RE: Reliable Email
Scott Garriss, Michael Kaminsky, Michael J. Freedman, Brad Karp, David Mazières, Haifeng Yu

Paper Presentation
Justin Ho
## Current Spam Protection

<table>
<thead>
<tr>
<th>Method</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Content filtering/rejection</td>
<td>What the computer thinks</td>
</tr>
<tr>
<td>Central database (DNSBL, human labour)</td>
<td>What someone else says</td>
</tr>
<tr>
<td>DNS Records (SPF/SenderID)</td>
<td>What the domain owner says</td>
</tr>
<tr>
<td>Digital signing / Computational Puzzle</td>
<td>What the email says</td>
</tr>
</tbody>
</table>
The Fight Against Spam

- PGP
- Computational puzzle

DNS Server

DNS Blacklists

Content filtering

Machine learning

SP
Getting the User Involved

- Leverage existing social networks
- What’s necessary?
Design Goals

- Prevent sender address forging
- Prevent attestation forging
- Maintain privacy while determining white list intersections
- Incremental deployability
RE: System Design

Friends List: C, -, -

Friends List: enc(C, D, E)
Results

Accuracy Rate

- 20 million messages, 172 identified false positives
- Direct RE would reduced to 28 false positives (84%)
- With FoF would reduced to 19 false positives (additional 5%)
**Results**

**Processing time of FoF**

- Intersection of two sets of 160 = 40s computation
- Most processing done by sender
Results

Worst case

- “3 GHz Xeon in 64-bit”? RAM? Disk I/O? Email queue lengths?
- Hotmail: 12 billion emails daily, over 130,000 servers
- Assume half are sent emails, requiring FoF 40s × 6 billion emails over 130k servers = 21.36 days of processing per server

![Diagram showing computation time vs. sender input size for different recipient input sizes.](image)
## Limitations

| Mailing lists or emails to multiple recipients | - Token to each recipient  
|                                            | - List moderation |
| False attestations cause false negatives    | - Require password to generate attestation? |
| Friend-Of-Friend Only                      | - How to move beyond 2 degrees of separation? |
What’s Wrong with PGP?

Find me the path from [ ] (eg 27141BB0) to [ ] (eg 5B430367).  

(ie find a set of keys such that ‘from’ signs key x which signs key y which signs key z which signs ‘to’, so that it may be possible for someone who trusts key ‘from’ to trust key ‘to’ to some extent.)

Pathfinder news is now on its own page here.

The pathfinder uses the key database of the key server running on the.earth.li (aka wwwkeys.uk.pgp.net). If you have any problems then please contact me on the address below.

Please be patient when waiting for results - don't click Find Path several times just because it's taking a while to respond as this puts extra load on the server. If people continue to do this I'll have to take the service down for the moment.
What’s Wrong with PGP?

Paths from Key 0xDD934139 to Key 0x7B7AE5E1
Email forwarding and multiple addresses

Unknown User

Justin

jho@cs
AS, bad spam filter

user@gmail.com
AS, good spam filter
Limitations

Privacy Problems?

Claim Z is a friend
RE: Reliable Email?

- Authentication implies reputation which allows for spam protection
  - PGP already provides web of trust - RE just allows decentralization
- Discussion about revocation was vague
- Cost of processing is too high
- Other works have cited privacy problems