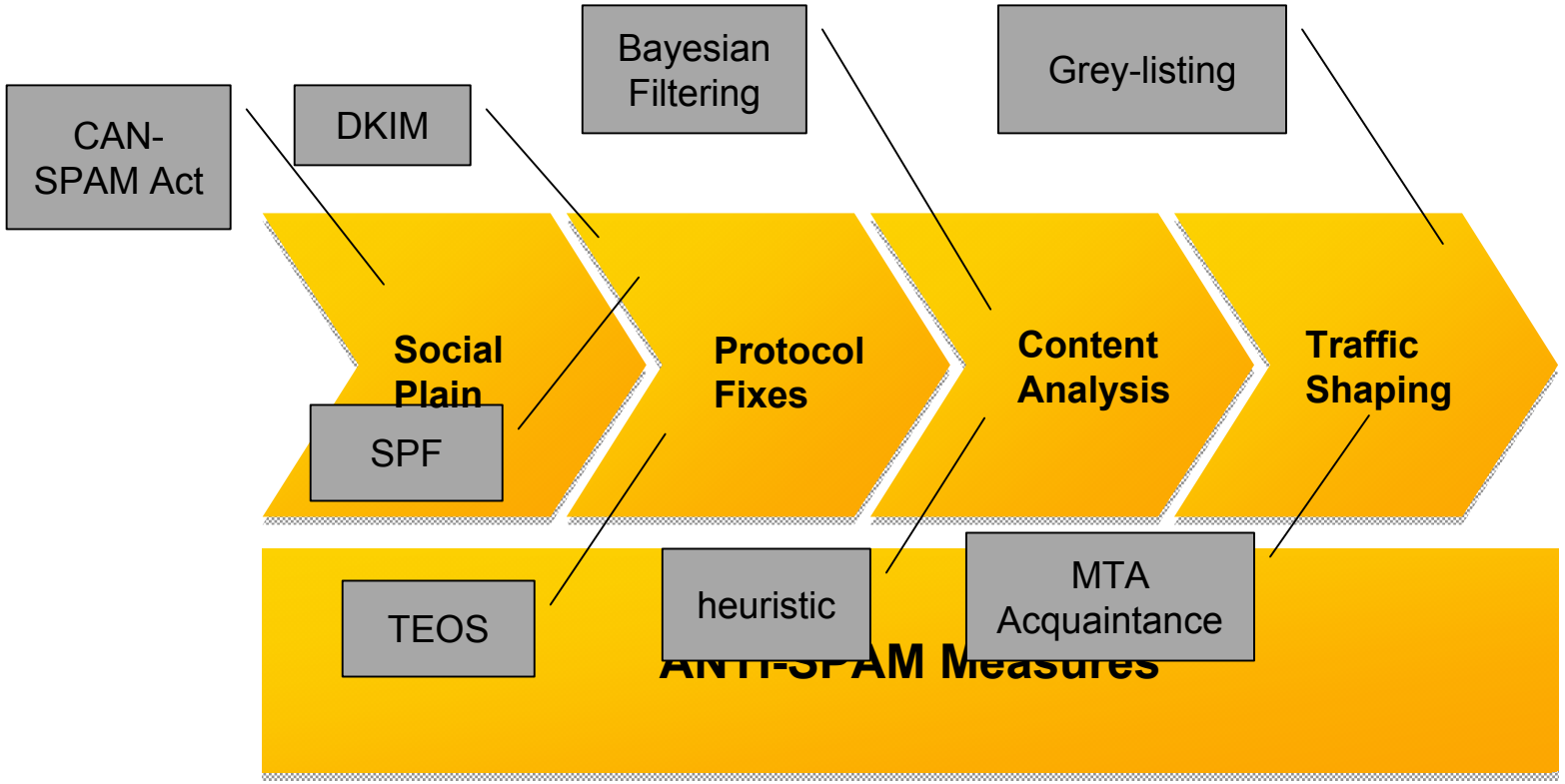
Grey-listing Experiences

Tariq Mustafa, Supernet
tm@nospam.super.net.pk
August 3, 2006
SANOG8, Karachi, Pakistan

The Fight Against SPAM



Anti Spam Classifications

- Content Analysis
- Source Address Blacklisting
- Grey-listing, White-listing
- Sender Identification System
- Challenge / Response

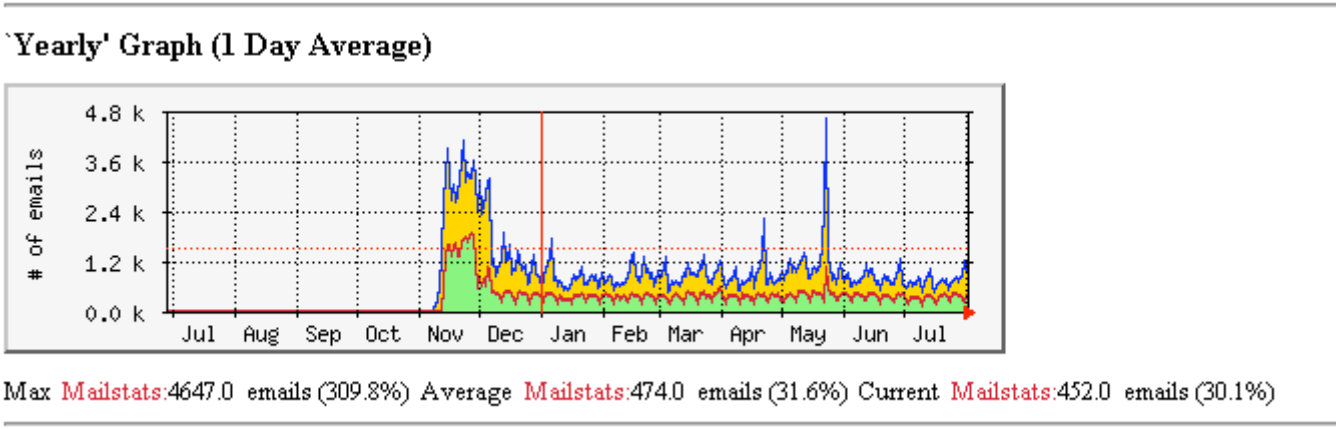
Grey-listing Implementation

- Platform: Slackware Linux version 9.2, Kernel Version 2.4.22;
- MTA: Sendmail 8.13.5
- Grey-listing Software: milter-greylist-2.0.2
  - http://hcpnet.free.fr/milter-greylist/
- In-memory database (other implementations use RDBMS)
- Supports
  - IPv6
  - SPF Records
  - SMTP Auth

How it works

- Concept
- The ‘magic triplet’
  - Sender Email Address
  - Sender IP Address (MTA)
  - Recipient Email Address
- Delay Timer (configurable) for triplets outside white-lists and auto-white-list
- White-listing
  - Recipients’ and Senders’ address based white-listing
  - Public White-lists
  - Private White-lists
  - Auto White-list (Configurable Timer)

Results



- More than 24,000 email users
- As old as 1997 (spam probability increases with email address age)
- 7 Times volume reduction (Down from 3,500 messages / 5 min to 500 messages / 5 min)
- Bandwidth Saving < Customers' Satisfaction
- Savings on mailbox utilization
- Savings on backup costs

Greylisting Tools

- Publicly available white-lists
  - Need for building local ISP white-lists
- Trusted IP Pools and Domains

The Good and Bad (and Interesting!) things of Grey-listing

- Good Things
  - No extra processing
  - Protocol compliance
  - Immediate relief from bulk spammers
  - Very low false positives
  - Works at Server Level
- Bad Things
  - Fails against ‘aspiring spammers’
  - No First-attempt delivery
  - Slight Delay
  - Can cause problems with SMTP server farms
- Interesting Things
  - Customers’ Complain – Not Getting Spam!
  - Broken networks

Thanks!