The Business Case for DomainKeys Identified Mail

Andy Spillane
Vice President, Yahoo! Mail

February 13, 2006
Fighting Spam & Email Abuse Requires a Multi-Faceted Approach

DomainKeys Identified Mail is part of a multi-faceted approach to protect consumers against spam and phishing scams.

- **Industry collaboration efforts**
  Cisco, Sendmail, PGP, AOL, IBM, and others worked together to submit DKIM to IETF

- **Legislation and litigation**
  CAN-SPAM; numerous lawsuits against spammers from Yahoo! & others

- **Increasing consumer awareness**
  Consumer information available at
  [http://antispam.yahoo.com](http://antispam.yahoo.com) and [http://security.yahoo.com](http://security.yahoo.com)

- **Enhanced technologies**
  Content filters, virus protection, sender reputation, and accreditation
The State of Email – Market Situation

Worldwide Estimates
[Radicati Group]

<table>
<thead>
<tr>
<th></th>
<th>2006</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Traffic</td>
<td>171B</td>
<td>331B</td>
</tr>
<tr>
<td></td>
<td>msgs/day</td>
<td></td>
</tr>
<tr>
<td>Email Installed base</td>
<td>1.4B</td>
<td>2.2B</td>
</tr>
<tr>
<td>mailboxes</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Original design makes email forgery & spoofing easy for spammers
- Phishing & online identity theft are the most egregious types of email abuse
The Proliferation of Phishing Attacks

Gartner Study: Increased Phishing and Online Attacks Cause Dip in Consumer Confidence (6/05)
- 2.42 million US adults report losing money due to phishing attacks
- In 2004 and 2005, 11 million phishing e-mail recipients clicked on the links
- More than 80 percent of online consumers say that their concerns about online attacks have affected their trust in e-mail from companies or individuals they don’t know personally.

Forrester Study: Phishing Spreads Among Consumers (9/05)
- 14,000 phishing attacks were reported to the Anti-Phishing Working Group from April to Sept 2005
- According to the APWG, the number of unique key logging Web sites increased 125% from April to Sept 2005
- 86% of phishing attacks target the financial services industry
Why Yahoo! Mail is Involved

• Yahoo! Mail is the largest webmail provider in the US and in the world
  – 67MM US monthly unique users [comScore MediaMetrix]
  – 231MM WW monthly unique users [comScore MediaMetrix]

• Yahoo! provides email for:
  – SBC/AT&T
  – Verizon
  – British Telecom
  – Rogers Cable
  – 100,000s of small business and personal domains
  – and more
Sender Reputation Based on IP Address Has Proven Problematic

- **Maintenance**
  - IP addresses change over time; changes aren’t communicated; occasionally changes aren’t even realized by senders
  - Mailbox providers end up relying on end-user reports

- **Email Service Providers and shared IP addresses**

- **Forwarding**
  - 80% of forwards traffic is spam
  - Extremely hard to distinguish legitimate forwarded mail from forgeries
  - Mailbox providers are between rock/hard place
    - protect user from phishing & other forgeries or yield false positives
  - Very significant amount of marketing mail gets legitimately forwarded
    - Yahoo!, EarthLink, Comcast, Juno, Mail.com, SBC, …

- **Users don’t know or care about IP addresses**
- **Marketers don’t care about IP addresses**
• DomainKeys was developed to solve these issues
  – Low maintenance for both sender and mailbox provider
  – Many domains can share the same IP address without sharing the same reputation
  – Survives forwarding
  – Users know about domains
  – Company’s domain is (or should be) a prime brand attribute to marketers
Key Benefits of DomainKeys

- Mailbox provider can measure the correct reputation
- Mailbox provider can help you protect your brand
- Reduce sender reputation maintenance
- Protect email users from forgery
Implementation Costs of DomainKeys

• CPU Cost:
  – Sendmail study shows 8-16% mail server software CPU increase
  – Several major mailbox providers & senders have not needed to add additional hardware

• Several royalty free software implementations available
  – E.g., http://domainkeys.sourceforge.net

• ESPs are beginning to implement

• DNS – infrequent updates required
Implementation Costs: Licensing

• Patent license designed to allow freedom to operate, while protecting the industry
  – Royalty free
  – Sub-licensable
  – Perpetual
  – No registration required

• Alternatively, GPL (GNU General Public License) is also available
How Yahoo! is using DomainKeys

- Signing and verifying email using DomainKeys
- Expect to begin using DKIM as specification stabilizes
- Showing positive verification results to users

- Skipping some antispam filters
  - Especially forgery detection
  - Filters that get fooled by forwarding most often
  - Not guaranteed inbox delivery!
- Working on providing complaint feedback loops for signed mail
- Continued integration into sender reputation systems
Domains from which Yahoo! has received a DomainKeys signed email
More information and specification:
http://antispam.yahoo.com/domainkeys

Tools for deployment
http://domainkeys.sourceforge.net