



International Cooperation

Working together to stop spam in the AsiaPac region

APNIC 20, Hanoi

Suresh Ramasubramanian
Coordinator, APCAUCE



Spam would just go away if ...

Spam is a fact of life – it is here to stay.

- A real life analogy – pest control and sanitation, or the control of an epidemic
- Spam and other forms of content pollution are an epidemic that threatens the well being of the Internet, and its users.
- Efforts should focus on mitigation and containment of spam rather than trying to find a “solution”, for there is no single solution
- Coordinated action required, with a multi-stakeholder, multi-pronged approach that addresses short-term goals, besides implementing long-term measures aimed at the mitigation and prevention of spam.



Spam hurts the Asiapac more

- Drain on limited and expensive resources
- Local ISPs blocked as spam sources
- Software piracy a spam and security risk
- Unaware users victims of spams / scams
- Phishing, viruses, malware and other threats make users fear going online, even to access their bank website or file their income tax returns.



Multipronged, Multistakeholder Approaches

- Infrastructure, Logical, Content and Social / Developmental measures required to combat spam and cybercrime.
- Introduction of comprehensive antispam and data privacy laws
- Empowering the executive and judiciary to act against spam and cybercrime, and increase their awareness of these issues
- This helps avoid fiascos like the arrest of eBay India's CEO.
- Increased cooperation between government, industry, civil society and the general public
- Implementation by ISPs of technical measures, policies and standard operating procedures against spam
- Education and empowerment of users – currently helpless targets of spam, identity theft and other cybercrime
- A detailed treatment of this can be found in the OECD report on Spam Problems in Developing Economies



A startling lack of tangible results so far

- A few minor victories – some malefactors prosecuted, ISPs become slightly more aware about spam and cybercrime, OS and software vendors increase their product's security. Not nearly enough.
- Massive communication gaps between stakeholders is a major obstacle to coordinated action against spam.
- Several countries in the AsiaPac region now faced with an influx of foreign spammers and Internet abusers offshoring to their countries.
 - Spammers quick to take advantage of lax policies at ISPs, and a lack of antispam and privacy legislation in countries,
- Communication gaps cause spam originating from ISPs, and on the whole, from entire countries not to be noticed or mitigated.
- This allows spammers and Internet abusers to operate with impunity, and consequently leads to widespread blocking of ISPs that don't adequately address spam



Antispam initiatives in Asia and Worldwide

Law and Regulation

- Some AsiaPac countries have, or are introducing antispam laws - Australia, New Zealand, Korea etc
 - Australia has successfully prosecuted a notorious spammer, Wayne Mansfield, under their antispam law

International cooperation - governments and regulators

- Seoul Melbourne Pact on Antispam – signed by several Asia Pacific regulators. Focuses on information sharing, technical, educational and policy solutions to the spam problem
- London Action Plan – Brings together regulators from the USA, Canada, EU, AsiaPac, as well as international organizations such as the ITU and OECD, civil society antispam organizations, and industry (ISPs and vendors of antispam technology).



APCAUCE – Bringing people together against spam in the Asia Pacific Region

- Asia Pacific Coalition Against Unsolicited Commercial Email
 - Grouping of CAUCE chapters in the Asia Pac region
 - CAUCE is the world's largest volunteer antispam organization, with groups in the USA, Canada, the EU and the Asia Pac region
 - APCAUCE includes members and CAUCE Chapters from Australia, China, Hong Kong, India, Japan, Korea, Malaysia, New Zealand, Taiwan and Thailand
- APCAUCE activities include
 - Technical tutorials and conferences at APNIC, SANOG, APRICOT
 - Speakers include technologists, ISPs, blocklist operators and lawmakers
 - Annual “Regional Update” meetings that bring together regulators, governments, ISP associations and interested citizens from around the region at an informal round table discussion of antispam laws and initiatives in the region. This is an annual event held on the sidelines of APRICOT
 - Contribution of public policy papers on spam related issues to organizations such as the OECD, UNDP/APDIP and the Hong Kong regulator OFTA



ORDIG – AsiaPac iGovernance Perspective

Open Regional Dialogue on Internet Governance

- WGIG/WSIS are the platforms, ORDIG has tried to give the Asia-Pacific region some voice

ORDIG Advisory Panel

- ORDIG is advised by a distinguished Panel of Advisors from government, academia, private sector and civil society

ORDIG Partners

- principally with UNESCAP and APNIC
- with financial support from IDRC
- ORDIG has released an excellent paper and policy brief on iGovernance issues, that covers spam as well as other key issues such as IP address allocation, root server management and IDN. These are available at <http://igov.apdip.net>



The OECD Antispam Toolkit

- Produced by the OECD Antispam Task Force
- Eight pronged approach encompassing
 - Regulation
 - International Enforcement and Cooperation
 - Industry driven solutions
 - Technologies
 - Education and Awareness Programs
 - Cooperation between different groups of stakeholders
 - Spam metrics to measure the effect of antispam initiatives
 - Outreach to non OECD economies.
- Documents released under the toolkit include an Antispam law enforcement report, and paper on spam problems in developing countries by Suresh Ramasubramanian
- <http://www.oecd.org/sti/spam/toolkit/>



WSIS Spam and Cybersecurity meetings

- The ITU Strategy and Policy Unit (SPU) has brought together several stakeholders from government, regulatory authorities, industry and civil society to hold two WSIS thematic meetings.
 - Thematic meeting on Spam (July 2004)
 - Thematic meeting on Cybersecurity (July 2005)
- A consistent theme has been the emphasis on multi-pronged, multi-stakeholder approaches that are inclusive, and keep in mind other legitimate concerns, such as privacy and free speech, when implementing measures against spam and security threats.
- There is a clear call to ensure that these must coexist so that while human rights are respected, measures for privacy and free speech must not hamper antispam and cybersecurity effort.
- Representatives of developing countries, in particular Syria and Nigeria, have advocated the signing of a global MoU on Spam



International Cooperation: ISP to ISP

- ISP to ISP cooperation is essential
- Clear and accurate whois records and maintenance of postmaster and abuse mailboxes in order to facilitate communication
- Participation of ISPs in antispam workshops and network operator conferences like SANOG and APRICOT.
- Active participation in Industry groups like MAAWG and Civil Society groups like APCAUCE, that bring ISPs from around the region together
 - APCAUCE will organize a conference track on spam at APRICOT 2006 (Perth)
 - The next MAAWG meeting is from November 8-10 (Montreal, Canada)
- ISPs should group together to form Internet Exchange Points, this enables them to conserve scarce local bandwidth, on which spam and other content pollution is a heavy, and needless drain, a drain that must be plugged to ensure the safety and stability of the Internet.



International Cooperation [continued] ISPs with Industry and Civil Society

- Work together with banks, e-commerce vendors and other legitimate senders of bulk email to ensure that their email is not treated as spam, and that the email senders follow ethical email marketing rules such as “confirmed optin” mailing lists.
- Work together with civil society antispam organizations such as APCAUCE and public, volunteer run antispam block lists such as spamhaus.org, in order to take quick and decisive action on spammers who are abusing their services
- Work together with the software and give users fast access to secure computing resources (windows update, antivirus software etc) by distributing CDs to their users, or setting up local mirrors and/or Akamai clusters of software, in order to give users fast, local access to secure computing resources such as OS security updates, antivirus updates and downloads of tools to search for and remove spyware.
- Work with civil society organizations like APDIP and ISOC for user education initiatives. Chamber of commerce meetings, and joint workshops organized by various civil society organizations, are a good place for all stakeholders to work together.
- ISPs, Industry and Civil Society should work together to give coordinated inputs to the government for comprehensive antispam and privacy laws and their effective enforcement in a manner that respects free speech / privacy



What now? The immediate and foreseeable future

Several different efforts (OECD, WSIS, Civil Society, Industry)

- There is a definite need for some of these initiatives to merge their efforts, or at least to work jointly, so that their joint skills can be harnessed by working together. This also widens the outreach of these efforts, as a larger constituency of governments, organizations and people can be approached.

Startlingly effective short term results perhaps, but long term?

- Even minor increases in targeted spam filtering efforts, or a weakly drafted antispam law, may have an immediately perceptible effect on spam levels. But this may be short lived.
- Capacity building and long-term strategic thinking necessary
- OECD style antispam toolkits, integrated with a broader Internet Governance toolkit approach.
- Develop capacity and cooperation at national and regional levels, and at grassroots levels, for quick and effective results. It may be a long time before any kind of global MoU or joint action on spam makes its efforts felt.
- APCAUCE and ORDIG are well placed to use their expertise in regional antispam and iGovernance issues, as well as their wide outreach in the Asia Pacific region, to play a coordinating and facilitating role in this process.



Q?
A!

Suresh Ramasubramanian
Coordinator, APCAUCE
Manager, Antispam Operations, Outblaze
suresh@outblaze.com



Filtering Millions Of Mailboxes

Capacity & Performance Lessons

suresh ramasubramanian

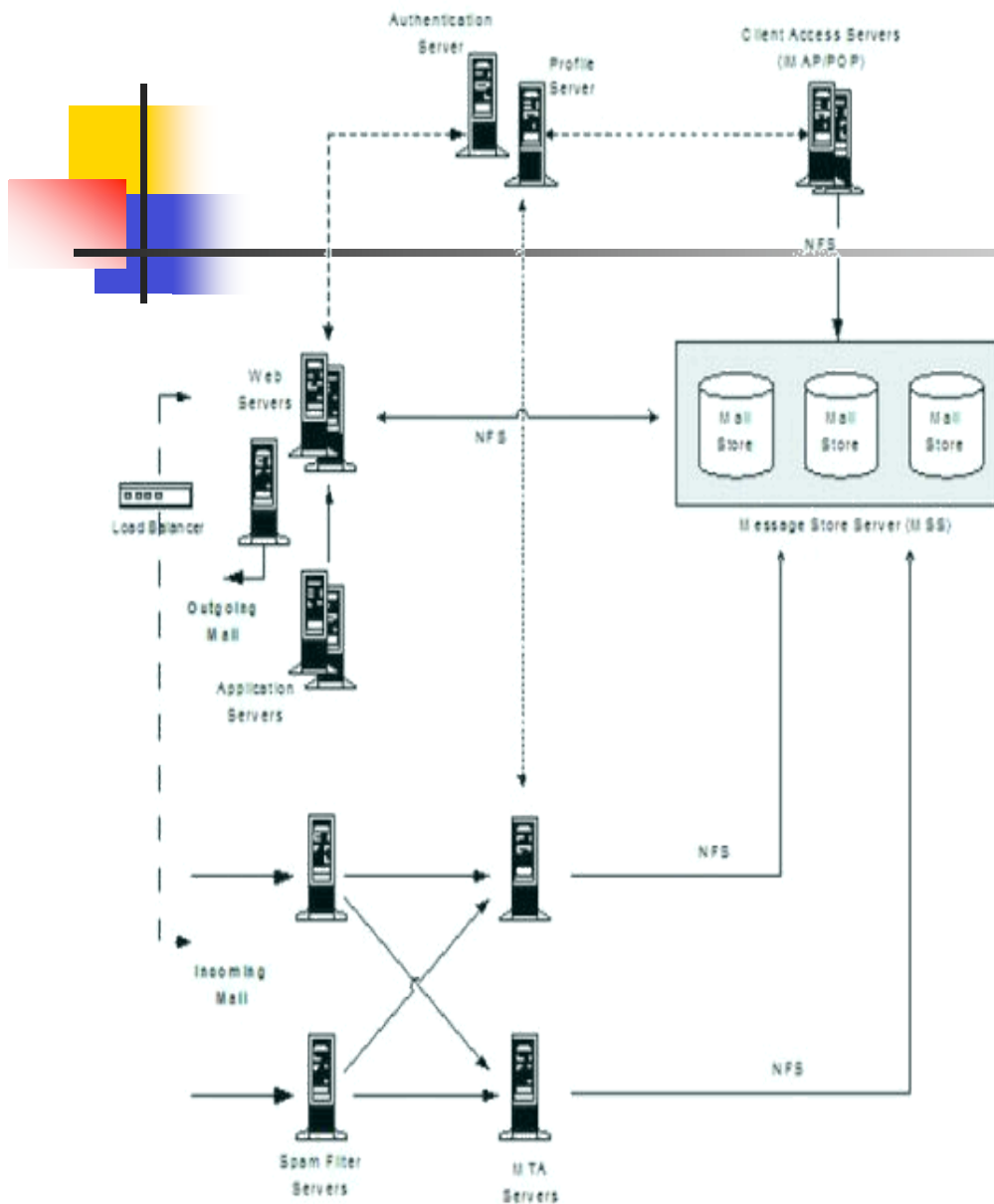
manager, antispam ops

<http://www.outblaze.com>



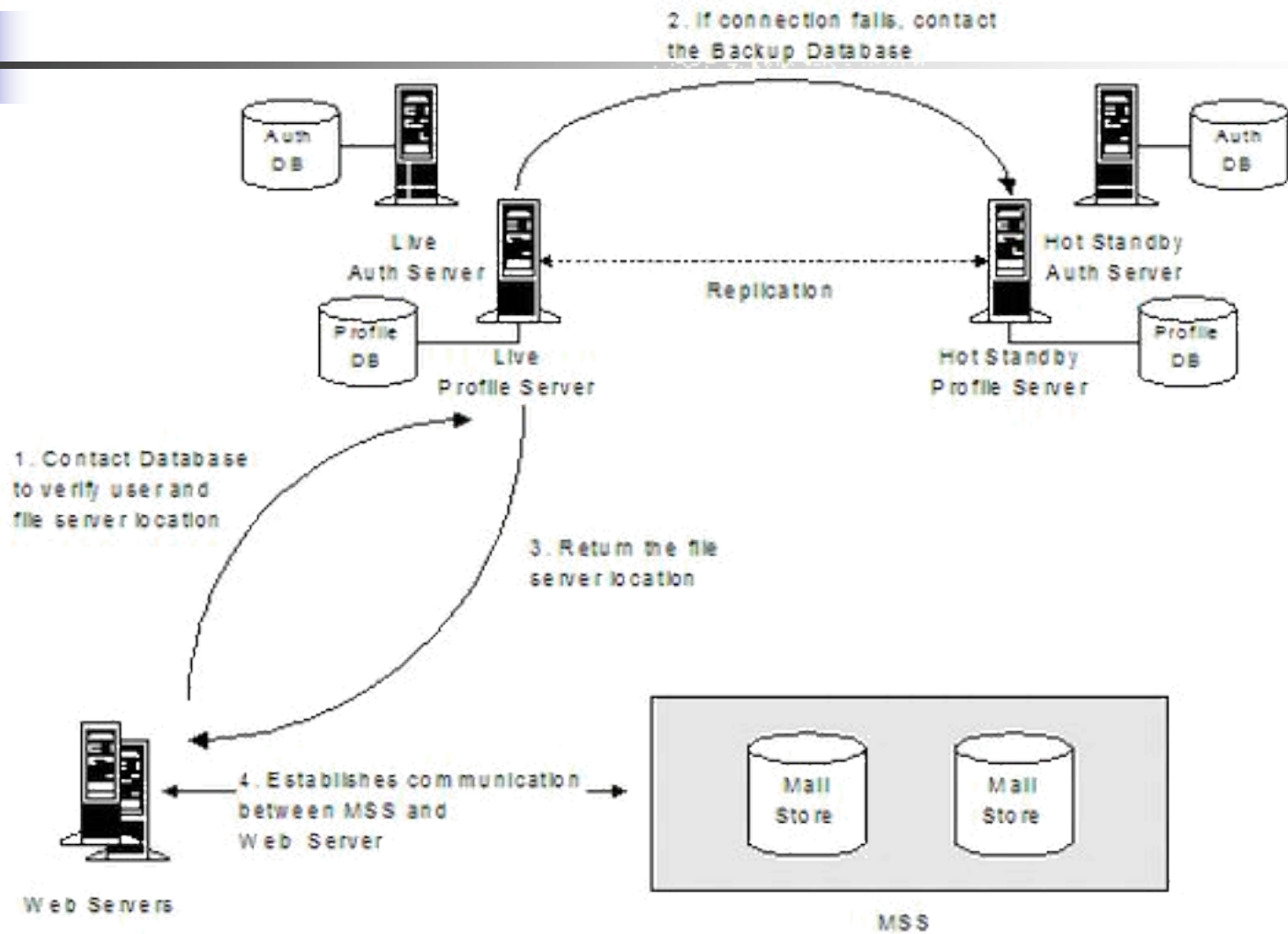
About Outblaze

- Hosts domains such as lycos.com, mail.com.
- 40 million mailboxes and counting.
- Mail system spread over two continents (North America and Asia).
- Multi-tiered, robust scalable mail architecture built with open source components.



- Inbound mail handled by a large cluster of linux mail gateways running postfix.
- Initial filtering for valid users, DNSBLs, HELO, viruses etc done at the mail gateways
- Mail is passed on to second tier MTAs (again postfix + linux) for delivery.
- MTAs have NAS devices mounted over NFS
- NAS stores hashed maildirs for user mail / user defined filters storage.
- Client interfaces (webmail, pop3 / imap and smtp auth servers) also access the filers using NFS.

Database Servers





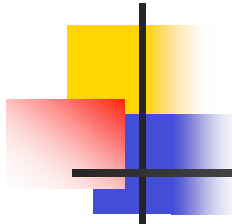
More on inbound email

- After filtering at the gateways, mail is rapidly moved out to
 - MTA servers (for local mailboxes).
 - External destination (for forwarding users).
- This keeps the gateway mail queues uncluttered, and mail flow uninterrupted.
- Deferred mail on the gateways is shunted out to a set of fallback mailservers. These are usually deferred mail to an external destination, or undelivered bounces.
- Analysis of the mail queue in the fallback mailservers:
 - helps catch mail delivery problems.
 - identifies candidates for our filters.



Webservers

- Application servers run a custom webmail interface
 - Coded in perl, runs on apache.
 - Squid used as a http accelerator.
 - Captcha to prevent automated signups
- Proxy servers (stripped down mod_perl powered apache servers) serve the signup and landing pages.
 - Only required libraries loaded, so the proxy's engine has 30% of the memory footprint of our application servers.
- Image servers (thttpd) - millions of requests for static image content.
- User maildirs accessed over NFS from NAS devices.
- Webservers run postfix for outbound email.



DNS

- Nameservers in USA / Asia (bind)
- Each cluster has dedicated resolver servers, backed up by local installs of dnscache on individual servers.
- Internal spam blocklist served across our network of MXs using rblDNS.



Spam filtering - inbound

- Selected blocklists imported using rsync / AXFR from external sources and served locally using rblDNS.
 - Spamhaus SBL/XBL, ORDB, SORBS DUHL
- Locally blocked IPs obtained by -
 - Spam trap analysis
 - Analysis of email marked as spam by users
 - Log parsers looking for spam like patterns
 - suspect HELO, multiple emails with from: freemail, but not from that freemail service's IP space, etc.
 - Relaytests of IPs that make SMTP connections to our MX and trigger a spam pattern



More spam filtering

- Suspect HELOs blocked “at the gate”
 - HELO our.own.domain, our.own.IP
 - HELO freemail but connecting IP doesn't have that freemail's reverse DNS
- Step Detector to auto-upgrade our IP blocks
 - any /24 that has more than a certain number of IPs blocked is flagged for blocking the entire /24
- Brand new domains that suddenly send huge volumes of email flagged for blocking.



Spam filtering - outbound

- Postfix on web servers does body filtering to catch spam runs in progress.
- All outbound mail is sent through an outbound mail filtering system (spamassassin).
- Mails are scanned for known bad strings (urls of sites advertised in spam).
- Accounts that send a sufficient number of caught emails are terminated.
- Checked mails are sent to an outbound postfix relay for final delivery.

Thank you.

