Adding Humans to Trusted Email

Chris Masone (PhD candidate)  www.cs.dartmouth.edu/~cmasone/
Sean Smith  (PI)  www.cs.dartmouth.edu/~sws/

ABUSE (Attribute-Based Usefully Secure Email)

- Explore the ways in which humans currently build trust during contingencies
- Develop a system to allow users to employ these methods over electronically mediated channels

Signed email says too little!

What is the right way to specify human trust relationships digitally?

How do we present this information in a clear and unforgeable manner?

Will allowing humans to both specify and interpret trust relationships result in a more usable and therefore more effective system?

**In the real world:** 2003 blackout phone transcripts give many examples of users exchanging data across facilities

Power grid operators leverage social connections in crises to perform sensitive tasks

Authentication relied on contextual cues and voice recognition -- inapplicable in email/IM

### Approach and Impact

<table>
<thead>
<tr>
<th>Starts with an identity PKI</th>
<th>Using relationships for ad-hoc authorization goes beyond this app</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use proxy certs to carry attributes</td>
<td>- Who is allowed to speak for the Dean?</td>
</tr>
<tr>
<td>Users sign attribute assertions about each other</td>
<td>Focusing security work on building systems to fit the users</td>
</tr>
<tr>
<td>• “Worked for me at MISO”</td>
<td></td>
</tr>
<tr>
<td>• “Was in my class at UIUC”</td>
<td></td>
</tr>
<tr>
<td>Senders bind assertions to outgoing messages</td>
<td>• Make the trust assertions match the human system, rather than the other way around</td>
</tr>
<tr>
<td>Receivers decide whether assertions lead to trust</td>
<td>• Get humans in the loop on both ends</td>
</tr>
</tbody>
</table>

### Evaluation:

We have identified real-world scenarios from the 2003 blackout phone transcripts that demonstrate users building informal chains of trust to access sensitive information or to get potentially dangerous actions taken on their behalf.

We simulate these power grid disaster scenarios

The subject receives a simulated message asking her to perform some potentially dangerous action to mitigate this crisis.

- In some cases, this message is from a trustworthy (but unfamiliar) source.
- In others, this message is from an attacker.

Rewarded if she fixes the problem, but punished if she accepts the request of an attacker

Subjects in our study are divided into three groups: the first receives simulated plaintext email; the second, simulated S/MIME signed messages, and the third, ABUSE-enhanced digitally signed messages.

**Next steps:** analyzing transcripts to discover delegation chain-length and frequency of cross-organization delegation/information disclosure; analyzing ABUSE using Cranor’s “humans-in-the-loop” framework.