Mitigating Email Attacks with Usable Email Encryption

John S. Koh
koh@cs.columbia.edu

Joint work with: Steven M. Bellovin, Jason Nieh

HotSec ‘17
How Hackers Broke Into John Podesta and Colin Powell’s Gmail Accounts

TENS OF MILLIONS OF HACKED GMAIL AND YAHOO EMAIL ACCOUNTS ARE BEING SOLD ON THE DARK WEB
Cock.li e-mail server seized by German authorities, admin announces

The FBI Is Sharing Seized TorMail Data with the DEA
Threat: Compromised email accounts and email servers.

- Emails spend seconds in transit, but years in storage.
- Problem: Encrypting email is hard.
Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0

Alma Whitten
School of Computer Science
Carnegie Mellon University

Why Johnny Still, Still Can’t Encrypt: Evaluating the Usability of a Modern PGP Client

Why Johnny Still Can’t Encrypt: Evaluating the Usability of Email Encryption Software
Steve Sheng
Engineering and Public Policy
Carnegie Mellon University
Levi Broderick
Electrical and Computer Engineering
Carnegie Mellon University
Colleen Alison Koranda
HCII Institute
Carnegie Mellon University

Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express
Simson L. Garfinkel
MIT CSAIL
Robert C. Miller
MIT CSAIL

Why Johnny Can't Encrypt: A Usability Study of PGP
Jan Sousedek
Technische Universität Berlin, Germany
Idea: Automatically encrypt your emails on receipt.

- No PGP and no PKI required.
- Done before, but not usably (previous approaches need highly technical setup).
How: Leverage IMAP.

Easy Email Encryption (E3)

Mail Client

1. Generate key pair*
2. Fetch email
3. Encrypt email
4. Upload ciphertext
5. Delete plaintext

IMAP Server

* Key-pair is locally self-generated. No PKI and no CA.
Why?

● Works with all standard IMAP servers.
● End users control their privacy.

Most importantly:
● It’s **usable** compared to PGP and S/MIME.
Key Management

- **Encrypted** backup of keys in:
  - Your email account (most convenient)
  - Cloud storage
  - ... Anything else?
Usability Study

● We performed two usability studies.
● Participants used:
  ○ Unmodified mail client (K-9 Mail)
  ○ E3 (our modified K-9 Mail client)
  ○ PGP (K-9 Mail with OpenKeychain)

● All agreed that E3 was much more usable than PGP.
Thank you!
(More Detailed) How: Leverage IMAP.

1. **Generate/retrieve key pair.**  
   (Locally self-generated X.509 certificate)
2. **Receive plaintext email.**  
   (FETCH)
3. **Encrypt it.**  
   (S/MIME format without PKI.)
4. **Upload ciphertext.**  
   (APPEND)
5. **Delete plaintext.**  
   (STORE \Deleted, EXPUNGE)
Addendum: Usability Study (1/4)

- We performed two usability studies.
- Participants used:
  - Unmodified mail client (K-9 Mail)
  - E3 (our modified K-9 Mail client)
  - PGP (K-9 Mail with OpenKeychain)
Addendum: Usability Study (2/4)

- Participants’ comments on PGP:
  - “[PGP] is garbage.”
  - “[PGP] is wildly impractical.”
  - “I’ve never actually seen [PGP] used.”

- Participants’ comments on E3:
  - “I would probably actually use this.”
  - Multiple comments on encrypting important emails (automatically detected using filters).
Addendum: Usability Study (3/4)

<table>
<thead>
<tr>
<th>Soln.</th>
<th>Count</th>
<th>Mean</th>
<th>Std. Dev</th>
<th>Min.</th>
<th>Q1</th>
<th>Median</th>
<th>Q3</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>K-9</td>
<td>12</td>
<td>82.12</td>
<td>11.67</td>
<td>65</td>
<td>72.50</td>
<td>82.50</td>
<td>90.00</td>
<td>100</td>
</tr>
<tr>
<td>E3</td>
<td>12</td>
<td>81.73</td>
<td>10.82</td>
<td>60</td>
<td>72.50</td>
<td>82.50</td>
<td>90</td>
<td>97.50</td>
</tr>
<tr>
<td>PGP</td>
<td>12</td>
<td>34.81</td>
<td>23.09</td>
<td>2.50</td>
<td>18.13</td>
<td>30.50</td>
<td>38.75</td>
<td>47.50</td>
</tr>
</tbody>
</table>

Figure 11. System Usability Scale summarized scores.
Addendum: Usability Study (4/4)

<table>
<thead>
<tr>
<th>#</th>
<th>Question (1 = Strongly Disagree, 5 = Strongly Agree)</th>
<th>Mean</th>
<th>Std.</th>
<th>Min.</th>
<th>Med.</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>I found it easy to use unmodified K-9 w/o encryption.</td>
<td>4.38</td>
<td>0.96</td>
<td>2</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>12</td>
<td>I found it easy to use K-9 w/ E3 encryption.</td>
<td>4.38</td>
<td>0.65</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>13</td>
<td>I found it easy to use PGP encryption.</td>
<td>2.08</td>
<td>0.95</td>
<td>1</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>14</td>
<td>I thought that K-9 w/ E3 was easier to use than PGP.</td>
<td>4.77</td>
<td>0.44</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>15</td>
<td>The extra security with K-9 w/ E3 encryption is worth the extra steps compared to unmodified K-9 w/o encryption.</td>
<td>4.23</td>
<td>0.73</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>16</td>
<td>The extra security with PGP encryption is worth the extra steps compared to unmodified K-9 w/o encryption.</td>
<td>2.69</td>
<td>1.44</td>
<td>1</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>17</td>
<td>The extra security with PGP is worth the extra steps compared to K-9 w/ E3 encryption.</td>
<td>1.92</td>
<td>0.95</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

Figure 12. Summarized scores for added survey questions. (Questions are abbreviated for spacing reasons.)