



# Email Issues - A Primer

**For the benefit of end users  
and administrators**

Copyright © Yukthi Systems Pvt. Ltd., 2006

All rights reserved.

This document can be circulated freely –  
no warranties and no obligations



# Email – why these issues?

- Today's email service is based on protocols/architecture which is ~ 25 years old
- Then, the Internet was a small US DARPA/Univ network (100s of hosts/sites)
- Everybody knew each other
  - Email service was created in this environment of trust
  - There was no reason to build in any controls
- The big problem then was connectivity



# Staggering growth

- Today's Internet has > 1 billion hosts
  - Billions of email messages
- Email has become an established means of business and personal communication
- Use extended in ways never anticipated
  - e.g. Attachments for exchanging files
- Security has replaced connectivity as the big problem



# Architectural deficiencies

- Total lack of security (too much trust!)
  - Neither sending user nor domain are authenticated
  - Sending host could be any IP address
  - Emails are open – anybody can read them
- SMTP – very simple!
- A few header lines (From, To, Cc, Date) standardized but nothing else
- Attachments are a clumsy add-on; inefficient
- No protocol based confirmations/return receipts



# How email works (simplified)

- Your email client (e.g. Outlook) sends email to your outgoing mail server, which may filter it (virus/spam)
- The mail server will do a DNS lookup on destination domain and then send the email
- Receiving server will deliver the email, or may forward to another server if so configured
  - Note: sender has no way of knowing any of this
- Recipient logs in, and retrieves the email. Many desktop clients have email scanning software too



# The problems - Viruses

- Email has become the most common medium for the spread of computer viruses
  - Lack of security and client bugs help virus writers
- Many viruses work by sending out infected emails directly from the infected system
  - Use the address book
  - Use a random From email address
    - Hence you may get complaints of people receiving emails you may never have sent
- Many send out the contents of address books



# The problems - Spam

- Unsolicited commercial email, without any identity of the sender or false identity
- Spammers have huge databases collected by various means
- It's a huge problem: some people get 90% spam
- Open Relay: A mis-configured email server which allows anyone to relay email on SMTP
  - Used by spammers, who keep looking for these
  - Eventually such a server will be “ black-listed”



# Viruses

- These are actually emails with virus infected attachments and come from other infected systems
  - The virus looks up the address book, creates an email body and attaches its program, and sends the whole email out to all addressees with a random From email id
  - Once it is opened & the attachment is **executed**, the system is infected and process repeats



# Other problems

- Databases of email servers from where spam originates (Blacklists) have come up
  - Most email servers refer to these & don't accept email connections from a listed server
- Email depends on the Domain Name Service (DNS). If DNS fails, email won't be delivered
- Often connectivity fails, and not the email service itself
- Companies/sysadmins are taking desperate measures to reduce spam



# Solutions & their problems

- Anti virus software generally deletes emails with infected attachments, without intimation
  - Desktop anti virus s/w and firewalls may block the TCP ports for email (SMTP – Port 25)
  - A genuine email but with an infected attachment could be deleted
- Your IP address could get blacklisted for various reasons, especially if it fails Open Relay tests



# Spam filtering & problems

- Spammers are intelligent people & keep changing their tactics, message patterns, etc.
- Filtering s/w uses various rules & ratings to decide if a message is spam
- False positive: A genuine message labeled as spam by the filtering software. E.g. If you deal in stocks, a lot of messages could look like spam
  - No s/w can do 100% accurate filtering



# Policy issues

- What checks should be done on incoming SMTP connections? How many to accept per minute?
- Which blacklist databases to refer to?
- Should filtering s/w intimate recipients or senders?
- Type of attachments, size & for which users?
- How to deal with emails identified as spam?  
Delete? Tag-and-send? Quarantine?



# Tips for users

- Email is insecure, contents can be read
  - Anybody can spoof a From address, beware!
  - Scan & open attachments; but never from strangers
  - Encrypt confidential information before sending
- Sometimes emails don't reach the recipients
- Bcc'd email ids aren't seen in the header
- Beware of ***phishing***: genuine looking emails from fraudsters (Ex. Getting your bank a/c info)
- Use FTP service for exchanging larger files



# Summary

- Email has reduced costs of communication; it is very fast and eco-friendly
- Unfortunately, it is based on a dated architecture and protocols. Fundamental changes are required. But the huge installed base and large corporate players makes radical change difficult
- With some sensible policies and user awareness, email is still very usable



# Thanks!

- Please send your feedback and suggestions to:
  - [connect@captain-mail.in](mailto:connect@captain-mail.in)
- Visit [www.captain-mail.in](http://www.captain-mail.in) for more information