner could bring better greylisting efficiency
Inlet filtering results

January 2010
February 2010
March 2010
April 2010

filtered by SBL
filtered by other postfix filters
Greylisting efficiency rectified
Greylisting efficiency comparison

- 3 SMTP servers as mentioned
- Short period data available from other sites
  - only single figure
  - average for the period available

<table>
<thead>
<tr>
<th></th>
<th>GL efficiency avg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ostrava Uni</td>
<td>89,3%</td>
</tr>
<tr>
<td>Nitra Uni</td>
<td>95,0%</td>
</tr>
<tr>
<td>Zebra</td>
<td>92,2%</td>
</tr>
</tbody>
</table>
Blacklisting issues

- Third-party database
  - not suitable for each organization
- Legal sender in case of message blacklist blocked:
  - refusal is announced to the sender
    - reason could be unclear
    - sender has limited tools to ask for exclusion from blacklist