Can Secure Email Be Adopted in a Grassroots Fashion?

- Secure email has not seen wide adoption outside of enterprises
- We performed a novel two-person study
  - We recruit pairs of novice users (Johnny and Jane)
  - To model grassroots adoption, each user pair were friends or family
- Users tested three types of secure email systems
  - Pwm: integrated with Gmail, identity-based encryption
  - Tutanota: email depot, PGP + password-based encryption
  - Virtru: integrated with Gmail + email depot, key escrow

Value of Two-Person Studies

- Integration with users' webmail clients viewed as extremely important.
- Pairing novice users familiar with one another put participants at ease, alleviating feelings of being in a lab setting which can elicit unnatural behavior.

Two-Person User Study

- Within-subjects test (n=25)
- Recruited friends to come in and exchange secure email
- Simulated both sender (Johnny) and recipient (Jane) roles
- No training or advance notice that the study focused on security
- Evaluated 3 types of secure email systems
  - Pwm: integrated with Gmail, identity-based encryption
  - Tutanota: email depot, PGP + password-based encryption
  - Virtru: integrated with Gmail + email depot, key escrow

Results — System Usability Scale (SUS)

<table>
<thead>
<tr>
<th>System</th>
<th>Johnny</th>
<th>Jane</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwm</td>
<td>74.5</td>
<td>72.7</td>
<td>73.1</td>
</tr>
<tr>
<td>Virtru</td>
<td>71.1</td>
<td>71.4</td>
<td>71.7</td>
</tr>
<tr>
<td>Tutanota</td>
<td>72.3</td>
<td>64.3</td>
<td>69.2</td>
</tr>
</tbody>
</table>

Results — Favorite System

- Pwm: Jane strongly preferred Pwm
- Tutanota: Disliked lack of webmail integration + password-based encryption scheme confused people
- Virtru: Starkly different favorability ratings between Johnny + Jane because of webmail integration for Johnny and email depot for Jane

Results — Task Completion Times

<table>
<thead>
<tr>
<th>System</th>
<th>Johnny</th>
<th>Jane</th>
<th>Both</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pwm</td>
<td>2:29</td>
<td>2:39</td>
<td>2:34</td>
</tr>
<tr>
<td>Virtru</td>
<td>3:49</td>
<td>3:06</td>
<td>3:22</td>
</tr>
<tr>
<td>Tutanota</td>
<td>5:49</td>
<td>5:28</td>
<td>5:36</td>
</tr>
</tbody>
</table>

Tutanota task completion times nearly twice that of Pwm and Virtru

Participant Feedback

“I thought it was good, I dunno, might’ve taken the pressure off too, where it’s like, ‘Okay, he’s figuring this out too so I can just, you know, I don’t have to feel as under-the-microscope.”

“I was more at ease probably than I would’ve been if it was someone random on the other end... It would’ve felt more mechanical, robotic, whereas I know [her] and I was calling my wife, ‘Hi wife! What’s the password?’ It felt a lot more personable for me...”

“It was good in that you saw the troubles, like the third system [Tutanota], I didn’t even know how it worked, so I ended up sending an email to myself on Gmail so then I could see what was happening on her end, to know like how it works on the other end. So I think it’s good to have two people on each end that don’t know what’s going on, because if it weren’t I’d assume the person on the other side had done it before...”

Full paper was presented at CHI 2016 and received an Honorable Mention Award