Content-Type: multipart/oracle
Tapping into Format Oracles in Email End-to-End Encryption

FABIAN ISING¹,², DAMIAN PODDEBNIAK¹, TOBIAS KAPPERT¹, CHRISTOPH SAATJOHANN¹,², SEBASTIAN SCHINZEL¹,²

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

&lt;b&gt;HTML is cool!&lt;/b&gt;

--alternative--
What’s an email?

MIME

HTML is cool!
What’s an email?

MIME

HTML is cool!

Plain old boring plaintext.
Decryption Oracle Attacks
Decryption Oracle Attacks

Leaky Oracle
Attacker Model

smtp.corp1

Passive MitM

imap.corp1

Paper Appendix

This Talk
IMAP – Fetching

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

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

<table>
<thead>
<tr>
<th>Criterion</th>
<th>S/MIME v3.2</th>
<th>OpenPGP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ciphertext Malleability</td>
<td>✓ No Integrity Protection</td>
<td>❌ MDC</td>
</tr>
<tr>
<td>Potential Oracles</td>
<td>✓ PKCS#7 Padding, PKCS#1v1.5</td>
<td>❌ CFB Mode, Weak Bleichenbacher Oracles</td>
</tr>
<tr>
<td>Required for practical exploit</td>
<td>Multiple Encrypted Parts</td>
<td>Fetching Behavior</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>●</td>
</tr>
</tbody>
</table>

**Legend**

- ✓ Yes
- - No
- ~ Situation dependent
- ? Not detectable.

- ● Automatic in background.
- ○ Needs explicit user interaction.
- ■ Found
- □ Not found
- Upon opening email.
<table>
<thead>
<tr>
<th>Client</th>
<th>Multiple Encrypted Parts</th>
<th>Fetching Behavior</th>
<th>Practical Exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>Body (Parts)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lazy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Decryption</td>
<td></td>
</tr>
<tr>
<td>Required for practical exploit</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client</th>
<th>Required for practical exploit</th>
<th>Body (Parts)</th>
<th>Lazy</th>
<th>Decryption</th>
<th>Practical Exploit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airmail</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>eM Client</td>
<td></td>
<td></td>
<td>✓</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Mail (macOS)</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MailDroid</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Nine</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Outlook 2016</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Outlook 2019</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Postbox</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>R2Mail2</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Thunderbird</td>
<td></td>
<td>✓</td>
<td></td>
<td>?</td>
<td></td>
</tr>
<tr>
<td>Client</td>
<td>Multiple Encrypted Parts</td>
<td>Fetching Behavior</td>
<td>Practical Exploit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------</td>
<td>-------------------</td>
<td>------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Body (Parts)</td>
<td>Symmetric</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lazy</td>
<td>Decryption</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Required for practical exploit</strong></td>
<td>✓</td>
<td>●</td>
<td>✓</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td><strong>Clients not automatically fetching single body parts</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Claws</td>
<td>✓</td>
<td>●</td>
<td>–</td>
<td>●</td>
<td>☐</td>
</tr>
<tr>
<td>Horde IMP</td>
<td>✓</td>
<td>●</td>
<td>✓</td>
<td>●</td>
<td>☐</td>
</tr>
<tr>
<td>Evolution</td>
<td>✓</td>
<td>●</td>
<td>–</td>
<td>●</td>
<td>☐</td>
</tr>
<tr>
<td>KMail</td>
<td>✓</td>
<td>●</td>
<td>–</td>
<td>○</td>
<td>☐</td>
</tr>
<tr>
<td>Mutt</td>
<td>✓</td>
<td>●</td>
<td>–</td>
<td>○</td>
<td>☐</td>
</tr>
<tr>
<td>The Bat!</td>
<td>✓</td>
<td>●</td>
<td>–</td>
<td>○</td>
<td>☐</td>
</tr>
<tr>
<td>Trojitá</td>
<td>✓</td>
<td>●</td>
<td>✓</td>
<td>○</td>
<td>☐</td>
</tr>
<tr>
<td>Client</td>
<td>Multiple Encrypted Parts</td>
<td>Fetching Behavior</td>
<td>Practical Exploit</td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>--------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Body (Parts)</td>
<td>Lazy</td>
<td>Decryption</td>
<td></td>
</tr>
<tr>
<td><strong>Required for practical exploit</strong></td>
<td>□</td>
<td>●</td>
<td>✓</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td><strong>Clients not using lazy fetching</strong></td>
<td></td>
<td>●</td>
<td>–</td>
<td>○</td>
<td>□</td>
</tr>
<tr>
<td>MailMate</td>
<td>□</td>
<td>●</td>
<td>–</td>
<td>○</td>
<td>□</td>
</tr>
<tr>
<td><strong>Clients fulfilling all criteria</strong></td>
<td>□</td>
<td>●</td>
<td>✓</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Mail (iOS)</td>
<td>□</td>
<td>●</td>
<td>✓</td>
<td>●</td>
<td>■</td>
</tr>
</tbody>
</table>
Empty Line Oracle
A NEW FORMAT ORACLE

Content-Type: text/plain
Plain text body.
Empty Line Oracle
A NEW FORMAT ORACLE

Content-Type: text/plain
No Empty Line
Plain text body.
The Empty Line Oracle Exploit

DECRYPTING A BLOCK

**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
https://youtu.be/1_nvhFfWVKs
Resistance

WHY ARE THE CLIENTS NOT VULNERABLE?

Incomplete Implementations

Selective Fetching

Parallel Decryption & Fetching

Implementation Quirks
Resistance

USABILITY VS SECURITY

Separate encryption of attachments

Notifications and Searching

Low Data Contingents & Flaky Connections
Countermeasures
SHORT- AND MID-TERM

Stopgap

Prevent Oracles

Restrict Features

Update Standards

AEAD

Constant Time Operations

[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

RFC
Thanks for Listening!

FABIAN ISING

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