Email Spam

A Study of different
Spam Handling Techniques
&
Technologies to Combat Spam

Prashanth Srikanthan
April 28, 2004
CS 756

What is Spam?

- Best Description: “Unsolicited Bulk E-Mail”
- In human terms: bulk e-mail you didn’t want, and didn’t ask for.
- Mailing Lists, newsletters, “latest offers”: not Spam, if you asked for them in the first place.
Examples

• Viruses
• Chain Letters
• Messages from strangers
• Fraud emails

Spam Trends

• The bigger they are – the harder they fall
  ➢ The larger an email system is – the higher percentage of Spam it tends to attract.
  ➢ Large ISP’s can receive more than 50% of their email as Spam
  ➢ Large Enterprises can receive more than 40% of their email as Spam.
  ➢ Large audiences are large targets.
Spam Trends (Cont.)

- Spam is non-discriminatory
  - Spam hits not just email networks but, SMS, and IM networks in an increasing manner.
  - Spam is a growing global problem
    - It comes in many languages.
    - It originates from and flows through many different locations
    - It hits email boxes globally

Anti Spam Techniques

“Once upon a time, Spam was easy to spot, and easy to kill…

Then an arms race began, both sides evolving with better and better tools.”
Glossary

- **False Positive** – These are cases where legitimate messages are misidentified as Spam.
- **False Negative** – means that some unwanted messages make it to your inbox.

**Anti Spam Techniques (Cont.)**

- **Simple filtering**

Typical Spam:

- “3 million email addresses for only $50”
- “Great Mortgage Rates!!!”
- “$$$$$$$$QUICK CASH$$$$$$$$$$”

Solution – add an email filter

If (subject contains ‘million’) move to maybe_spam
If (subject contains ‘Mortgage’) move to maybe_spam
If (subject contains ‘$$’) move to maybe_spam
Anti Spam Techniques (Cont.)

- **Domain Level Black- and Whitelists**
  - Most basic form of blocking Spam
  - Administrator puts
    - An offending spammer’s email address on a “blacklist”, so that all future emails are blocked
    - A legitimate email address on a “whitelist”, so that email from that sender is accepted.

---

Anti Spam Techniques (Cont.)

- **Disadvantages**
  - Black- and white list management take constant maintenance to be effective
  - Spammers use thousands of different email addresses to send emails, so blocking only a few of these addresses is unlikely to have any significant impact on the flow.
  - Spammers often “spoof” their address, so it looks like their junk emails are coming from a legitimate sender.
  - In short, black- and whitelists alone tend to stop about 5-10% of Spam.
Anti Spam Techniques (Cont.)

- **Distributed Blacklists**
  - They catalog known spammer addresses and domains, and make them available on the Internet (free or paid subscription).
  - Automatically block any email coming to you from one of these known spammers.
  - Disadvantages
    - Occasionally legitimate email senders get added to the list.
    - Organizations with a high sensitivity to “false positives” tend to avoid using it.

Anti Spam Techniques (Cont.)

- **Heuristic Engines**
  - Heuristics are essentially “rules of thumb”.
  - Human-engineered rules by which a program analyses an email message for spam-like characteristics.
    - Example, a rule might look for the use of phrases like “Get Rich!!” or “Free Viagra!”.
  - Has hundreds or even thousands of these rules to catch Spam.
  - Operate based on a Scoring System: the more rules detect spam-like characteristics in a message, the higher the message’s score.
Anti Spam Techniques (Cont.)

- **Statistical Classification Engines**
  - The most promising recent method to fight Spam.
  - Unlike rules-based heuristics engines, they assess the probability that a given email is Spam.
  - The most common method is the “Bayesian Filtering”

---

Anti Spam Techniques (Cont.)

- **Bayesian Filtering** – How does it work?
  - Make a decision based on previous information and training.
  - Example
    - Say, we see the word ‘click’, we classify email as Spam if
      
      \[
      \text{probability}(\text{spam}|'\text{click}') > \text{probability}(\text{non-spam}|'\text{click}')
      \]
Anti Spam Techniques (Cont.)

- **Bayesian Filtering** – How does it work?
  - Manually classify some spams and non-spams, to build up the training database of words likely to indicate spam, or likely to indicate non-spam.
  - Test a new arriving email against the spam word database, using bayesian decision theory.
  - If the automatic classification is correct, we add this latest email to our training database (stronger database).

Anti Spam Techniques (Cont.)

- **Bayesian Filtering** – How do we classify email?
  - Tokenize the entire email (including headers)
    - 0-9, A-Z, a-z = tokens. Rest are delimiters.
  - Iterate through all tokens in email.
    - Calculate spam probability for each token, store in array.
    - Sort array. So ‘most strong decision’ tokens come first.
  - Choose the top 15 tokens.
  - Combine probabilities together.
  - Determine overall probability that this email is Spam.
  - If >90%, mark as Spam.
Anti Spam Techniques (Cont.)

- Advantages of Bayesian filtering.
  - Less False Positives
  - Filters out 99.5% of Spam

Summary of Anti Spam Techniques

- Accuracy is Key
  - False Positives created by spam filters are unacceptable to email users

- Effectiveness
  - Blocking as much Spam as possible without creating false positives is the name of the game.
  - An anti-spam solution must catch a large majority of all Spam to satisfy end users.
Avoiding Spam

• Never respond to Spam – it validates your email address – you get more Spam.
• Never buy anything advertised in Spam. Doing so encourages Spammers.
• Never go to a site to “Opt Out”
  ➢ It validates your email address.
  ➢ You get more Spam.
• Consider using free “throw-away” accounts for un-trusted services.

Facts & Statistics

• In 2003, Spam costs for American Corporations were $10 - $13 billion, or $14 per employee – Ferris Research
• Email users received an average of 6.2 junk email messages per day in 2002, up from 3.7 in 2001.
• The overall trend of Spam is increasing at about 20% per year.
### Top 15 Spam Originating Countries

<table>
<thead>
<tr>
<th>Country</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>30</td>
</tr>
<tr>
<td>[IANA Reserved]</td>
<td></td>
</tr>
<tr>
<td>[ARIN Unlisted]</td>
<td></td>
</tr>
<tr>
<td>CHINA</td>
<td>25</td>
</tr>
<tr>
<td>Korea - KR [Multicast]</td>
<td></td>
</tr>
<tr>
<td>CANADA</td>
<td>20</td>
</tr>
<tr>
<td>JAPAN</td>
<td>15</td>
</tr>
<tr>
<td>BRAZIL</td>
<td>10</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>5</td>
</tr>
<tr>
<td>Germany</td>
<td>5</td>
</tr>
<tr>
<td>[RIPE Unlisted]</td>
<td></td>
</tr>
<tr>
<td>[APNIC Unlisted]</td>
<td></td>
</tr>
</tbody>
</table>

### Originating Networks

- comcast.net
- rr.com
- atbii.com
- pacbell.net
- ameritech.net
- optonline.net
- charter.com
- hk cable.com.hk
- swbell.net
- verizon.net
- moosq.com
- shawcable.net
- adelphia.net
- dsl-verizon.net
- ne.jp

### Facts & Statistics
Facts & Statistics

- About 40% of all email traffic in the United States is Spam, up from 8% in late 2001.
- Cost Comparison of unsolicited marketing methods.

<table>
<thead>
<tr>
<th>Form</th>
<th>Cost to Sender</th>
<th>Cost to Recipient</th>
<th>% of Cost borne by sender</th>
</tr>
</thead>
<tbody>
<tr>
<td>Telemarketing</td>
<td>$1.00</td>
<td>$0.10</td>
<td>91%</td>
</tr>
<tr>
<td>Postal Mail</td>
<td>$0.75</td>
<td>$0.10</td>
<td>88%</td>
</tr>
<tr>
<td>Automated Phone</td>
<td>$0.07</td>
<td>$0.10</td>
<td>41%</td>
</tr>
<tr>
<td>Spam</td>
<td>$0.00001</td>
<td>$0.10</td>
<td>0.01%</td>
</tr>
</tbody>
</table>

Interesting URLs

- [http://www.spamconference.org](http://www.spamconference.org)
- “What is Spam?” [http://spam.abuse.net/overview/whatisspam.shtml](http://spam.abuse.net/overview/whatisspam.shtml)
- “Email Harvesting Techniques” [http://secinf.net/anti_spam/Email_Harvesting_Techniques_FAQ.html](http://secinf.net/anti_spam/Email_Harvesting_Techniques_FAQ.html)
- Spam Assassin [http://www.spamassassin.org](http://www.spamassassin.org)
Questions

Q?

A!