

# **Email Spam**

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

Prashanth Srikanthan

April 28, 2004

CS 756

CS 756

1

## **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.

CS 756

2

## Examples

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

CS 756

3

## 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.

CS 756

4

## 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

CS 756

5

## 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.”

CS 756

6

## Anti Spam Techniques(Cont.)

### 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.

CS 756

7

## 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

CS 756

8

## 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.

CS 756

9

## 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.

CS 756

10

## 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 spammer.
  - Disadvantages
    - ☞ Occasionally legitimate email senders get added to the list.
    - ☞ Organizations with a high sensitivity to “false positives” tend to avoid using it.

CS 756

11

## 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.

CS 756

12

## 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”

CS 756

13

## 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
$$\text{probability}(\text{spam}|\text{'click'}) > \text{probability}(\text{non-spam}|\text{'click'})$$

CS 756

14

## 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).

CS 756

15

## 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.

CS 756

16

## Anti Spam Techniques (Cont.)

### □ Advantages of Bayesian filtering.

- Less False Positives
- Filters out 99.5% of Spam

CS 756

17

## 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.

CS 756

18

## **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.

CS 756

19

## **Facts & Statistics**

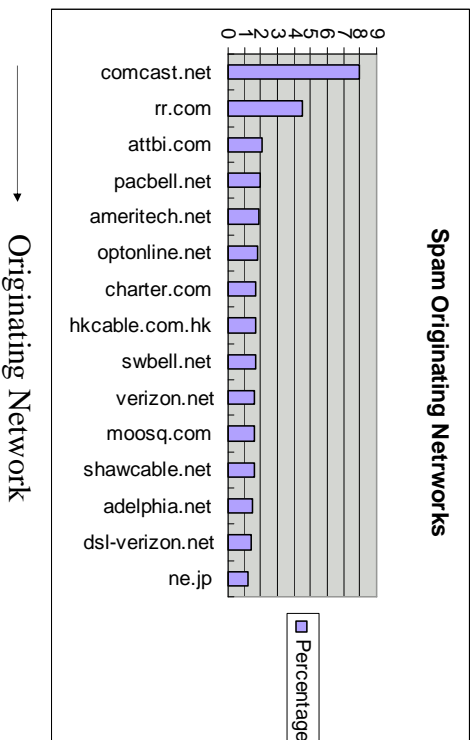
- In 2003, Spam costs for American Corporations were \$10 - \$13 billion, or \$14 per employee – Ferris Research
- Email users received an average of 6.2 junk email messages per day in 2002, up from 3.7 in 2001.
- The overall trend of Spam is increasing at about 20% per year.

CS 756

20

## Facts & Statistics

Spam Originating Networks



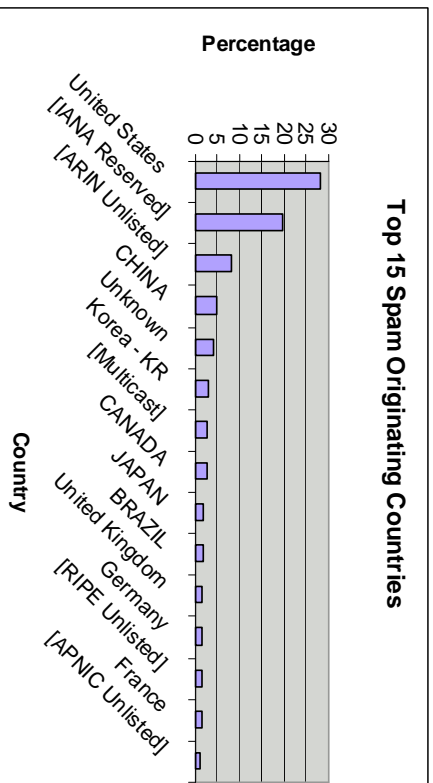
← Originating Network

CS 756

21

## Facts & Statistics

Top 15 Spam Originating Countries



CS 756

22

## 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.

Form	Cost to Sender	Cost to Recipient	% of Cost borne by sender
Telemarketing	\$1.00	\$0.10	91%
Postal Mail	\$0.75	\$0.10	88%
Automated Phone	\$0.07	\$0.10	41%
Spam	\$0.00001	\$0.10	0.01%

CS 756

23

## Interesting URLs

- <http://www.spamconference.org>
- “What is Spam?” <http://spam.abuse.net/overview/whatisspam.shtml>
- “Spam Filtering Techniques – Comparing Half-Dozen Approaches to Eliminating Unwanted Mail”  
<http://gnosis.cx/publish/programming/filtering-spam.html>
- “Email Harvesting Techniques”  
[http://secinf.net/anti\\_spam/Email\\_Harvesting\\_Techniques\\_FAQ.html](http://secinf.net/anti_spam/Email_Harvesting_Techniques_FAQ.html)
- Top 10 Free Spam filtering tools for Windows  
[http://email.about.com/cs/winspamreviews/tp/free\\_spam.htm](http://email.about.com/cs/winspamreviews/tp/free_spam.htm)
- Top 10 Anti Spam Plugins for Outlook  
[http://email.about.com/cs/outlookaddonrev/tp/anti-spam\\_ol.htm](http://email.about.com/cs/outlookaddonrev/tp/anti-spam_ol.htm)
- Spam Assassin  
<http://www.spamassassin.org>

CS 756

24

# Questions

Q?

A!