Email Trust
Does Not Look for Miscreants

Dave Crocker
Brandenburg InternetWorking
bbiw.net

SF INET – 7 May 2010
Mistrust vs. Trust

Receiver is on their own:
Forced to make guesses

Sender/Receiver collaboration

Mistrust

Trust
What is DKIM for?

* Means a message is not spam
* Guarantees delivery
* Puts a domain name on a message
* Validates a message
* Authenticates the author or origin of a message
* Authenticates the sender of a message

What DKIM really does

* Allows an organization to claim responsibility for transmitting a message, in a way that can be validated by a recipient.
* The organization can be the author's, the originating sending site, an intermediary, or one of their agents.
* A message can contain multiple signatures, from the same or different organizations involved with the message.
Differential Handling, with Trust as a Component

<table>
<thead>
<tr>
<th>Stream Risk</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td><strong>BENIGN:</strong> Moderate filter</td>
<td><strong>DILIGENT:</strong> Mild filter</td>
<td><strong>PRISTINE:</strong> Accept</td>
</tr>
<tr>
<td>Medium</td>
<td><strong>UNKNOWN:</strong> Strong filter</td>
<td><strong>TYPICAL:</strong> Targeted filter</td>
<td><strong>PROTECTED:</strong> Accept &amp; Contact</td>
</tr>
<tr>
<td>High</td>
<td><strong>MALICIOUS:</strong> Block &amp; Counter</td>
<td><strong>NEGLIGENT:</strong> Block</td>
<td><strong>COMPROMISED:</strong> Block &amp; Contact</td>
</tr>
</tbody>
</table>
Trust Service Architecture
Identifying Mail Streams

- An organization has multiple “types” of mail
  - Corporate
  - Transactions (purchase order, order confirmation...)
  - Proposals
  - Marketing mass mailings
  - Customer Support

- Label them with different DKIM d= subdomains to help receiver

- Allow different reputations to develop
Different and Complementary

- **Mistrust**
  - Bayes, Blacklists, etc.
  - Look for mail to **reject**

- **Trust**
  - DKIM, SPF, Whitelists
  - Look for mail to **accept**