A Comparison of PGP, IBE, and Password-based Secure Email

Scott Ruoti
Jeff Andersen
Tyler Monson
Daniel Zappala
Kent Seamons
https://isrl.byu.edu

What’s the right key management philosophy for grassroots adoption?

- Usable, secure email is still an open problem
- There has been significant progress in key escrow-based systems
  - Can PGP be made equally usable?
- We conducted an A/B comparison of key management approaches
  - PGP, IBE, passwords
  - First A/B usability comparison of key management in secure email

Seeking to identify inherent usability differences between each key management philosophy

Methodology

- Paired-participant [1]
- Within subject
- Participants collaboratively learn how to use secure email
- Gather quantitative and qualitative data
- 94 participants; 47 pairs

MessageGuard

Secure Compose

PGP Key Discovery

Whoopee! One or more of your recipients hasn’t installed MessageGuard yet. Click here to send them a message requesting that they install MessageGuard.

Once your recipient has installed MessageGuard, you will be able to encrypt messages for them. In the meantime, feel free to close this message and it’ll be saved as a draft.

Secure Read

Password Entry

In-line, Context-Sensitive Tutorial

Participation

- All three systems highly rated by participants
- Our systems out-performed other similar systems [1]
- PGP can be made usable for novices!

Results

Table: Participants’ Favorite System

<table>
<thead>
<tr>
<th>Percentile</th>
<th>Sender</th>
<th>Recipient</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>40</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>60</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>80</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

PGP

- Public key cryptography
- Recipient needs to generate a key pair before they can receive secure email
- Our implementation focuses on usability
  - Automatic discovery of public keys
  - Private key not password-encrypted

Identity-based Encryption (IBE)

- Public key cryptography
  - Email address = public key
  - Private keys managed by a key server
  - Recipients don’t need to do anything before they can receive secure email

Passwords

- Quick-and-easy email encryption
- Users share passwords out of band

SUS Score

Chart: Participants’ Favorite System


† Systems previously evaluated with same methodology; Mailvelope ↔ PGP
  Pwm ↔ IBE
  Tutanota ↔ Password