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

LORENZO FRANCESCHI-BICCHIERAI
Oct 20 2016, 9:30am

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
HCI Institute
Carnegie Mellon University

Why Johnny Can't Encrypt: A Usability Study of PGP

Jan Sousedek
Technische Universität Berlin, Germany

Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express

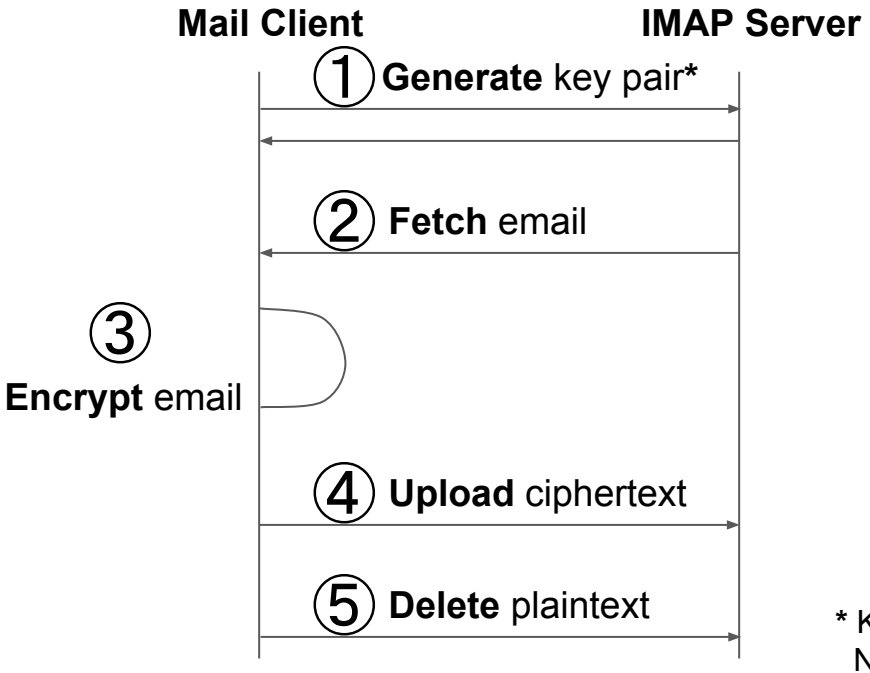
Simson L. Garfinkel
MIT CSAIL

Robert C. Miller
MIT CSAIL

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.



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

Easy Email Encryption (E3)

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

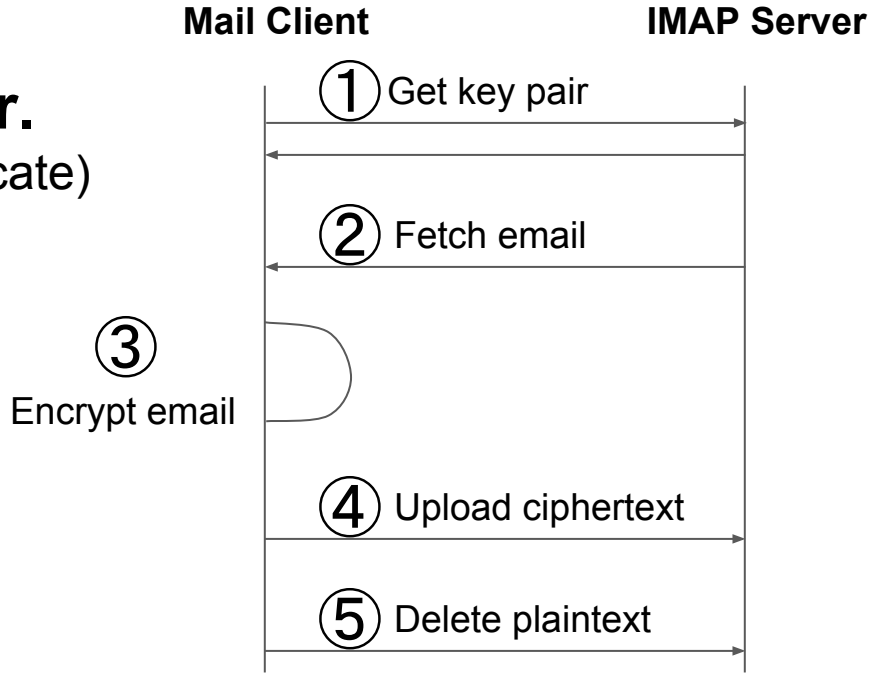
- We performed two usability studies.
- Participants used:
  - **Unmodified** mail client (K-9 Mail)
  - **E3** (our modified K-9 Mail client)
  - **PGP** (K-9 Mail with OpenKeychain)

- 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)

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

Figure 11. System Usability Scale summarized scores.

Addendum: Usability Study (4/4)

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

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