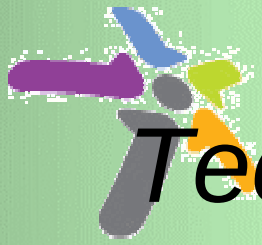


Technical Approaches to Spam and Standards Activities (ITU WSIS Spam Conference)

John R. Levine, Chair

IRTF Anti-Spam Research Group

ituwsis@taugh.com

+1 607 330 5711

Taughannock Networks

Overview

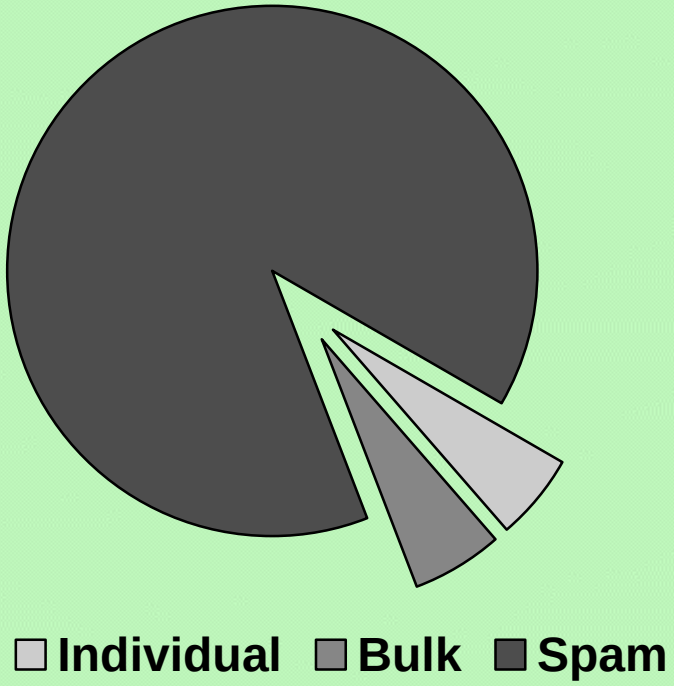
- **The e-mail landscape**
- Technical filtering possibilities
- Standards activities

The e-mail landscape

- ≈100 billion messages / day
  - 50% to 95% spam
- Millions of senders and receivers
- **Scaling** is a critical issue

At one large provider

- 150M individual messages / day
- 150M legitimate bulk messages / day
- Over 2000M spams / day



Taughannock Networks

E-mail infrastructure

- Very decentralized
- No chokepoints other than perhaps DNS
- Mail directly from server to server

E-mail delivery

- No prior arrangements
- Doesn’t match national boundaries
- Doesn’t match network boundaries
- Often doesn’t match administrative boundaries

E-mail users

- Users all over the world
  - Dialup and broadband ISPs
  - Via employer network
  - Mobile phones and Blackberry
  - Libraries, cyber cafés, WiFi hotspots
- User numbers
  - 1000M? Nobody really knows
  - Large mail systems have >100M mailboxes

User profiles

- As varied as telephone users
- Wide range of incomes, language, experience, and technical expertise

Overview

- The e-mail landscape
- **Technical filtering experience**
- Standards activities

Filtering points

- Manage untrustworthy senders
- Evaluate the source
- During receipt
- After receipt
- At delivery

Sender time filtering

- Port blocks
- Sender authentication e.g. SMTP AUTH
- Rate limiting
- Filter as though receiving
  - These work well but are moderately disruptive

Receipt time source filtering

- Mechanical DNSBLs
  - Open relay, proxy, spam trap, ...
- Untrustworthy senders (dialups)
- Shared reports (Spamcop)
- Spam sources (SBL, MAPS RBL)
  - DNSBLs have wide quality range
- DNS “poisoning” forward/backward
  - Defensive move against worst spammers

Per-Message Content filtering

- Protocol defects: Reverse DNS, SMTP errors
- Header analysis: Sender white/blacklists, header defects, …
- Body strings (fixed or adaptive/Bayesian)
- "Spammy" behavior (hashbusters, …)
  - Can be effective, spammers try hard to defeat

Message stream filtering

- Bulk counting (DCC)
  - Need to whitelist valid bulk
- Shared denouncements (Razor, Spamcop)
  - Depends on quality of reports

Hybrid filtering

- Combine any and all of the others
  - Spamassasin
  - Mailshield
  - Many others
  - Add-ons to MTAs and home-brew

Sender identification

- PGP, S/MIME signatures
- Real time mail-back
- Challenge/response
- Source authorization
- Trusted sender schemes

Per-correspondent addresses

- Disposable addresses for untrustworthy correspondents
- “Channel” addresses to identify correspondents and sort mail
- The introduction problem

John R. Levine, Chair
IRTF Anti-Spam Research Group
ituwsis@taugh.com
+1 607 330 5711

Taughannock Networks

Postage schemes

- Computational Hashcash
- E-postage
  - Micropayments
  - Attention bonds
- All have identity/authentication problems
- E-postage has infrastructure and fraud problems

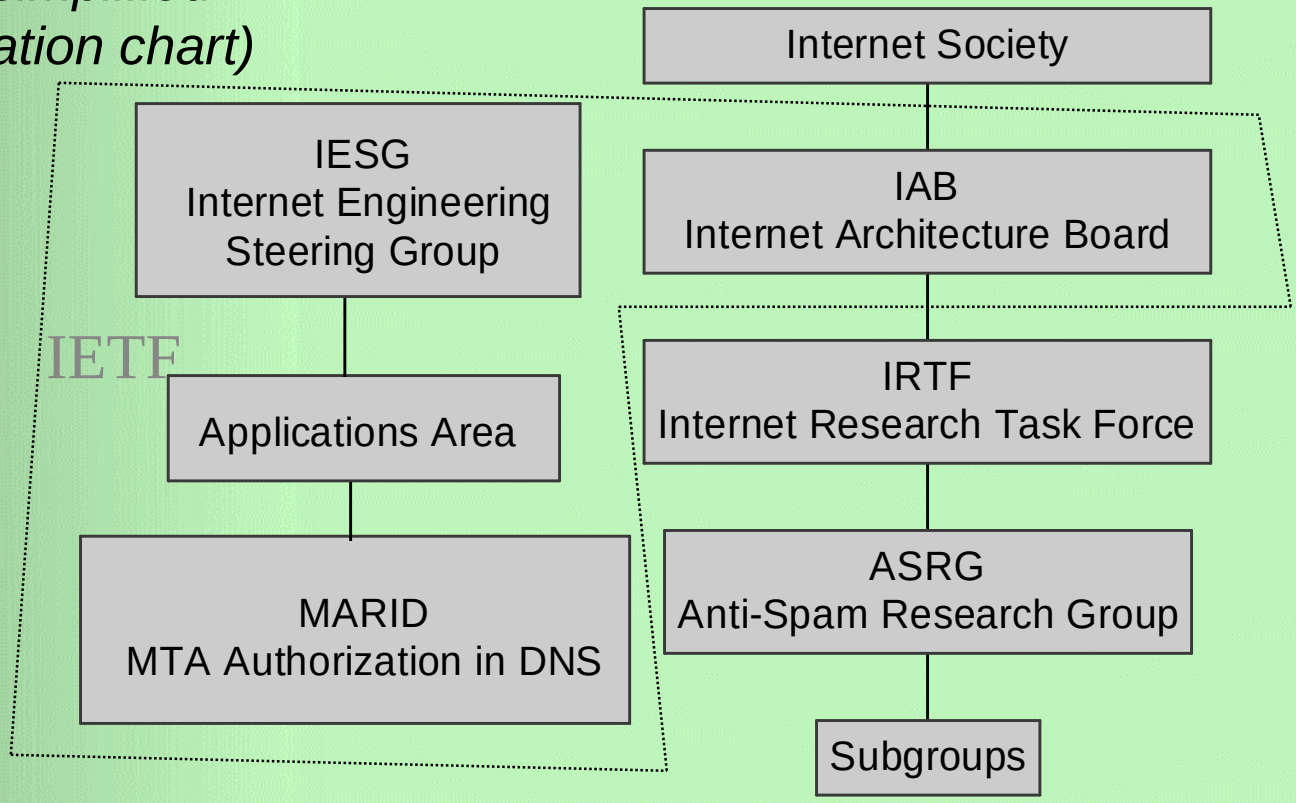
Taughannock Networks

Overview

- The e-mail landscape
- Technical possibilities
- **Standards activities**

ASRG and MARID

(Oversimplified organization chart)



Taughannock Networks

Anti-Spam Research Group

- Rechartered in late 2003
- Multiple subgroups
- No budget, works by e-mail
- Members participate as individuals

ASRG subgroups

- Lightweight Mail Authentication (LMAP)
  - Work passed to MARID
- Abuse reporting
- Filtering standards
- Identity, Authentication, Reputation (IAR)
- Other inactive subgroups

IETF MARID

- Charged with DNS based authentication
- Very aggressive schedule
  - Hope to have a draft standard by late 2004
- Sender ID
- CSV

Sender ID

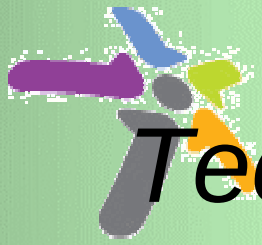
- Combines SPF (M. W. Wong et al.) and Caller ID (Microsoft)
- Validates message sender's address via originating IP address
- Technically straightforward
- Debatable effectiveness and "collateral damage"
- Needs reputation system

Client SMTP validation

- CSV developed by D. Crocker, J. Leslie et al.
- Validates sending mail host
- Debatable effectiveness, less collateral damage than Sender ID
- Also needs reputation system

Future work

- Domain keys, TEOS, and other message validation
- Reputation and accreditation systems



Technical Approaches to Spam and Standards Activities (ITU WSIS Spam Conference)

John R. Levine, Chair

IRTF Anti-Spam Research Group

ituwsis@taugh.com

+1 607 330 5711

Taughannock Networks