ATHENE
National Research Center
for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences

Content-Type: multipart/oracle

Tapping into Format Oracles in Email End-to-End Encryption

FABIAN ISING[1,2], DAMIAN PODDEBNIAK[1], TOBIAS KAPPERT[1],
CHRISTOPH SAATJOHANN[1,2], SEBASTIAN SCHINZEL[1,2]

EMAIL: FABIAN.ISING@SIT.FRAUNHOFER.DE

MASTODON: @MURGI@INFOSEC.EXCHANGE

[1] *FH Münster University of Applied Sciences*
[2] *National Research Center for Applied Cybersecurity ATHENE*

What's an email?

MIME

```
From:          Alice
To:            Bob
Subject:       Example
Content-Type: text/plain

Hello Bob, how was your weekend?
```

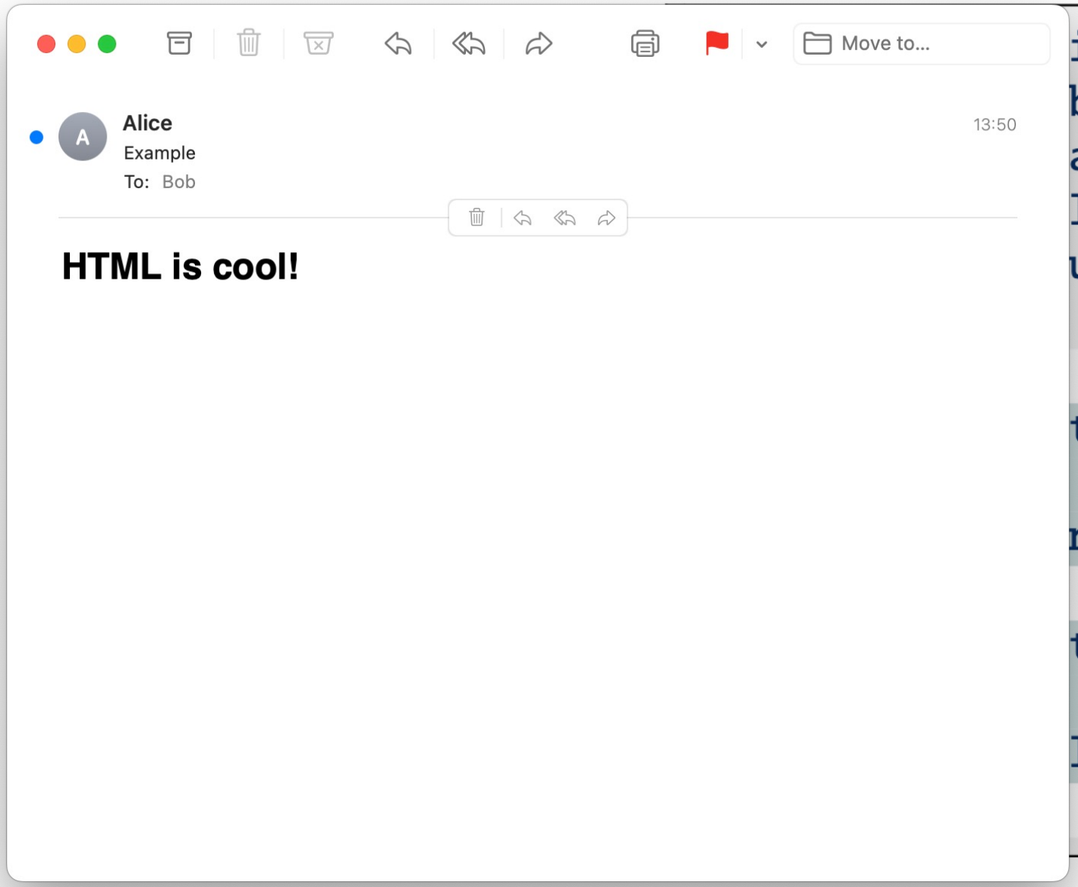
What's an email?

MIME

```
From:          Alice
To:            Bob
Subject:       Example
Content-Type: multipart/alternative;
              boundary=alternative

--alternative // --------------------
  Content-Type: text/plain

  Plain old boring plaintext.
--alternative // --------------------
  Content-Type: text/html

  <b>HTML is cool!</b>
--alternative--
```

What’s an email?

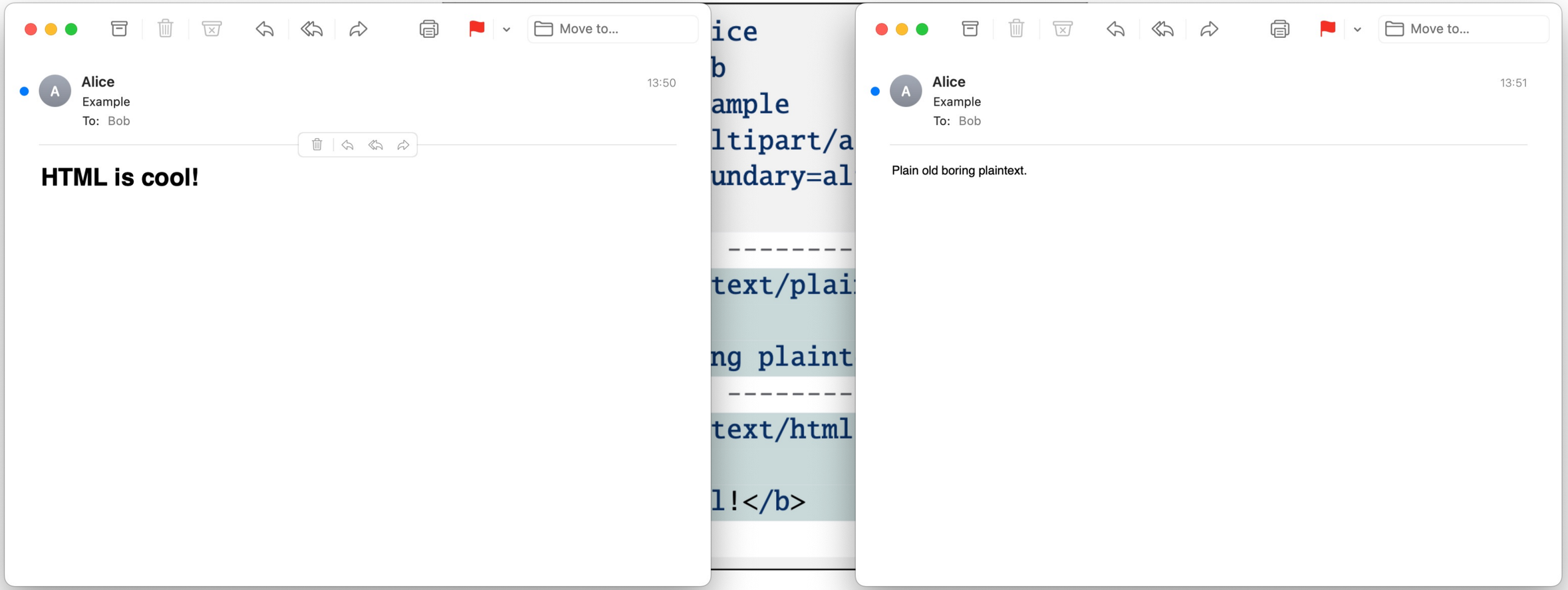
MIME



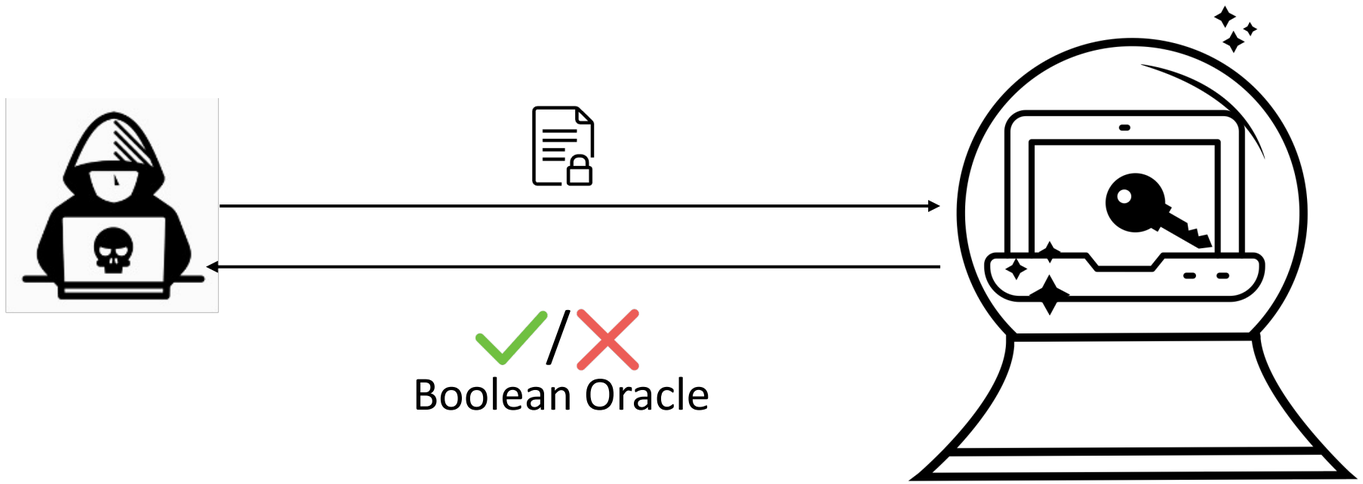

```
ice
b
ample
ltipart/alternative;
undary=alternative

 --------------------
text/plain

ng plaintext.
 --------------------
text/html

l!</b>
```

What’s an email?

MIME

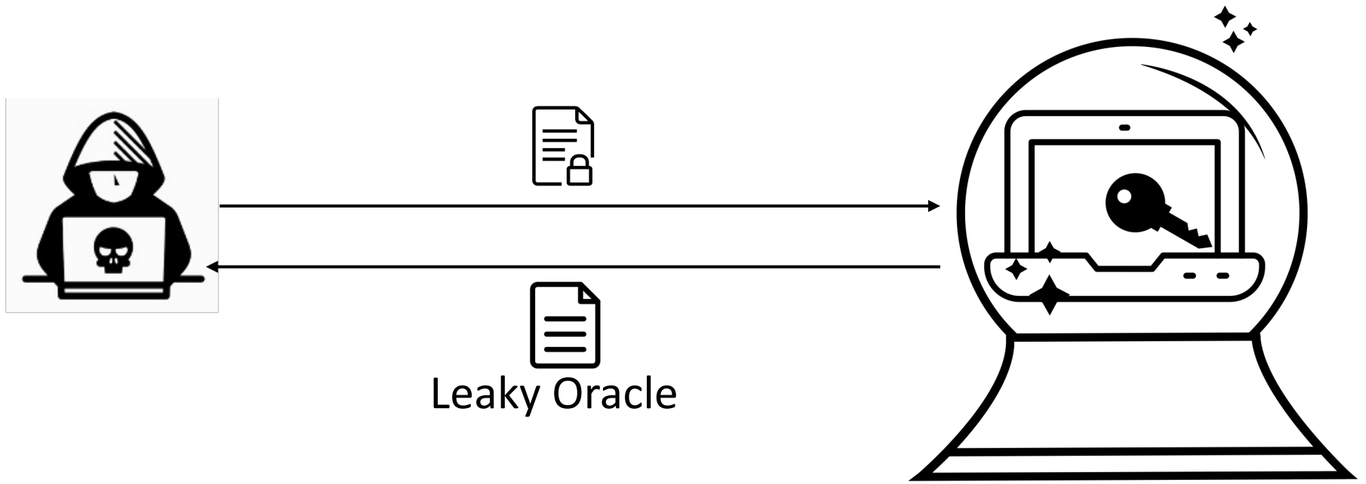


Decryption Oracle Attacks

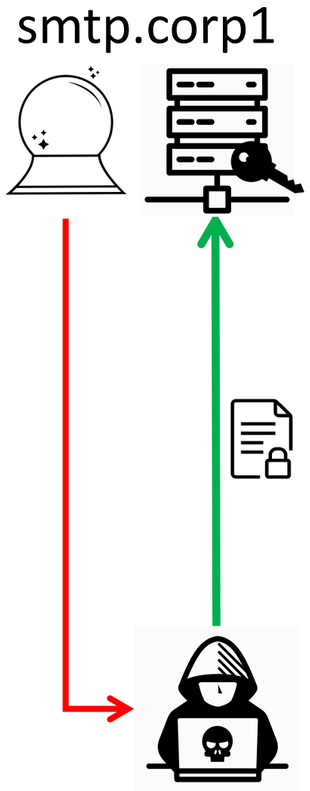


Decryption Oracle Attacks

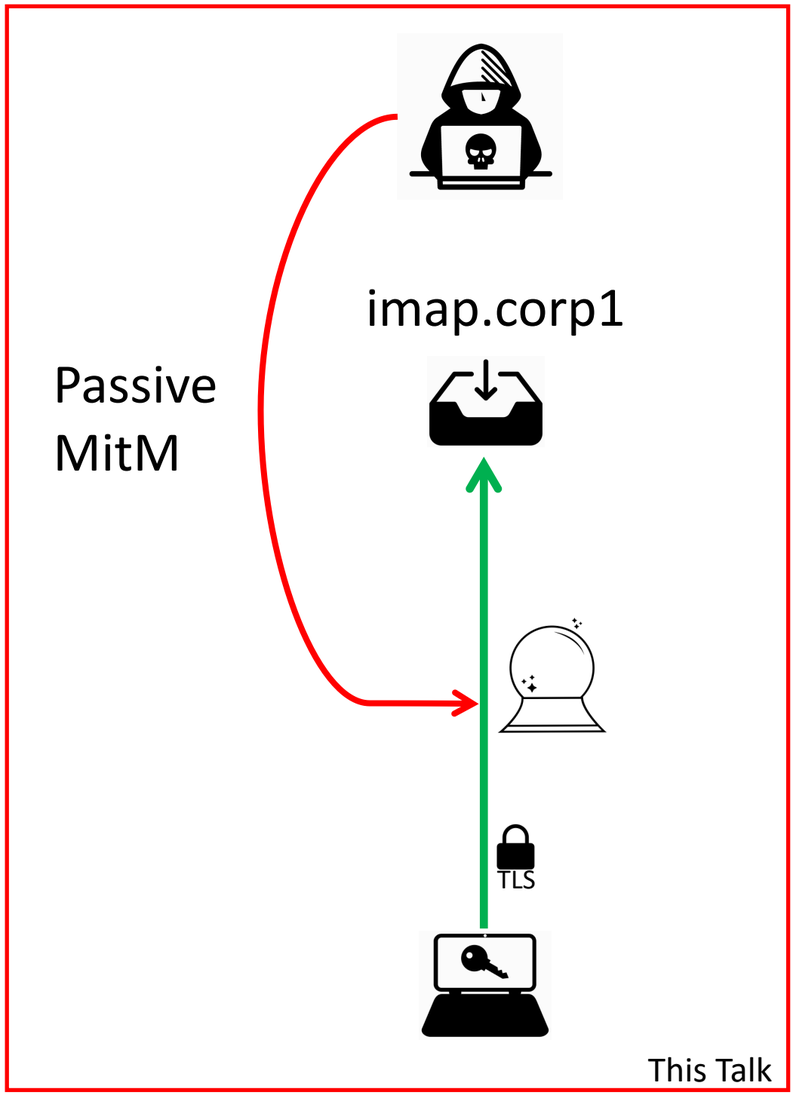
ATHENE
National Research Center
for Applied Cybersecurity
FH MÜNSTER
University of Applied Sciences



Attacker Model



Paper Appendix



IMAP – Fetching

ATHENE
National Research Center for Applied Cybersecurity
FH MÜNSTER
University of Applied Sciences

Message ID Data Items

```
C: A FETCH 1 (BODYSTRUCTURE)
S: * 1 FETCH (BODYSTRUCTURE (
        ("text" "plain" NIL NIL NIL "7BIT" 29 NIL)
        ("text" "html" NIL NIL NIL "7BIT" 22 NIL)
        "alternative" ("boundary" "alternative") NIL NIL NIL))
S: A OK fetch done.
C: B FETCH 1 (BODY[1])
S: * 1 FETCH (BODY[1] {29}
         Plain old boring plaintext.
     )
S: B OK fetch done.
```

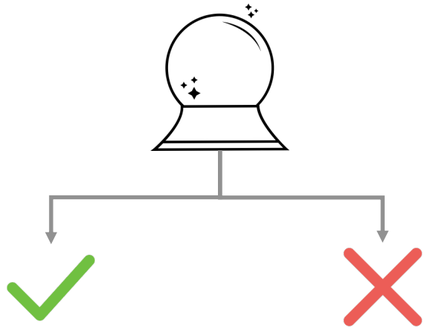
```
From:          Alice
To:            Bob
Subject:       Example
Content-Type:  multipart/alternative;
               boundary=alternative

--alternative // --------------------
  Content-Type: text/plain

  Plain old boring plaintext.
--alternative // --------------------
  Content-Type: text/html

  <b>HTML is cool!</b>
--alternative--
```

In Search of Side-Channels

ATHENE
National Research Center for Applied Cybersecurity
FH MÜNSTER
University of Applied Sciences

```
From:          Alice
To:            Bob
Subject:       Example
Content-Type:  multipart/alternative;
               boundary=alternative

--alternative // ------------------------------------
  Content-Type: application/encrypted

  [Base64-encoded ciphertext]
--alternative // ------------------------------------
  Content-Type: application/encrypted

  [Base64-encoded ciphertext]
--alternative--
```

```
C: A FETCH 1 (BODYSTRUCTURE)
S: * 1 FETCH (BODYSTRUCTURE (…))
C: B FETCH 1 (BODY[2])
S: * 1 FETCH (BODY[2] {…}
```

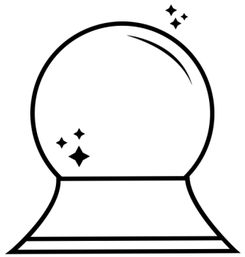


C: C LOGOUT C: C FETCH 1 (BODY[1])

Oracle in E-Mail E2EE

ATHENE
National Research Center for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences

Criterion	S/MIME v3.2	OpenPGP
 Ciphertext Malleability	 No Integrity Protection	 MDC
 Potential Oracles	 PKCS#7 Padding, PKCS#1v1.5	 CFB Mode, Weak Bleichenbacher Oracles

	Multiple Encrypted Parts	Fetching Behavior		Decryption	Practical Exploit
		Body (Parts)	Lazy		
Required for practical exploit	✓	●	✓	●	

Legend					
✓	Yes	●	Automatic in background.	■	Found
–	No	○	Needs explicit user interaction.	□	Not found
~	Situation dependent	◑	Upon opening email.		
		?	Not detectable.		

Client	Multiple Encrypted Parts	Fetching Behavior		Decryption	Practical Exploit
		Body (Parts)	Lazy		
Required for practical exploit	✓	●	✓	●	
Clients not supporting multiple encrypted parts					
Airmail	–	●	–	◑	□
eM Client	–	◑	✓	?	□
Mail (macOS)	–	●	~	●	□
MailDroid	–	●	✓	○	□
Nine	–	●	–	◑	□
Outlook 2016	–	●	–	?	□
Outlook 2019	–	●	–	?	□
Postbox	–	●	–	?	□
R2Mail2	–	◑	✓	◑	□
Thunderbird	–	●	–	?	□

Client	Multiple Encrypted Parts	Fetching Behavior		Decryption	Practical Exploit
		Body (Parts)	Lazy		
Required for practical exploit	✓	●	✓	●	
Clients not automatically fetching single body parts					
Claws	✓	◑	–	◑	□
Horde IMP	✓	◑	✓	◑	□
Evolution	✓	◑	–	◑	□
KMail	✓	◑	–	○	□
Mutt	✓	◑	–	○	□
The Bat!	✓	◑	–	○	□
Trojitá	✓	◑	✓	◑	□

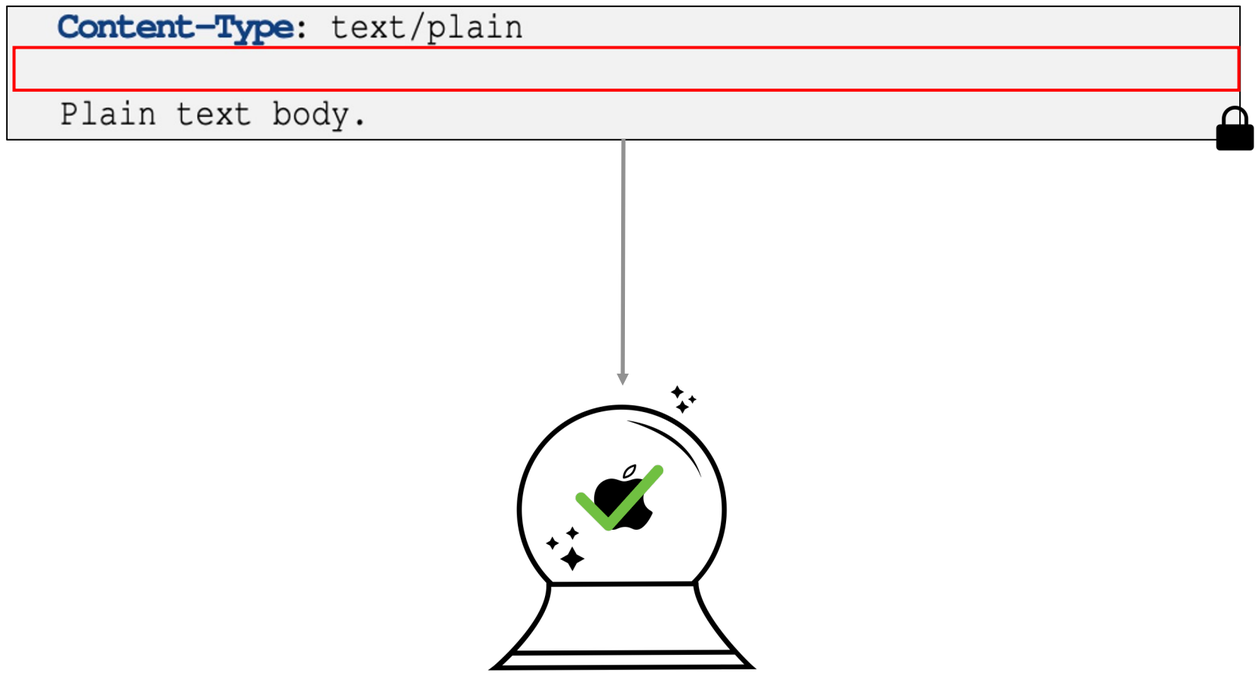
Client	Multiple Encrypted Parts	Fetching Behavior		Decryption	Practical Exploit
		Body (Parts)	Lazy		
Required for practical exploit	✓	●	✓	●	
Clients not using lazy fetching					
MailMate	✓	●	–	◑	□
Clients fulfilling all criteria					
Mail (iOS)	✓	●	✓	●	■

Empty Line Oracle

A NEW FORMAT ORACLE

ATHENE
National Research Center for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences



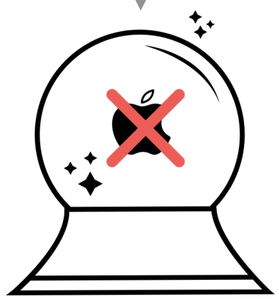
Empty Line Oracle

A NEW FORMAT ORACLE

ATHENE
National Research Center for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences

```
Content-Type: text/plain
No Empty Line
Plain text body.
```

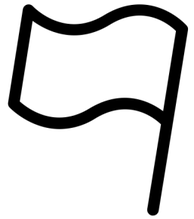


The Empty Line Oracle Exploit

DECRYPTING A BLOCK

ATHENE
National Research Center for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences



Setup:

Guess two bytes in a block.

```
\x00    \x00  ✗
\x00    \x01  ✗
  ⋮
\n      \n    ✓
```

Per Byte:

Fixate one known byte to `\n`

```
\n      \x00  ✗
\n      \x01  ✗
  ⋮
\n      \n    ✓
```

Result:

Decrypted Ciphertext Block

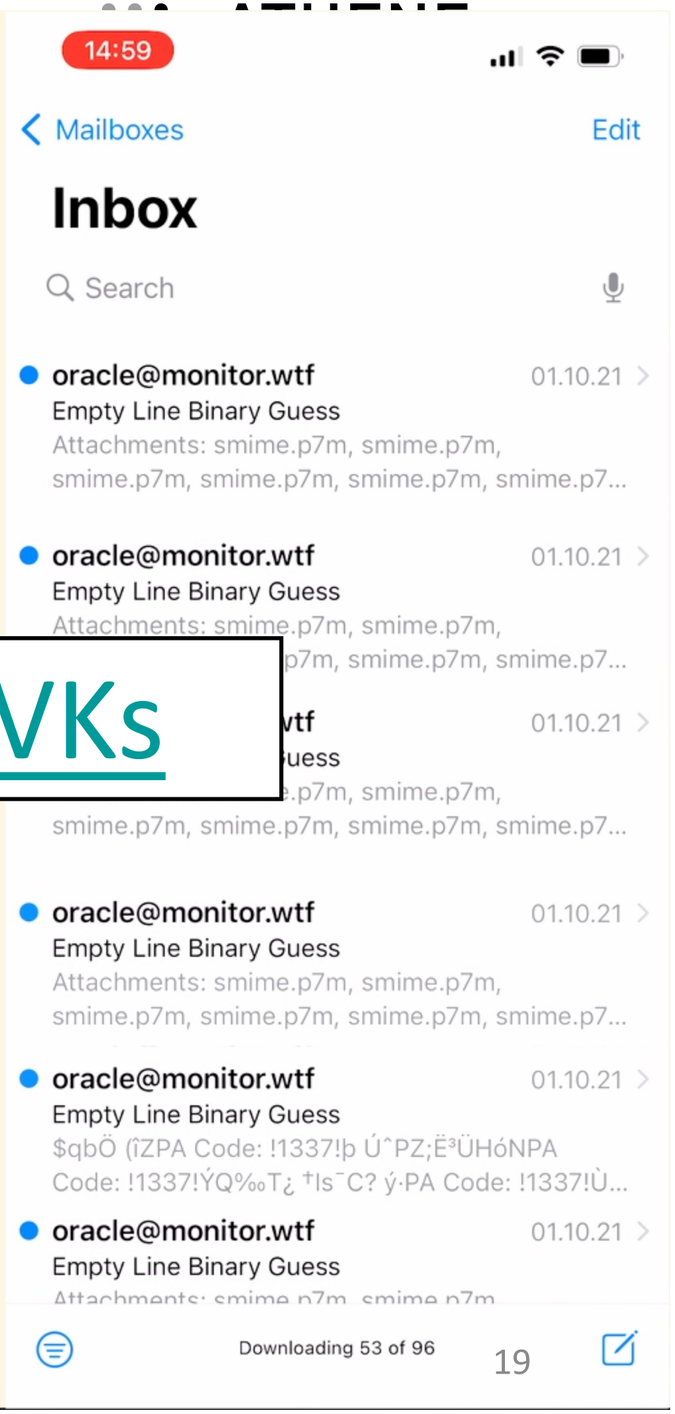
Optimizations:

900 Queries/Ciphertext Block
< 7 Minutes

```
2022-12-07 14:59:22,462 - INFO - UID 200104 Using Alphabet b'1\x00'..b'1\x0f'
2022-12-07 14:59:22,463 - INFO - UID 200105 Using Alphabet b'1\x10'..b'1\x1f'
2022-12-07 14:59:22,465 - INFO - UID 200106 Using Alphabet b'1 '..b'1/'
2022-12-07 14:59:22,468 - INFO - UID 200107 Using Alphabet b'10'..b'1?'
2022-12-07 14:59:22,472 - INFO - UID 200108 Using Alphabet b'1@'..b'1O'
2022-12-07 14:59:22,476 - INFO - UID 200109 Using Alphabet b'1P'..b'1_'
2022-12-07 14:59:22,477 - INFO - UID 200110 Using Alphabet b'1`'..b'1o'
2022-12-07 14:59:22,479 - INFO - UID 200111 Using Alphabet b'1p'..b'1\x7f'
2022-12-07 14:59:22,484 - INFO - UID 200112 Using Alphabet b'2\x00'..b'2\x0f'
2022-12-07 14:59:22,488 - INFO - UID 200113 Using Alphabet b'2\x10'..b'2\x1f'
2022-12-07 14:59:22,493 - INFO - UID 200114 Using Alphabet b'2 '..b'2/'
2022-12-07 14:59:22,497 - INFO - UID 200115 Using Alphabet b'20'..b'2?'
2022-12-07 14:59:22,499 - INFO - UID 200116 Using Alphabet b'2@'..b'2O'
2022-12-07 14:59:22,501 - INFO - UID 200117 Using Alphabet b'2P'..b'2_'
2022-12-07 14:59:22,503 - INFO - UID 200118 Using Alphabet b'2`'..b'2o'
2022-12-07 14:59:22,506 - INFO - UID 200119 Using Alphabet b'2p'..b'2\x7f'
2022-12-07 14:59:22,509 - INFO - UID 200120 Using Alphabet b'3\x00'..b'3\x0f'
2022-12-07 14:59:22,512 - INFO - UID 200121 Using Alphabet b'3\x10'..b'3\x1f'
2022-12-07 14:59:22,513 - INFO - UID 200122 Using Alphabet b'3 '..b'3/'
2022-12-07 14:59:22,516 - INFO - UID 200123 Using Alphabet b'30'..b'3?'
2022-12-07 14:59:22,520 - INFO - UID 200124 Using Alphabet b'3@'..b'30'
2022-12-07 14:59:22,523 - IN
2022-12-07 14:59:22,527 - IN
2022-12-07 14:59:22,531 - IN
```

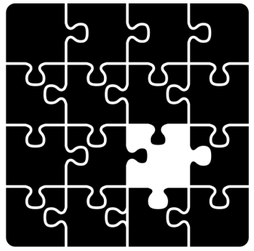
https://youtu.be/1_nvhFfWVKs

```
59D12Jwp | .. Kh/FIKPKLomw6O
59D12Jwp | .. I0ItLehv7CofxSCjyi6JsOjufkfOcdwD5h28zBx1dsUjQy0t6G/sKh/FIKPKLomw6O5+R85x3APm\n
59D12Jwp | .. HbzMHHV2xSNALS3ob+wqH8Ugo8ouibDo7n5HznHcA+YdvMwcdXbFI0EtLehv7CofxSCjyi6JsOju\n
59D12Jwp | .. fkfOcdwD5h28zBx1dsUjRi0t6G/sKh/FIKPKLomw6O5+R85x3APmHbzMHHV2xSNHLS3ob+wqH8Ug\n
59D12Jwp | .. o8ouibDo7n5HznHcA+YdvMwcdXbFI0QtLehv7CofxSCjyi6JsOjufkfOcdwD5h28zBx1dsUjRS0t\n
59D12Jwp | .. 6G/sKh/FIKPKLomw6O5+R85x3APmHbzMHHV2xSNaLS3ob+wqH8Ugo8ouibDo7n5HznHcA+YdvMwc\n
59D12Jwp | .. dXbFI1stLehv7CofxSCjyi6JsOjufkfOcdwD5h28zBx1dsUjWC0t6G/sKh/FIKPKLomw6O5+R85x\n
59D12Jwp | .. 3APmHbzMHHV2xSNZLS3ob+wqH8Ugo8ouibDo7n5HznHcA+YdvMwcdXbFI14tLehv7CofxSCjyi6J\n
59D12Jwp | .. sOjufkfOcdwD5h28zBx1dsUjXy0t6G/sKh/FIKPKLomw6O5+R85x3APmHbzMHHV2xSNcLS3ob+wq\n
59D12Jwp | .. H8Ugo8ouibDo7n5HznHcA+YdvMwcdXbFI10tLehv7CofxSCjyi6JsOjufkfOcdwD5h28zBx1dsUj\n
59D12Jwp | .. Ui0t6G/sKh/FIKPKLomw6O5+R85x3APmHbzMHHV2xSNTLS3ob+wqH8Ugo8ouibDo7n5HznHcA+Yd\n
59D12Jwp | .. vMwcdXbFI1AtLehv7CofxSCjyi6JsOjufkfOcdwD5h28zBx1dsUjUS0t6G/sKh/FIKPKLomw6O5+\n
59D12Jwp | .. R85x3APmHbzMHHV2xSNWLS3ob+wqH8Ugo8ouibDo7n5HznHcA+YdvMwcdXbFI1ctLehv7CofxSCj\n
59D12Jwp | .. yi6JsOjufkfOcdwD5h28zBx1dsUjVC0t6G/sKh/FIKPKLomw6O5+R85x3APmHbzMHHV2xSNVLS3o\n
59D12Jwp | .. b+wqH8Ugo8ouibDo7n5HznHcA+YdvMwcdXbF\n
59D12Jwp | .. )\r\n
59D12Jwp | S: 4 OK fetch done.\r\n
59D12Jwp | C: 5 LOGOUT\r\n
59D12Jwp | S: * BYE bye done.\r\n
59D12Jwp | S: 5 OK logout done.\r\n
59D12Jwp | {"message": "Connection was closed."}
```

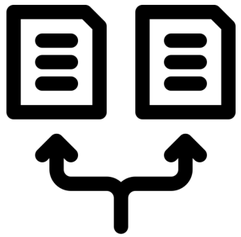


Resistance

WHY ARE THE CLIENTS NOT VULNERABLE?



Incomplete Implementations



Selective Fetching

Parallel Decryption & Fetching

Implementation Quirks

Resistance

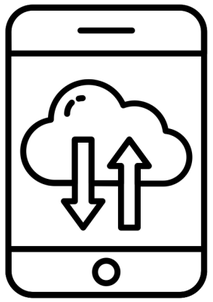
USABILITY VS SECURITY

ATHENE
National Research Center for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences

Separate encryption of attachments

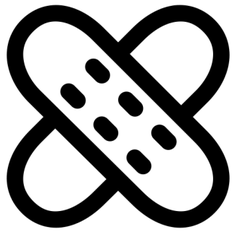
Notifications and Searching



Low Data Contingents & Flaky Connections

Countermeasures

SHORT- AND MID-TERM

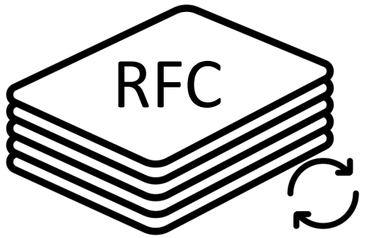


Stopgap

Prevent Oracles

Constant Time Operations

Restrict Features



Update Standards

AEAD

[1]

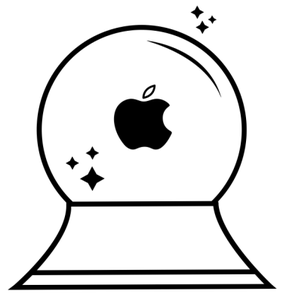
[1] Schwenk et al. - Mitigation of Attacks on Email End-to-End Encryption

Conclusion

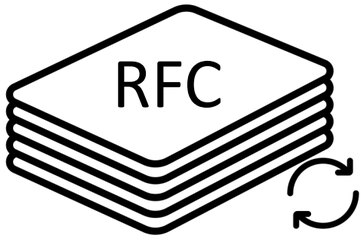
ORACLE ATTACK ON EMAIL E2EE

Many Clients
are safe

'Defenses' are
involuntary



Some Attacks
still possible



Explicit Countermeasures
are necessary

ATHENE
National Research Center
for Applied Cybersecurity

FH MÜNSTER
University of Applied Sciences

Thanks for Listening!

FABIAN ISING

EMAIL: FABIAN.ISING@SIT.FRAUNHOFER.DE
MASTODON: @MURGI@INFOSEC.EXCHANGE