The Hard(er?) Problems

Phillip Hallam-Baker
Comodo Group Inc.
### 'Four' Box Model

<table>
<thead>
<tr>
<th></th>
<th>Overt</th>
<th>Covert</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Traffic</strong></td>
<td></td>
<td>Increase Work Factor</td>
</tr>
<tr>
<td><strong>Meta</strong></td>
<td>Make Attack Visible</td>
<td>Prevent Compromise</td>
</tr>
<tr>
<td><strong>Content</strong></td>
<td>Make Attack Visible</td>
<td>Prevent Compromise</td>
</tr>
</tbody>
</table>
Blocking Constraints

- **Usability**
  - Security must not require extra effort
    - [And can't make sending insecure email harder]
  - Security must make sense
    - User has to think they understand what is going on

- **Business model**
  - Infrastructure must have a business model

- **Viral Marketing**
  - Chicken and egg problem before critical mass
Defeating Traffic Analysis?

- Routers must see routing information
  - Can't protect at IP layer
  - How about
    - encrypting hop by hop
    - Flood fill all lit fiber with encrypted bits
Message Security

• Asynchronous is harder than Synchronous
  – Recipient can't provide keys in-band

• Email Problems:
  1 Send encrypted email to people we know well
  2 Send encrypted email to a stranger

  – Don't insist that we solve 2 to solve 1!
The Trust Problem

• Can't be solved without infrastructure
  - Can we fuse PGP and S/MIME trust models?
  - Can we do better?

  - Work factor analysis

  - What should the work factor be?
    • GDP of adversary $\times$ 100 years
    • Global military budget / Number of Internet users