Spam:  Ready, Fire, Aim!

APCAU CE / APRICOT
Kuala Lumpur - 2004

Dave Crocker
Brandenburg InternetWorking
<http://brandenburg.com/current.html>
Spam is complicated and simplistic solutions will be damaging

- Email is more complex than people usually realize
- Spam is a social problem
- Technical solutions need to follow the social assessment
- No single action will eliminate it and nothing will “eliminate” it

- After working on email for 30 years
  - I feel a bit proprietary about it
What We Will Discuss

- The problem
- Our reactions to it
- Technical environment
- Proposals
- Making choices
This? Oh, this is the display for my electronic junk mail.
We Do Have A Problem!

- We do not need to cite statistics
  - It is clear we have a dire problem now!
  - It is clear the situation is getting worse, quickly
  - It is like moving from a safe, small town to a big (U.S.) city
- Nothing has yet reduced global spam!

- We must distinguish
  - Local, transient effects that only move spammers to use different techniques, versus
  - Global, long-term effects that truly reduce spam at its core
Dangerous Logic

“...but this is urgent!!”

- “We have to do something now!”
  (Ignore any side-effects, or dismiss them as minor.)
- “Maybe it’s not perfect...
  but at least we’re taking some action!”
- “What have we got to lose?”
- “At least it reduces the problem...
  for now.”
- “We must replace SMTP...
  even though we don’t know what we want to do
- “We can do something in the interim...”
Hysteria Also Can Destroy Email

- 30 years of experience making Internet changes
  - Risky, difficult, expensive and slow
  - Always has unintended consequences (usually bad)
  - Service providers have highly variable operations
  - Changes to infrastructure require caution!

- Changes need to produce direct benefit
  - Directly affect key problem or directly improve service
  - Orchestrated inter-dependent changes do not work
Control of spam
- Cannot be “surgically” precise
- Must balance the wheel
- Needs range of partial solutions
- Different techniques for near-term vs. long-term, except that near-term never is

Heuristics
- Long lists \(\rightarrow\) complicated
- Complicated \(\rightarrow\) Be careful!
But What Is Spam, Exactly?

And why do we still need this slide?

- Still no pragmatic, community definition!
  - Unsolicited commercial or bulk
  - Anything I don’t want
  - Anything you don’t want me to receive(?)

- How can we formulate Internet-wide policies
  - When we cannot formulate a common, Internet-wide definition?

- Try a pragmatic approach
  - Focus on core, identifiable characteristics
  - Ignore the rest, for now

- For example, specify
  1) Type of targeted spam
  2) How it is occurring
  3) How the mechanism will fix the problem
  4) Dependencies, before mechanism will work

And why do we still need this slide?
Different Spammers

Different responses

- “Accountable” spammers
  - Legitimate businesses engaging in aggressive marketing
  - Need formal rules to dictate constraints

- “Rogue” spammers
  - Actively avoid accountability
  - Likely to always have “safe haven”
  - Not always seeking money
  - Need to treat them like virus and worm attackers
Email is **Human** Messaging

- Richly diverse
  - Content
  - Authorship
  - Sources
  - Patterns of use
- Spontaneous
  - Serendipitous
- Timely
- Do not assume precise
  - Usage scenarios
  - Access
  - Tools
  - Service operations
- Do not penalize legitimate users
- Or, at least, keep the pain to a minimum

D. Crocker

APCauce/Apricot – KL, 2004
Email Points of Control

Price
Accountability
Filtering
Enforcement

Filtering

Originator
User Agent

Receiver
User Agent

Origin Mail
Transfer Agent

External Mail
Transfer Agent

External Mail
Transfer Agent

Receive Mail
Transfer Agent

Proactive Controls – Prevention

- Accountability
  - **Content**: Sender/author
  - **Mail**: Sending MTA
  - **Access**: Sending provider

- Access provider controls
  - **Rate-limit**
  - **Limit outbound ports** (e.g., SMTP’s 25)
  - **Redirect through authorized MTA’s**
  - **Too intrusive and too much inconvenience for legitimate senders?**
Proactive Controls – Prevention

• Charging – Sender pays fee
  • Some vs. all senders
  • How much?
  • Who gets the money?

• Enforcement – Laws and contracts
  • Scope of control - national boundaries?
  • Precise, objective, narrow?
Constituencies in the debate

- **Business providers:** Legitimate need
- **Direct marketing:** Legitimate need (?)
- **Service providers:** Reduce complaints/cost
- **Outraged consumers:** Reduce hassles/cost

Core social principles

- Careless laws alter society and defeat the goal
- Consider complexity of English plug/socket...
# Accountability

## Levels

1. **Identity**
   - A label
   - What the label refers to

2. **Authentication**
   - Validate the identity
   - Who is doing the validation

3. **Reputation**
   - Predict behavior, using history & opinion of others

## Real world systems

- **Friends, colleagues**
- **Third-party service**
  - Trust the rating service?
  - Like credit-reporting
- **Yourself(!)**
  - E.g., pre-authorize email receipt, after purchase

---

D. Crocker

APCauce/Apricot – KL, 2004
Authentication

Channel chain-of-trust
- Trust via each handling entity
  - SSL/TLS
  - PPP login
  - SSH
- Works well for point-to-point

Object origin validation
- Message validated
  - Channel is irrelevant
  - S/MIME, PGP
- Works well for store-and-forward
Security Models

**Object**
- Secure Mail
- MTA
- MTA
- MTA
- Secure Mail
- Secure Mail

**Channel**
- Mail
- Secure MTA
- Secure MTA
- Secure MTA
- Secure MTA
- Secure MTA
- Secure MTA
- Secure MTA
- Mail
- Mail
- Mail

D. Crocker
Reactive Controls – Filtering

Detection
- **Source:** Good/Bad sender
- **Destination:** Honey pot, attracts spammers
- **Content:** Advertising, pornography
- **Aggregate traffic:** Massive bulk mail flow

Action
- Divert, delete or return
- Label and deliver
- Notify administrator
# Source Information

<table>
<thead>
<tr>
<th>Type</th>
<th>Meaning</th>
<th>Current Validation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MTA IP</td>
<td>SMTP client</td>
<td>Net validates address</td>
</tr>
<tr>
<td>EHLO Domain</td>
<td>SMTP client</td>
<td>DNS match actual IP</td>
</tr>
<tr>
<td>Provider IP</td>
<td>Site of SMTP client</td>
<td>DNS in-addr.arpa</td>
</tr>
<tr>
<td>Mail-From</td>
<td>Bounces address</td>
<td>None</td>
</tr>
<tr>
<td>From</td>
<td>Author</td>
<td>None</td>
</tr>
<tr>
<td>Sender</td>
<td>Posting agent</td>
<td>None</td>
</tr>
<tr>
<td>Received</td>
<td>Handling sites</td>
<td>None</td>
</tr>
</tbody>
</table>
**Proposals – Out of Band**

- Legal efforts define
  - Common use of term “Spam”
  - Requirements when sending classes of mail
  - Remedies for violations

- Administration
  - Exchange filtering rules
  - Exchange incident (abuse) reports
  - Are abuse desks used, useful?
Proposals – Authentic Channel

MTA Registration

Presumed-Author
- MTA IP registered with
  - Mail-From domain
  - EHLO domain
- Registration in DNS
  - New record, or TXT
  - Simple authentication, versus “policy”
- Proposals
  - RMX, SPF, LMAP, DMP, DRIP, FSV, Caller-ID

Provider Network
- MTA IP registered with net hosting it
- Registration in DNS
  - in-addr.arpa
  - New record
- Proposals
  - MTA Mark, SS
Proposals – Authentic Content
Certify the author

Classic Authentication
- S/MIME – OpenPGP
  - Classic public key service
  - Message content only
- Challenge-Response
  - Block until response to challenge received
  - Patented

Good-Guy
- Validate identity
- Certify reputation
- Proposals
  - Challenge-Response
  - Project LUMOS
  - TEO S
  - DomainKeys
Evaluating Efficacy

Look with a very critical eye!

- **Adoption**
  - Effort to adopt proposal
  - Effort for ongoing use
  - Balance among participants
  - Threshold to benefit

- **Impact**
  - Amount of Net affected
  - Amount of spam affected

- **Robustness**
  - How easily circumvented

- **Test scenarios**
  - Personal post/Reply
  - Mailing List
  - Inter-Enterprise
Evaluating OA&M

* Operations impact on…
  * Adopters of proposal
  * Others

* Internet scaling – What if…
  * Used by everyone
  * Much bigger Internet
  * Individual vs. Group use

* System metrics
  * Cost
  * Efficiency
  * Reliability

Look with a very critical eye!
Spam is a complicated topic
- It needs to be treated with all due respect

- Many factors, proposals, and constituents
  - Complicated considerations and effects

- On the Internet, interim never is
  - Deploy strategic solutions